

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Adobe® PDF
Magazine Version

NETWORK SECURITY

**BLACKBERRY – A SECURITY SYSTEM
THAT CHANGED THE WORLD**

**GET IN THROUGH THE BACKDOOR:
POST EXPLOITATION WITH ARMITAGE**

NETWORK SECURITY – DATA BREACHES

EXAMINE YOUR NETWORK WITH NMAP

EXPLORING GCIH CERTIFICATION

**IS DATA SECURE ON THE PASSWORD
PROTECTED BLACKBERRY DEVICE?**

**BREAKING THE CODE:
BRUTE FORCING THE ENCRYPTION KEY**

Vol.6 No.2
Issue 02/2011(38) ISSN: 1733-7186

PLUS

EMERGING THREATS:
WHAT IS GOOD ENOUGH COVERAGE?

Penetration Testing Training that will make you stand out



[Click here
Free SQL Injection
module](#)



Learn at your own pace, when you want, with lifetime

Learn how much you want everyday with no expiry pressure. Our engaging e-learning environment is ideal if you work. It sets you free from long boring learning sessions.



Learn Professional Penetration Testing and Function in one course

Penetration testing has evolved. It's time to be professionals. Study how to handle your pentesting project and how to report your findings to executives, clients or your employer

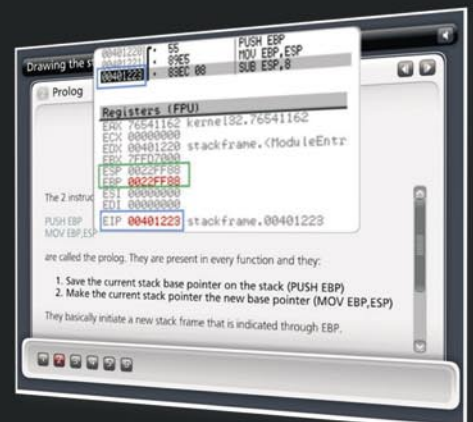


Get certified. Become an eCPPT

Our certification proves your skills as a hacker and as a professional. Produce your penetration testing report, have it reviewed by one of our instructors, get recognized as a professional penetration tester.

included in price

The fastest path to Professional Penetration Testing



Get Yourself Trained And Certified As A Penetration Tester... At Your Own Pace!

Penetration testing is big business. As companies and government organizations go increasingly electronic, there is a growing demand for IT professionals who can evaluate the security of these computer systems, networks and suggest safeguards.

Traditionally, training to become a certified "penetration tester" or "ethical hacker" has been a long, drawn-out process. Most certifications assume that candidates already have some form of networking or programming background, which makes it difficult for beginners to get started. Others require the physical attendance of training classes conducted only at certain locations. In all, the time and money spent in obtaining such a certification can be costly.

A new breed of penetration testing courses in the market looks set to change all this. One such course is "Penetration Testing Pro" offered by eLearnSecurity, an Italian IT security firm headed by Armando Romeo, who is also founder of the respected Hackers Center Web Portal.

His real world credentials aside, Armando hopes "Penetration Testing Pro" will change the way such training is conducted in the industry. "We set out to design the most comprehensive training course for IT professionals and anyone who cannot take time off to attend physical lessons. Our course allows them to learn the latest intrusion methods at their own pace, through over 1600 interactive e-learning slides and video lessons. There's no longer a need to sit through hours of boring classes," he says.

A CEH AND LPT KILLER?

Industry experts seem to agree with his methodology, too. Jason Haddix, columnist at EthicalHacker.net, feels the course has great potential.

"I kept thinking – this is what the CEH / LPT should have been – and I am delighted to say that if students can master the topics and techniques in eLearnSecurity's Penetration Testing Pro, they should be well on their way to being an accomplished pentester," he writes.

CEH and LPT refer to *Certified Ethical Hacker* and *Licensed Penetration Tester*

respectively, both the gold standards for penetration testing in the industry.

Another veteran industry insider, Timothy Everson from Novell, who holds multiple certifications such as MCNE, CDE, CLE, CCNA on top of the CEH says, "For anyone who is budget constrained, I'd say, with total confidence, that the value of eLearnSecurity training meets or exceeds the value of many of the other programs available. If one truly desires to learn the technical aspects of IT security, it's a certification course well worth the time and investment."

Nathan Suri, an Information Security Architect who holds CISSP, SCJP and CSSLP certifications agrees, "The combination of slides, video, hands-on examples with the lab to practice some of the techniques makes it very effective. I like the balance of theory and practice."

REAL WORLD APPROACH USED BY PENTESTERS

Perhaps it is this real world, raw approach to teaching penetration testing that has made this course so popular. Besides Armando, the other co-authors include Brett Arion, a U.S IT Security specialist, Nitin and Vipin Kumar. Nitin and Vipin, both from India rose to fame after authoring the acclaimed "Windows Vista Bootkit" and "Windows 7 Bootkit" researches at BlackHat.

HOW TO BECOME A HIGHLY SOUGHT AFTER PENTESTER

Armando explains, "Just because someone is certified does not make him a good penetration tester. Penetration testing is part art and science. A tester needs to have experience to know which vulnerabilities to look out for. He also needs to give workable, business-minded suggestions to his clients for countering these exploits."

Given the depth of knowledge required, can someone with no prior experience still be trained to become a good penetration tester?

"Absolutely. The training aspect is key. We start with our e-learning slides and videos which explain every aspect of web application, system and network security testing.

We then follow up with labs and practical exercises. Instead of a multiple choice certification exam, ours is an actual penetration testing exercise. We are not just interested in testing theoretical knowledge. Candidates are required to conduct their own penetration tests on a given target and submit an actual test report for grading."

These rigorous requirements, Armando insists, are needed to ensure that the course is as realistic as possible. "Every student should have the confidence to conduct actual penetration testing in a commercial or mission critical setting."

IS THIS FOR YOU?

If you are looking to further your IT career, or even make a transition to the lucrative field of Penetration testing, these new breed of courses such as "Penetration Testing Pro" may be a great choice. Not only do they cost a mere fraction of what other certifications ask for, it is a great way to get up to speed with the latest penetration testing methods by learning from *actual* hackers and understanding their psychology. Learning at one's own pace without having to set time aside for regular lessons is also a big draw.

At the end of the day, does Armando hope that his course will *replace* the CEH as the de facto certification in the industry?

"Definitely not," he says with a laugh. "We provide the technical training and flexibility that the CEH does not. In fact, students who take our course as a starting point will also acquire most of the knowledge needed to pass other certifications such as CEH and LPT. This means they'll find it much easier later on to pass their certifications as well."

For more information on eLearnSecurity's Penetration Testing Pro course, visit <http://www.eLearnSecurity.com>.

HAKIN9 team

Editor in Chief: Karolina Lesińska
karolina.lesińska@hakin9.org

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Steve Lape, Shyaam Sundhar, Donald Iverson, Michael Munt

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Allan Konar, Michael Munt

Top Betatesters: Rebecca Wynn, Bob Folden, Shyaam Sundhar, Steve Hodge, Nick Baronian.

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Pawel Marciniak

CEO: Ewa Łozowicka
ewa.łozowicka@software.com.pl


Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org


Marketing Director: Karolina Lesińska
karolina.lesińska@hakin9.org

Subscription: Iwona Brzezik
Email: iwona.brzezik@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by  SmartDraw

The editors use automatic DTP system 
Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

We always try to meet your expectations and follow the most recent issues in the IT security field. Based on the most popular discussions among IT security experts and the results of the survey on our website, we decided that network security would be one of the most appreciated topics.

In this issue you will find several topics with a strong focus on network security. Our ID fraud expert – Julian Evans talks about network security in terms of data breaches with an emphasis on protecting our personal and financial information. Matt Jonkman warns you about the so called 100% secure products. In the Defense section Mohsen shows you how to scan your network using Nmap.

I would also recommend you to take a look at the article about data security on Blackberry devices by Yury Chemerkin. You will find an introduction to Blackberry and its security aspect in Basic section.

We have also prepared some useful info on certifications, since it has become a must-have for all who wants to be in the IT security field.

Enjoy your reading
Editor in Chief: Karolina Lesińska
Editor-in-Chief



REGULARS

6 in Brief

Latest News From the IT Security World

Armando Romeo, *eLearnSecurity*
ID Theft Protect

8 Tools

Wuala – Secure Online Storage
by Michael Munt

9 Book review

A Beginners Guide to Ethical Hacking
by Shyaam Sundhar

36 ID fraud expert says...

Network Security – Data Breaches
by Julian Evans

40 Emerging Threats

What is Good Enough Coverage?
by Matthew Jonkman

BASICS

10 A Security System That Changed The World

by Yury Chemerkin

Enterprise data is a valuable corporate asset, and therefore ensuring it's over integrity is an issue of superior business cycle model to any commercial or government organization.

ATTACK

14 Get in Through the Backdoor: Post Exploitation with Armitage

by Raphael Mudge

IT professionals have a dated image of hacking. Many picture the process as running nmap, finding an exploit, and running it to compromise a server. This romantic scenario was alive around 2003, but it has since gone out of style.

18 Breaking The Code: Brute Forcing The Encryption Key

by Rich Hoggan

There's no way around it, cryptography is an aspect of our digital lives that's becoming more and more prevalent. It's because we interact in a vast social network that is the internet.

DEFENSE

22 Is Data Secure on the Password Protected Blackberry Device?

by Yury Chemerkin

People who have ever heard of password utility think the usage of it can protect their private data. There are, however, several ways to steal a lot of information in spite of the fact that device locked by password. These ideas are not complicated to first-time malware developer.

30 Examine your Network With Nmap. What is network Scanning?

by Mohsen Mostafa Jokar

Network scanning is an important part of network security that any system administrator must be comfortable with. Network scanning usually consists of a port scanner and vulnerability scanner.

CERTIFICATIONS

42 Exploring GCIH Certification for Fun and Employability

by Alexandre Teixeira

Do you remember the time when you used to read a lot of underground e-zines? How many years of professional experience do you have? These really count. Enhance your skill set by challenging this certification exam!

48 Certification Smart?

by Douglas Chick

A job in computers is a position of experience; if you don't have experience the next best thing is a computer certification.



eLearnSecurity
Forging security professionals



**Penetration testing course
Like CEH.
Only...One mile deep**

Interactive elearning system
1600 slides
4 hours videos
Hacking Labs on DVD
Reporting & Methodology
Certification



3 domains - 18 modules
Web Application Security
Network Security
System Security
Web 2.0 attacks
Vuln. Assessment
Writing Rootkits
Privilege escalation
Advanced Buffer Overflows

The fastest path to
Professional
Penetration Testing

www.elearnsecurity.com

STUXNET CREATORS NOT SO ELITE?

Everyone knows what Stuxnet is and if you don't you probably missed the most discussed and much praised worm of the past few years.

The worm targeting Siemens systems, controlling critical power infrastructures, has been subject of deep analysis by researchers to uncover who's behind it and who the final target was.

Both of the above questions had readily found an answer: at least according to the authoritative Times, it's been a joint effort between US and Israel governments, to destroy alleged Iranian projects to build a nuclear arsenal.

Although the goal has not been reached, Iranian path to having nuclear bombs has been set back by 2 years, as President Obama, although skirting the Stuxnet issue, stated in an interview regarding Iran.

The much hyped Stuxnet, dubbed as the most sophisticated worm ever, has also been subject of analysis of Tom Parker. Tom is a security researcher who has presented his own analysis and view of the Stuxnet case at BlackHat DC.

For the first time, someone states that Stuxnet worm is not so *elite* as everybody thought in the beginning and probably media played an important role in the matter.

Still according to Parker, *too many mistakes (have been) made* and too many logic flaws made things go wrong. Parker seconded the hypothesis according to which code was produced by two separate groups: one building the core of it and another, much less experienced, providing the exploits and the command and control code.

Another security expert, Nate Lawson, considers Stuxnet code nothing more elite than any other malware around, not even implementing advanced obfuscation techniques such as anti-debugging routines.

Source: Armanod Romeo,
www.elearnsecurity.com

ANOTHER (SERIOUS) MOBILE PHONE HACK: BASEBAND HACKING

If you thought this was another GSM hacking announcement you are wrong.

This is a completely new hacking vector, a new exploitation door opened by researcher Ralf-Philipp Weinmann.

Every smartphone has a multi-cpu architecture with an Application processor and a Baseband processor, both ARM CPU's and implemented in a single chip. While Application processors deal with the execution of the phone tasks, Baseband deals with the protocols *in the air*: GSM, UMTS...

According to Ralf, firmware code for the Baseband was created in 90s and there's almost no mitigation for

code execution beside hardware DEP implemented in iPhone 4. This makes exploitation possible, however no one until now took the time to reverse engineer the firmware binaries and uncover *many, many unchecked memory copies through `memcpy()`*.

The possibilities of running a payload on poorly coded phones Baseband firmware was also mitigated by the costs involved in having malicious BTS, base stations usually operated by carriers, required for the exploitation to take place.

The researcher, demoed a remote code execution against a mobile phone through \$1250 worth of equipment simulating a BTS through the OpenBTS code, an open source project on purpose.

A price that can be afforded by the majority of the criminals out there considering the potential outcome presumed by Weinmann: eavesdropping conversations, stealing corporate passwords, installing rootkits, propagating worms, bricking phones and so on.

Source: Armanod Romeo,
www.elearnsecurity.com

BLOGGER AND RESEARCHER DANCHEV DISAPPEARED IN BULGARIA

Famous ZDNet blogger Dancho Danchev is missing since August 2010 and no one seems to be able to contact him since October. The ZDNet ZeroDay blog co-author Ryan Naraine has made the news public in hope that someone might respond with hopefully good news about the disappearance.

One of the hypothesis are that Danchev, Bulgarian, was being spied by someone due to his researches in the cyber underground of his native country. Pictures of the spy-equipment found in his bathroom were taken by the blogger and handed to a trusted third party to be published in case something bad happened. The pictures are now online and serve, according to Danchev's letter, to demonstrate who was after him.

Although pictures are not clear about what kind of spy equipment that was, lack of news from the person and internet word of mouth are building a mythological spy story around the case.

Most recent news, from a Bulgarian newspaper, talks about Danchev being confined in a psychiatric hospital. All the news are fragmentary and not confirmed and as such should be treated.

Source: Armanod Romeo,
www.elearnsecurity.com

GOOGLE PAYING FOR HIGH RISK CHROME VULNERABILITIES

Google has managed to make private vulnerabilities disclosure a legal and even fun activity for researchers.

Full disclosure is well gone and nowadays companies are more and more willing to pay for responsibly disclosed vulnerabilities in their products. Google being among the very first.

The opportunity for vendors is huge: they can cut down the costs of out of band patches while having a bunch of researchers readily providing proof of concepts of vulnerabilities without having much bad press for exploits in the wild.

According to Google, more than \$14,000 have been paid until now to researchers who reported critical vulnerabilities in Google Chrome. Not a big amount at all if you consider the costs involved in consultancy, or in hiring a bunch of talented testers.

Sergey Glazunov, researcher who has found several critical vulnerabilities in Chrome, has received an *elite award* early this month: \$3133.7. More than just money: an *elite* bank account statement to show to all the friends.

Source: Armanod Romeo,
www.elearnsecurity.com

MICROSOFT IE8 EMET VULNERABILITY

ID Theft Protect is aware of a vulnerability affecting Microsoft Internet Explorer 8. This vulnerability is due to improper handling of circular memory references. Exploitation of this vulnerability may allow an attacker to execute arbitrary code in the context of the user or cause a denial-of-service condition.

At this time, the vendor has not released a fix or a workaround to address this vulnerability. Users and administrators are encouraged to consider implementing the mitigations provided in Microsoft's *Enhanced Mitigation Experience Toolkit* (EMET). These mitigations will not rectify the vulnerability but will make exploitation of the vulnerability more difficult.

Source: ID Theft Protect

OBAMA EYES INTERNET IDS FOR US CITIZENS

President Obama is planning to hand the U.S. Commerce Department authority over a forthcoming cybersecurity effort to create an Internet ID for Americans, a White House official said here today. It's *the absolute perfect spot in the U.S. government* to centralize efforts toward creating an *identity ecosystem* for the Internet, White House Cybersecurity Coordinator Howard Schmidt said. That news, first reported by CNET, effectively pushes the department to the forefront of the issue, beating out other potential candidates, including the National Security Agency and the Department of Homeland Security.

Source: ID Theft Protect

OHIO STATE UNIVERSITY DATA BREACH

During a *routine* IT security review in late October 2010, Ohio State University discovered that unauthorized people had logged onto a server that contained information on current and former faculty, students and staff, applicants, and others with university ties. That data included name, *Social Security number* (SSN), date of birth, and address. A forensic investigation led security experts to conclude that the access was set up to launch cyber attacks against other businesses on the Internet and that no records were actually taken.

Source: ID Theft Protect

RUSTOCK BOTNET IS BACK WITH A VENGEANCE

Spam levels have resumed after a precipitous drop in December, but without the innovations security specialists had feared might be imminent. In December, spam levels declined dramatically and continued at relatively minuscule levels from 25 December 2010 to 9 January 2011. The security community speculated that this might be because the criminal gangs behind the botnets and the spammers who are their clients were thinking up new schemes.

But spam levels bounced back overnight on 10 January with no sign of a change in tactics. An increase of about 98 per cent in volume has pushed spam back up to *normal* levels – some 90 per cent of all traffic. This was mostly down to the activity of Rustok, the world's biggest botnet, output from which plunged after a late splurge on 24 December. Security researchers say the decline and resumption of spam may be due to a temporary lack of clients for Rustok.

Source: ID Theft Protect

SMS SMISHING SCAM IDENTIFIED

A new security risk has crept into the world of online shopping, and it combines the trickery of phishing scams with the ease and availability of text messages. Called *smishing* the scam is a nefarious update to the traditional phishing hoax; rather than sending the phishing bait – a legitimate-looking offer from a supposedly trusted source such as a bank – through e-mail, the message is sent via SMS (text). The victim is told in the text that an urgent bank matter needs to be discussed; the text instructs the recipient to call a toll-free number and provide their account number and password to a fake automated voice-response system.

Source: ID Theft Protect

Wuala – Secure Online Storage

There are a lot of online storage/backup solutions available nowadays and it is hard to find differences between them, but I think Wuala from LACIE may have something unique in the way their solution works.

Trading

You start off with 1GB free and you can either purchase more space or *trade* up to gain more. By trade I mean you offer space from your machine for LACIE to store parts of other peoples files locally on your machine. How it works is quite simple actually, by multiplying your offered storage against the amount of time you are online will give you the extra online space so you aren't really losing the drive space, instead your gaining access to your files wherever you are.

You can offer upto 100GB and if your online 50% of the time, you would gain 50GB of online storage.

For every friend you invite and they sign up you will gain 250MB (free user) all the way upto 3GB. If you decided to become a pro user this bonuses then becomes 500MB and goes upto 6GB.

Data Security

By encrypting the data locally before its even transmitted up to the cloud storage not even the staff at LACIE will be able to view your files. Your files are split into multiple pieces and then stored in multiple places so that your data will never be lost. Even your password never leaves your computer. (I checked this claim by running wireshark whilst logging in and adding files to my storage, and I was unable to see any details referencing my passwords or data in any of the traffic capture)

Data

There are three types of sharing available to you.

- *Private* (where you and only you have access)
- *Shared* (where you have setup friends and or groups to be allowed access)
- *Public* (the whole world can see your files)

Sharing your data couldn't be easier, just a simple case of right mouse click and select share. Then you are presented with the option on how you wish to share, public or private. Finally you can decide to share via a weblink or even send your friends and family an email with the link included. If you had decided to share

your data publicly, then you are able to utilise all the social bookmarks from all your favourite sites that are included with the application.

Extra Features for Pro users

For those of you who decided to go for the Pro option, there are some excellent additions to your service.

Backup

By creating a folder where you can just drag and drop data onto and know it is automatically uploaded to Wuala for safekeeping is a great feature, and will give peace of mind to those who have a habit of *accidentally* deleting a file or folder. You can also setup scheduling on this folder so you will know everything in there will always be regularly backed up and kept safe. Don't forget as its a folder you can share this with anyone and everyone.

Sync

When you create a sync folder, every time you drag and drop something new into here it will appear on all your other machines where you are using Wuala, so this will be of great use to all those people who regularly use more than one machine on a day to day basis.

File Versioning

If your like me there will be times when you will name files the same name and then overwrite the wrong file at the wrong time. By having the file versioning you are able to literally skip backwards in time to access the file at an earlier time. Before you made the mistake in the first place.

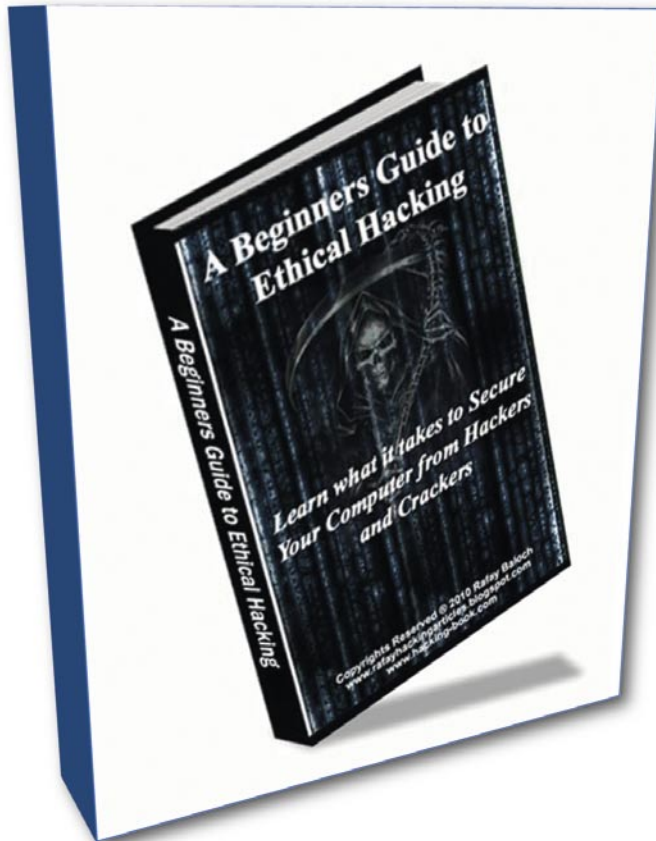
Conclusion

Considering that this is still in Beta, Wuala has some excellent strong features that make it a superb option to all us users out there that always need somewhere to safely store our pictures, videos and our documents. I was very grateful to test this product and will continue to use it long into the future.

URL: <http://www.wuala.com>

MICHAEL MUNT

A Beginners Guide to Ethical Hacking



URL: www.hacking-book.com
 Author: Rafay Baloch
 Cost: \$20

A Beginners Guide to Ethical Hacking is a great resource for people interested in ethical (white-hat) hacking. It is targeted at „beginners“, but some „intermediate“ users may find value in this book as well.

Some people think that there is nothing ethical about hacking – I think that there is nothing ethical about attacking, but hacking can almost always be done ethically. Hackers are thinkers who seek to determine their limitations through challenging their skills, and this book serves to educate readers about how they can challenge themselves in an ethical way.

The book starts by defining the ethical boundaries of hackers – what the cognoscenti considers *too far*. It then quickly jumps into the realm of programming and how code-writing can be leveraged to achieve the readers' goals. Some might argue that programming or reverse-engineering is *old school*, and the *new school* is all about root, but just like in school, you have to start with the *Introduction* to classes before you can move on to the *Advanced* ones. A solid foundation makes for a sturdy building. Programming doesn't mean learning a coding language from scratch, it

means finding the resources you need, when you need them. And this book does just that.

The author then moves on to hacking and cracking of passwords, Microsoft Windows OS, Wi-Fi, and websites. In the website section, the author details the web-application side of hacking, then covers malware and virii. This book not only helps you learn the hacking (or *offense*) side of information security, but also the anti-hacking (or *defense*, or *counter-measures*) side of the coin, detailed in the last chapter. By providing a good balance of both offense and defense, the reader is presented with the tools needed to make accurate and educated decisions regarding not only ethical hacking, but also how to properly secure themselves when doing business online.

Overall, I give this book a thumbs-up!

SHYAAM SUNDHAR

A Security System

That Changed The World

Enterprise data is a valuable corporate asset, and therefore ensuring it's over integrity is an issue of superior business cycle model to any commercial or government organization.

What you will learn...

- Design of BlackBerry Enterprise Solution
- Mobile malware tendency

What you should know...

- basic knowledge about networking
-

Security is the cornerstone of the BlackBerry legendary security system, allowing users to confidently access sensitive information at all times.

The BlackBerry devices, BlackBerry-enabled devices and supporting technology are developed by *Research In Motion* (RIM), a Canadian software and hardware company based in Waterloo, Ontario.

Special selling feature is that it provides an integrated wireless messaging system, providing push email access over cellular wireless networks throughout the world. Another major factor in the BlackBerry's popularity is its comprehensive approach to security. BlackBerry devices are diversified, and can be used for a various functions including such ordinary functions like telephony, SMS, MMS, email, photos, videos, music, and web-browsing amongst other things.

End-users are divided into two categories.

- End-user consumers who bought their own BlackBerry devices, who uses *BlackBerry Internet Service* (BIS)
- Enterprise end-users who are given the use of a BlackBerry by their employers with another service called *BlackBerry Enterprise Solution* (BES).

The first environment make an end-users are responsible for the any security measure configuration.

In opposition to BES environment where the end-users have an amount of control, but security is usually performed by the enterprise by an IT Policy. Here's a custom list of BES features, from RIM:

- Wirelessly synchronize their email, calendar, contacts, notes and tasks
- Manage email folders and search email on the mail server remotely
- Book meetings and appointments, check availability and forward calendar attachments
- Set an out-of-office reply
- Edit Microsoft Word, Excel and PowerPoint files using Documents To Go
- Access files stored on the company network
- Use mobile applications to access business systems behind the firewall

The following table identifies the features available with the BlackBerry Internet Service and the BlackBerry Enterprise Server.

BlackBerry smartphone applications include inherent virus protection and spyware protection that is designed to contain and prevent the spread of viruses and spyware to other applications. Application controls are available on BlackBerry smartphones that are running on a BlackBerry Enterprise Server or on the BlackBerry Internet Service. BlackBerry smartphone users can use the application controls on their BlackBerry smartphones to prevent the

installation of specific third-party applications and to limit the permissions of third-party applications.

BlackBerry Enterprise Solution

The BlackBerry Enterprise Solution (consisting of a BlackBerry smartphone, BlackBerry Device Software, BlackBerry Desktop Software, and the BlackBerry Enterprise Server) is designed to protect organization from data loss or alteration while a BlackBerry smartphone user is sending and receiving, reading and typing messages and accessing your organization's data over the wireless network using the BlackBerry smartphone. In other words solution is designed so that data remains encrypted at all points between the BlackBerry smartphone and the BlackBerry Enterprise Server. Only the BlackBerry Enterprise Server and the BlackBerry smartphone can access the data that they send between them, while third-parties, including service providers, cannot access potentially sensitive organization information in a decrypted format.

The BlackBerry Enterprise Solution is a flexible, IT-friendly solution that gives mobile users secure wireless access to their enterprise email and business-critical applications. The key elements of the BlackBerry Enterprise Solution architecture include:

- BlackBerry Enterprise Server – Robust software that acts as the centralized link between wireless devices, wireless networks and enterprise applications. The server integrates with enterprise messaging and collaboration systems to provide

mobile users with access to email, enterprise instant messaging and personal information management tools. All data between applications and BlackBerry smartphones flows centrally through the server. Learn more about BlackBerry integration with

- IBM Lotus Domino and IBM Lotus Sametime
- Microsoft Exchange and Microsoft Office Live Communications Server 2005
- Novell GroupWise and Novell GroupWise Messenger
- BlackBerry Smartphones – Integrated wireless voice and data devices that are optimized to work with the BlackBerry Enterprise Solution. They provide push-based access to email and data from enterprise applications and systems in addition to web, MMS, SMS and organizer applications. Learn more about BlackBerry smartphones
- Devices with BlackBerry Connect software (BlackBerry-enabled Devices) – Devices available from leading manufacturers that feature BlackBerry push delivery technology and connect to the BlackBerry Enterprise Server*.

While the BlackBerry technology has a comprehensive embedded security system at all levels it's still susceptible to a range of attacks. Attacks, in whatever types, will confer power to design devices are being backdoored allowing any data (especially confidential data) to be exported from various blackberry handhelds. By the way, it's being used to build covert channels for attackers, in spite of exploits are digitally signed or not. Also, the efficiency and success of such attacks

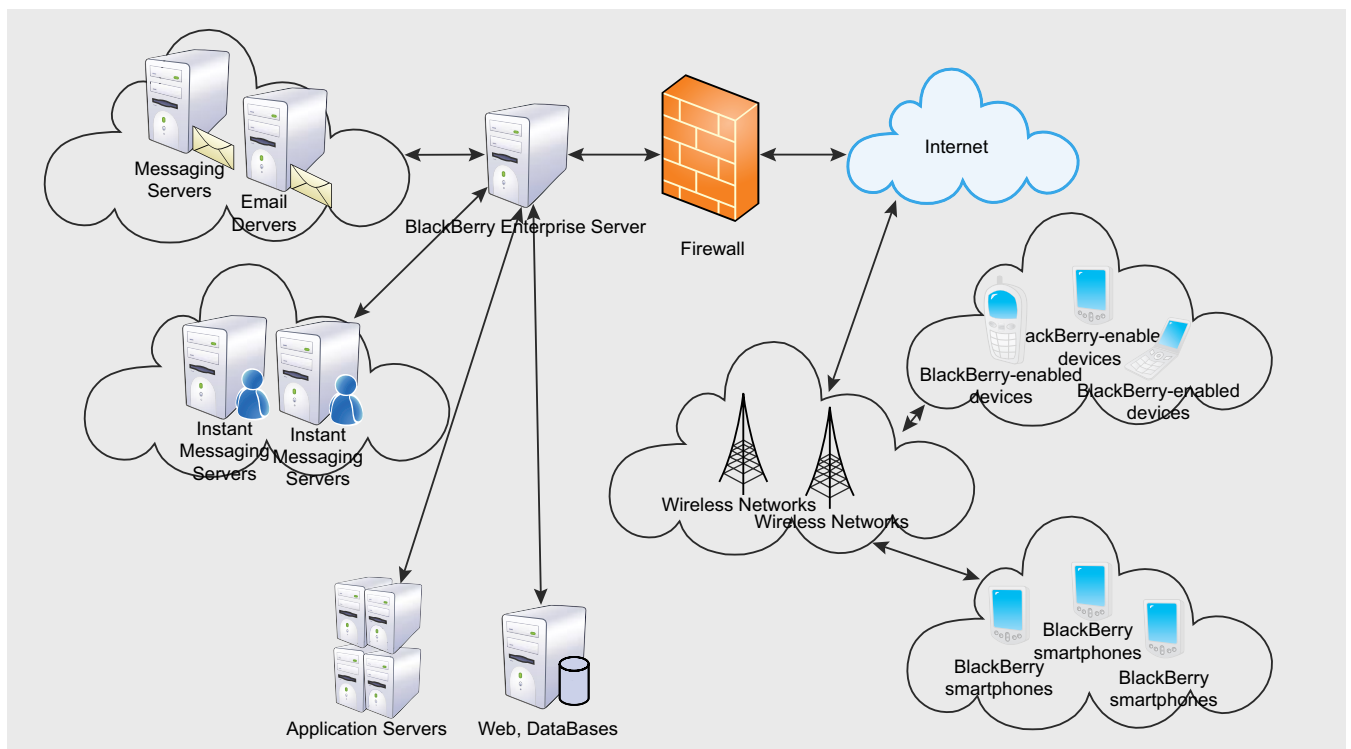


Figure 1. BlackBerry Enterprise Solution

On The 'Net

- http://docs.blackberry.com/en/admin/deliverables/12077/BlackBerry_Enterprise_Server_for_Microsoft_Exchange-Feature_and_Technical_Overview-T305802-817456-1102035401-001-5.0.1-US.pdf – BlackBerry Enterprise Server for Microsoft Exchange. Version: 5.0. Feature and Technical Overview, RIM,
- http://docs.blackberry.com/en/admin/deliverables/12035/Security_Technical_Overview.pdf – BlackBerry Enterprise Solution Version: 5.0. Security Technical Overview, RIM,
- [http://www.comscore.com/Press_Events/Press_Releases/2010/2/comScore_Reports_December_2009_U.S._Mobile_Subscriber_Market_Share/\(language\)/eng-US](http://www.comscore.com/Press_Events/Press_Releases/2010/2/comScore_Reports_December_2009_U.S._Mobile_Subscriber_Market_Share/(language)/eng-US) – December 2010 U.S. Mobile Subscriber Market Share, comScore, 2010,
- [http://www.comscore.com/Press_Events/Press_Releases/2010/3/comScore_Reports_January_2010_U.S._Mobile_Subscriber_Market_Share/\(language\)/eng-US](http://www.comscore.com/Press_Events/Press_Releases/2010/3/comScore_Reports_January_2010_U.S._Mobile_Subscriber_Market_Share/(language)/eng-US) – January 2010 U.S. Mobile Subscriber Market Share, comScore, 2010,
- [http://www.comscore.com/Press_Events/Press_Releases/2010/4/comScore_Reports_February_2010_U.S._Mobile_Subscriber_Market_Share/\(language\)/eng-US](http://www.comscore.com/Press_Events/Press_Releases/2010/4/comScore_Reports_February_2010_U.S._Mobile_Subscriber_Market_Share/(language)/eng-US) – February 2010 U.S. Mobile Subscriber Market Share, comScore, 2010,
- http://www.comscore.com/Press_Events/Press_Releases/2010/9/comScore_Reports_July_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports July 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/11/comScore_Reports_September_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports September 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/10/comScore_Reports_August_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports August 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/12/comScore_Reports_October_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports October 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/6/comScore_Reports_April_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports April 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/9/comScore_Reports_July_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports July 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/7/comScore_Reports_May_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports May 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/3/comScore_Reports_January_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports January 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/4/comScore_Reports_February_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports February 2010 U.S. Mobile Subscriber Market Share
- http://www.comscore.com/Press_Events/Press_Releases/2010/5/comScore_Reports_March_2010_U.S._Mobile_Subscriber_Market_Share – comScore Reports March 2010 U.S. Mobile Subscriber Market Share

depends on the configuration of existing security controls, i.e. Firewall and IT Policy rules (see Figure 1).

Malware development background

The development of mobile together with wireless technologies has evidently improved the way

everybody communicates with each other during the past several years. The growing use of it has made a good background for re-engineering range of malwares that identical to PC-malware types, like viruses, worms, trojans, backdoors, and adwares. There were major factors requisite for attack on the

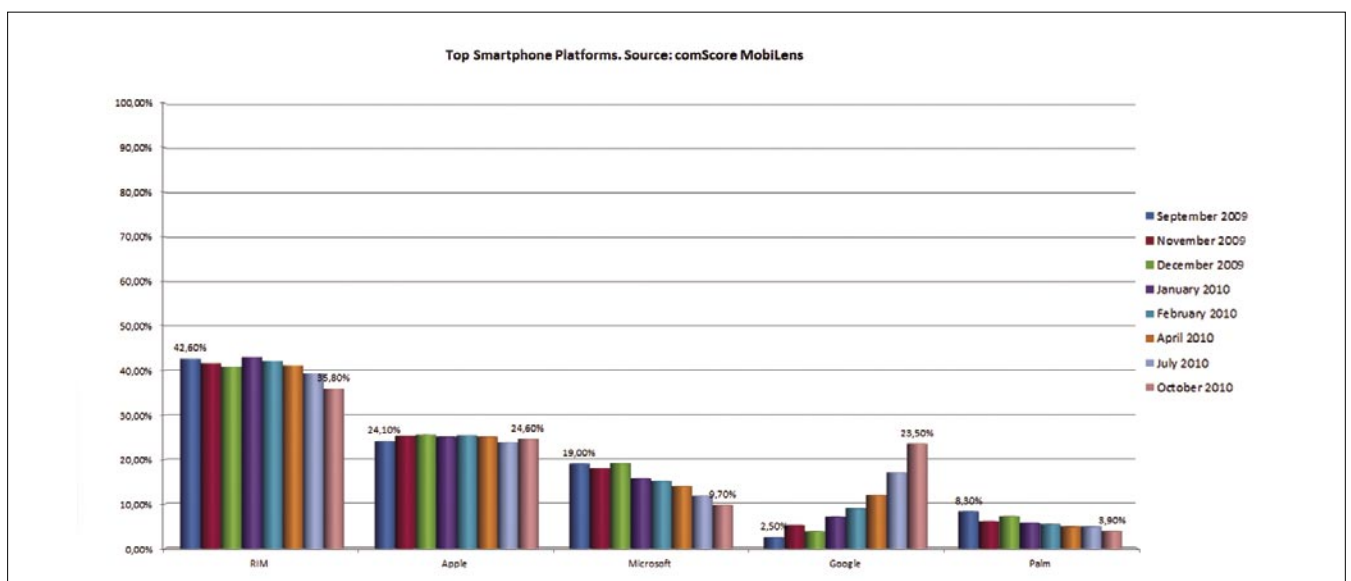


Figure 2. ComScore market trend analysis (09.2009 – 10.2010)

Table 1. comScore market trend analysis (09.2009 – 10.2010)

Producer	September 2009	November 2009	December 2009	January 2010	February 2010	April 2010	July 2010	October 2010
RIM	42,60%	41,60%	40,80%	43,00%	42,10%	41,10%	39,30%	35,80%
Apple	24,10%	25,30%	25,50%	25,10%	25,40%	25,10%	23,80%	24,60%
Microsoft	19,00%	18,00%	19,10%	15,70%	15,10%	14,00%	11,80%	9,70%
Google	2,50%	5,20%	3,80%	7,10%	9,00%	12,00%	17,00%	23,50%
Palm	8,30%	6,10%	7,20%	5,70%	5,40%	4,90%	4,90%	3,90%

smartphone. However, it didn't happen. This was due to the rapid changing situation on the mobile handset market. In spite of Symbian was leading for two years smartphone producers could shift industry-leading Nokia in favour of Windows Mobile (Microsoft) and BlackBerry (RIM).

Faced with the lack of a market leader in mobile operating systems and as a consequence, the impossibility of a simultaneous attack on the majority of users, malware writers had to try to solve the problem of *cross-platform*. Solution was the use of Java Micro Edition. It's the well-known fact that almost all modern phones have Java support and allow you to run Java-based applications that can be easily downloaded from the Internet. Java-based malware made significant contribution in damage area increasing by involving not only smartphones users, but also almost every owner of a mobile phone.

Exemplary malware to do list of realizable actions is below:

- Spreading via Bluetooth and MMS,
- Sending SMS, MMS,
- Making backdoor background,
- Blocking antivirus actions,
- Stealing confidential information, etc.

Displaced Nokia surrendered the initiative to the RIM, Apple and Google. According to comScore market trend analysis RIM is in lead (see Table 1).

Because of security is the cornerstone of the BlackBerry legendary security system most of consumers prefer BlackBerry smartphones to another like iPhone or Android. cursory acquaintance with the BlackBerry Solution shows us various products and components that are designed to extend organization's communication methods to BlackBerry devices. The BlackBerry Solution is designed to help protect data that is in transit at all points between a device and the BlackBerry Server. To help it devices use symmetric key cryptography to encrypt the data sent between them. Solution uses confidentiality, integrity, and authenticity, which are principles for information security, to help protect your organization from data loss or alteration.

YURY CHERMERKIN

Graduated at Russian State University for the Humanities (<http://rggu.com/>) in 2010. At present postgraduate at RSUH.

Security Analyst since 2009 and currently works as mobile security researcher in Moscow.

E-mail: yury.chemerkin@gmail.com.

Facebook: <http://www.facebook.com/people/Yury-Chemerkin/100001827345335>.

a d v e r t i s e m e n t



HAKIN9

**Subscribe to our newsletter
and stay up to date with all
news from Hakin9 magazine!**

<http://hakin9.org/newsletter>

Get in through the backdoor:

Post exploitation with Armitage

IT professionals have a dated image of hacking. Many picture the process as running nmap, finding an exploit, and running it to compromise a server.

What you will learn...

- How to attack a network without a memory-corruption exploit
- Tricks to seize internal hosts and keep your network access
- Ways to use the powerful Armitage user interface with Metasploit

What you should know...

- Basic Metasploit use

This romantic scenario was alive around 2003, but it has since gone out of style. Patch management, secure software development, and other good practices have changed the game. Rather than attacking services, the easiest way in to a network is usually through the users.

Using Armitage [1], this article will show you tactics used to break the security of modern organizations. You'll learn how to bypass the perimeter defenses through a social engineering attack. We'll then cover how to use this foothold to pivot through the network and take over more hosts. More over, we will not use a

single memory corruption exploit. Does this sound like fun? Keep reading.

Armitage

Armitage is a new interface for Metasploit [2]. Metasploit, as you know, is the popular open source exploitation framework. Metasploit provides tight integration between scanners, evasion techniques, exploits, and payloads.

One of the most powerful Metasploit payloads is Meterpreter. Meterpreter provides post-exploitation capabilities to you. With Meterpreter: you can work with files, route connections through the current host, and dump password hashes. Meterpreter is just a payload

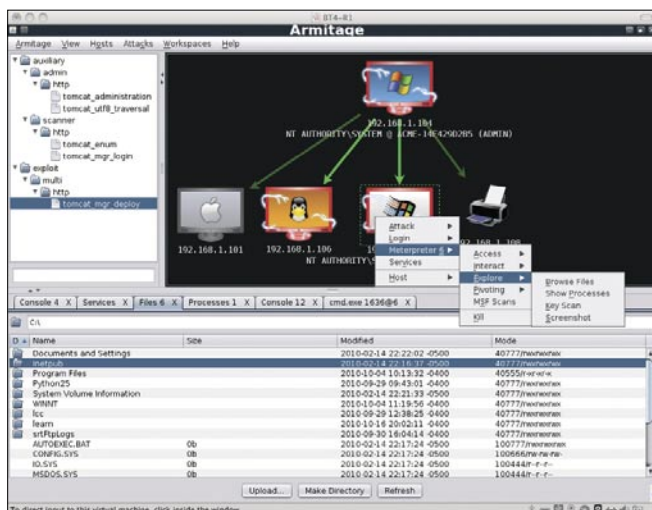


Figure 1. Armitage User Interface

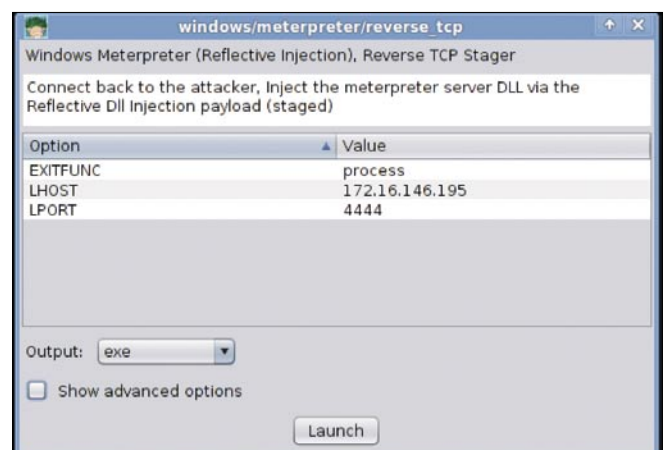


Figure 2. Payload Generation Dialog

though. You need to use an exploit (or clever social engineering) to get it on to a host.

Armitage is organized around the attack process. You can import hosts or scan targets through the hosts menu. You can use the *Attacks->Find Attacks* menu to get intelligent exploit recommendations based on scan data. This article won't use exploits, but know that this functionality is there. You need to know what you can do next after you get access. Armitage helps you by providing a user-interface to Meterpreter. We'll cover post-exploitation through Armitage in the rest of this article (see Figure 1).

Figure 1 shows the Armitage user interface. The top left is the module browser. Through the module browser you can access Metasploit's payloads, exploits, and auxiliary modules. The top right is the target area. Armitage displays the current hosts and any sessions you have in the target area. A compromised host appears red with lightning bolts surrounding it. The bottom is the tabs area. Armitage opens each console, browser and dialog in its own tab.

Create a Payload

Exploits are not always reliable. Why use one when your target will run your post-exploitation program for you. Let's use Armitage to create an executable of Meterpreter.

Navigate to `payloads/windows/meterpreter/reverse_tcp` in the module browser and double click it. Figure 2 shows the dialog that you will see. Double click a value to edit it. The LPORT value is the port your executable will communicate back to. Change it to something common, like 80. Select exe for the output type and click launch. Armitage will ask you where to save the executable. I like `backdoor.exe`.

You now have a post-exploitation program that will connect to your attack computer on port 80 when run (see Figure 2.).

If you run your program now, it will try to connect to your attack computer, fail, and close. It fails because your attack computer is not listening for a connection. Go to *Armitage->Listeners->Reverse Listeners*. Type in the port number (e.g., 80) and click Listen. Your attack computer is ready to receive connection attempts from your backdoor program.

To get access to your target you will need to convince a target to run your program.

You can provide your targets with your executable as-is. Sometimes this is enough. However, users may become suspicious when the program you provide seemingly does nothing when run. If you care about being stealthy, you may want to add Meterpreter to another program.

Create a Backdoor

One technique to combine two programs is to use IExpress 2.0 from Microsoft. IExpress 2.0 combines multiple programs into a self-extracting and self-running executable. The combined programs silently run in sequence. Figure 3 shows IExpress 2.0 after you first run it. Part of hacking is repurposing legitimate functionality for your nefarious purposes. This is a great example of that.

You can abuse this tool to add Meterpreter to any program you choose. I first read about this technique on Mubix's blog [3] (see Figure 3).

To run IExpress 2.0, go to *Start->Run in Windows*, and type: `iexpress`. Answer the questions it asks and you will have a combined program, ready to run. The program output by IExpress 2.0 has its own icon. Use the IcoFx [4] icon editor to replace this icon with the icon from the original program. Tape's blog [5] discusses how to do this.

Post Exploitation

Get your victim to run your backdoored executable. If everything works correctly you will see a red computer surrounded, as in Figure 4, by lightning bolts in the target area of Armitage.

Right-click this compromised computer and navigate to the Meterpreter menu. Each Meterpreter session will



Figure 3. IExpress 2.0 from Microsoft (thanks guys!)

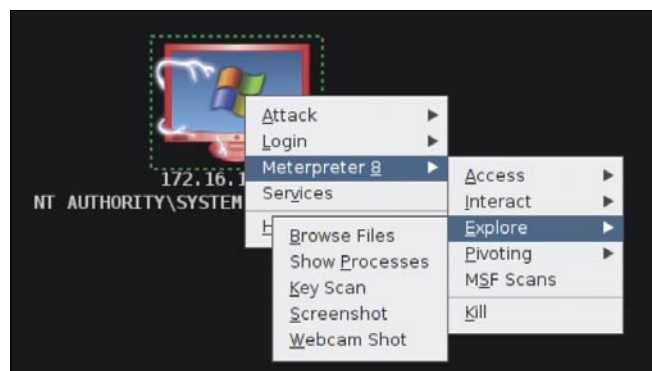


Figure 4. Ownership Achieved

have its own menu item. The access menu is where you will dump hashes, escalate privileges, and duplicate your access.

If possible, I recommend using this duplicate option. Armitage will upload and execute another Meterpreter instance so you have two sessions. If something happens to one of your sessions, you will still have access.

Use the interact menu to open a Windows command shell or a Meterpreter shell. Use explore to access the local system. Here you can browse the file system, view a process list, start a key logger, take a screenshot, or even take a picture with any built-in camera. Armitage adds extra features to what Meterpreter already offers. For example, the webcam and screenshot can automatically refresh every 10 seconds, if you choose to activate this option.

Here we've covered some of your system level post exploitation options. Your next two concerns are compromising more hosts and persisting your access.

Pivoting

You need internal network access before you can compromise other internal hosts. Metasploit has a powerful feature, called pivoting, that lets you tunnel traffic through an active Meterpreter session. To set up pivoting: right-click a compromised host, go to *Meterpreter 1->Pivoting->Add Pivot*. A dialog similar to Figure 5 will appear. Select a local network from this dialog. Armitage will tell Metasploit to route all traffic destined for that host through the existing meterpreter session. As you discover hosts, Armitage will draw a line from the pivot host to hosts that match this pivot you created.

Metasploit also includes a SOCKS proxy server. Any tools that you configure to use this proxy server will have their traffic routed based on the pivots you've set up. The Metasploit proxy server module allows you to use your web browser to browse other hosts

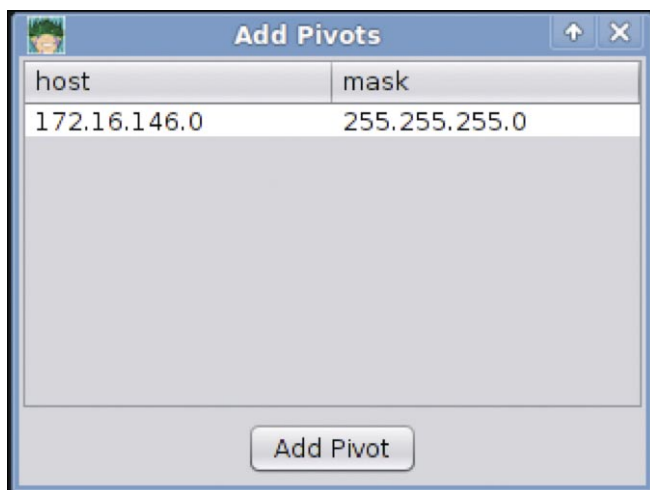


Figure 5. Set up pivoting

on the network you've compromised. Go to *Armitage->SOCKS Proxy* and click Launch to activate the proxy server.

Discovery Scans

Now you have access the internal network of your victim. You should scan and see what is there. Metasploit has many auxiliary modules to identify services and fingerprint hosts. Go to *Hosts->MSF Scans* and enter the address of the network you want to scan. Armitage will launch 19 discovery modules and record its findings in the Metasploit database. New hosts will show up in the target area as they're discovered. These scans will take advantage of the pivoting you have set up (see Figure 6).

Attack: Pass the Hash

Now that you have discovered hosts on the internal network, it's time to attack them. When you login to a Windows host, your password is hashed and compared to a stored hash of your password. When they match, you're able to login. When you attempt to access a resource on the same Windows domain, this stored hash is sent to the other host and used to authenticate you. You can use captured hashes to authenticate to other hosts on the same Windows domain. This is a pass-the-hash attack.

You need administrative privileges to dump hashes on a Windows host. To escalate privileges in Armitage, right-click the compromised host, and go to *Meterpreter N->Access->Escalate Privileges*. Metasploit will try several Windows privilege escalation techniques. A dialog will tell you the process succeeded or failed.

Right-click the compromised host, go to *Meterpreter N->Access->Dump Hashes*. Meterpreter will dump the password hashes and store them in Metasploit's credentials database. Go to *View->Credentials* to see the contents of this database.

Click *Attacks->Find Attacks->by port* and wait. A dialog will tell you the attack analysis is complete. The discovery

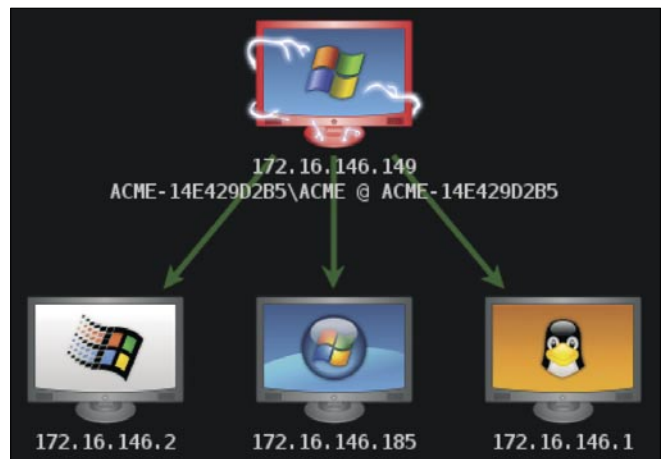


Figure 6. Host discovery with pivoting

scans you executed gave Metasploit and Armitage information used to recommend these attacks.

Right-click a Windows host and go to *Attack->smb->pass the hash*. Select a username and password (or hash) to login to that host with (see Figure 7). Highlight several hosts to try this attack on all of them. You will see the iconic red computer with lightning bolts if your attack is successful.

Attack: Launching an Exploit

If you do not get administrative privileges on your first host, all is not lost. Look for a Windows XP host or Windows Server 2003 among your targets. There are usually a few of these hosts on a large network.

Highlight these Windows hosts in the target area. Search for `ms08_067` in the module browser. Double click the module name and click launch. If this exploit is successful, you'll have administrative access to the host. This will allow you to follow the pass-the-hash steps to access the patched hosts. I said we wouldn't use exploits in this article. My apologies, I couldn't help myself.

Persistence

Now that you've compromised the network and gained access to more hosts, it's time to persist your access. Persistence assures your access to the network in the future. If you're evil, you will persist on a host other than your initial access host. This will make it harder to discover how you're getting back into the network.

Let's persist your access using a backdoor. Right-click a compromised host and select *Meterpreter N->*



Figure 7. Pass the Hash

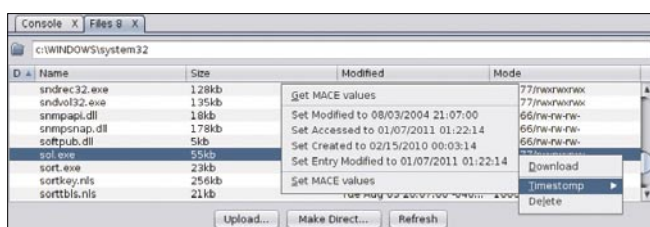


Figure 8. The File Browser

On The 'Net

- Armitage Project, <http://www.fastandeasyhacking.com/>
- Metasploit Project, <http://www.metasploit.com/>
- Metasploit Heart's Microsoft. <http://www.room362.com/blog/2009/3/2/metasploit-hearts-microsoft.html>.
- lcoFX, <http://icofx.ro>
- Creating an executable with Metasploit and gaining access to target PC. <http://adaywithtape.blogspot.com/2010/05/creating-backdoored-exe-with-metasploit.html>

Explore->Browse Files. You will now see a tab, similar to Figure 8, that lets you navigate the local file system, upload files, and download files.

Navigate to an executable that the user is likely to use. Right-click the executable and select Download to save it locally. Use IExpress 2.0 to add your Meterpreter executable to the downloaded program.

In the file browser, right-click the program you want to replace and select *Timestomp->Get MACE* values. This will save the file's current access, modified, and creation times to Armitage. Right-click the program and choose Delete to delete the file. Now use the Upload button to upload your backdoored version of the program. Right-click the uploaded file and select *Timestomp->Set MACE* values. This will set the access, modified, and creation time values of the file to what you saved a moment ago.

You have now replaced the original program with a backdoored version and updated the time/date information to match the original file. To the user, the program will function as normal. When they close it, they will give you a connection to their machine through your backdoor.

Conclusion

This article explored the hacking process without exploits. You saw how to get a foothold in a network with a social engineering attack. From there, you set up a pivot and executed the attack process anew. You discovered hosts, executed a pass-the hash attack, and established persistent access to the network. Armitage provided you an interface organized around these tasks.

I recommend staging target virtual machines and trying these techniques on your own. Reproduce the steps from this article to gain a greater awareness of how attackers think. It is my hope that you will reflect on your defensive posture and develop ideas to improve it. Good luck and happy hacking.

RAPHAEL MUDGE

Raphael is a Washington, DC based security engineer. He is also the developer of Armitage. You may contact him at <http://www.hick.org/~raffi/>

Breaking The Code:

Brute Forcing The Encryption Key

There's no way around it, cryptography is an aspect of our digital lives that's becoming more and more prevalent.

What you will learn...

- Basic encryption
- The process of breaking encryption using software

What you should know...

- Basic knowledge of C++

It's because we interact in a vast social network that is the internet where we enter our personal information into countless profile pages and make the majority of our purchases online that we have an increasing need to focus on cyber security and cryptography. But at the same time that cryptography has great potential in securing our information, it's just as vulnerable to attack.

In order to illustrate the points set forth by the author, we will be focusing on a single encryption cipher – the simple-substitution cipher. We will demonstrate software implemented for the purposes of encrypting, decrypting, but also breaking such encryption. As a result, the knowledge imparted through this article can and should be used as a stepping stone towards *re-thinking* cryptography and how we use it to secure information.

Cipher Basics

The simple substitution cipher – generally considered weak encryption – was known for offering a relatively

$$X = (O + K)$$

where:

X is the encrypted letter
O is the original letter
K is the encryption key

Figure 1. Calculating Cipher Text

secure means of hiding information back when it was first introduced. This style of encryption worked by – as it's name states – shifting the clear text a certain number of positions right or left of the original character. We refer to this shift value as the encryption key. For example, the letter A shifted four spaces to the right gives us the letter E. Using this method, we could shift all the letters of the English alphabet four spaces to create what's called a cipher alphabet. This cipher alphabet could then be used to encrypt longer pieces of information.

We will be using a variant of the simple-substitution cipher in that we don't limit the encryption key to 25 (because we start counting from 0 in C++) but rather allow the shift to occur past the 26th letter of the alphabet. This will become clearer as the encryption and decryption algorithms are explained in the following section. Within a computer, each character is referenced by a number, this number is referred to as the character's ASCII value. To encrypt each character we need to use its ASCII value so we

$$69 \text{ or } E = (A + 4) \text{ or } (65 + 4)$$

where:

E is the encrypted letter
A is the original letter
4 is the encryption key

Figure 2. Calculating Cipher Text in Practice

$$X = (E - K)$$

where:

X is the original letter
 E is the encrypted letter
 K is the encryption key

Figure 3. Calculating Clear Text

know from where in the alphabet the shift needs to occur. So to look at our previous example, the ASCII value of A is 65 and when shifted 4 spaces becomes 69 or E; Figures 1 and 2 demonstrate this more mathematically.

The decryption process is exactly the same as encryption except we subtract the encryption key from the encrypted character's ASCII value in order to recover the original text. This can be seen more clearly in Figures 3 and 4.

Understanding the Algorithms

It's time to put our theory into practice, Listing 1 shows the encryption algorithm we wrote for the demonstration software. In order to encrypt the clear text we need to loop through the entire string and process each character one by one. The for loop starts by grabbing the first character of the clear text, converting to its ASCII value and shifting to the value of the encryption key. Once the character has been shifted, the encrypted value is then converted back to a character and concatenated to a string variable that will store the encrypted text.

The algorithm continues to execute until the end of the clear text at which point the loop exits and we are left with the encrypted text printed to the screen. As previously mentioned, the decryption algorithm works just like its encryption counterpart except everything is reversed. Instead we loop over the encrypted text and subtract the encryption key from the encrypted character's ASCII value to once again recover the clear text, much like we saw in the previous section. The decryption algorithm is documented in Listing 2.

Following is a sample run of the encryption and decryption algorithms. Listing 3 shows how the message *the quick brown dog* gets encrypted and Listing 4, the decryption. Taking a closer look at the encrypted text we see that the word length is not reflected or is more difficult to visualize when encrypted as opposed to when looking at normal English. Consider this example from a more cryptanalytic perspective for a moment. If this were the only text we had to work with, a red flag already has to be raised. Because there are multiple instances of the dollar sign in the encrypted text, we can assume that this character represents a letter in the original text or another widely used character. But just by looking at the ratio of the dollar sign to the other encrypted characters, we know that it doesn't represent

$$65 \text{ or } A = (E - 4) \text{ or } (69 - 4)$$

where:

A is the original letter
 E is the encrypted letter
 4 is the encryption key

Figure 4. Calculating Clear Text in Practice

a letter, mainly because the dollar sign's ASCII value is greater than any of the `A` to `Z` or `a` to `z` characters. Knowing this, it's a safe bet to assume that the dollar sign represents a space. And subsequently, we can now gain a better idea of where the word lengths occur in the example. While we have now entered into the realm of frequency analysis, it's good to point these things out as the simple-substitution cipher wears its flaws for public display.

Algorithmic Attacks

Our previous discussions have centered around the fact that we knew the encryption key. Most likely, that

Listing 1. Encryption Algorithm

```
for (int i = 0; i <= clearText.length; i++)
{
    currentChar = clearText[i];
    currentInt = int(currentChar);
    encryptedInt = currentInt + encryptionKey;
    encryptedChar = char(encryptedInt);
    encryptedText += encryptedChar;
}
```

Listing 2. Decryption Algorithm

```
for (int i = 0; i <= encryptedText.length; i++)
{
    currentChar = encryptedText[i];
    currentInt = int(currentChar);
    clearInt = currentInt - encryptionKey;
    clearChar = char(clearInt);
    cleartext += clearChar;
}
```

Listing 3. Encrypting A Message

```
Original Message: the quick brown dog
Decrypted Message: xli$uymgo$fvs[r$hrk
```

Listing 4. Decrypting A Message

```
Decrypted Message: xli$uymgo$fvs[r$hrk
Original Message: the quick brown dog
```

will not be the case and we will only have the encrypted message to work with.

When this is the case, there are a couple of attacks we can use. One – and the most widely used – is frequency analysis as we previously alluded to, the other is brute force. Now while it's not our goal to discuss how to use frequency analysis to break encryption, the process basically requires that we find the frequency of the characters used in the encrypted text along with the characters used in the clear text's language – this is usually English.

The second attack and the one we are going to learn how to use is brute force. In regard to the simple-substitution cipher, brute forcing simply involves using a range of numbers to test which one if any is the encryption key. We do this process until the encryption key is found and/or we are able to decipher the encrypted message. The brute forcing algorithm is described in Listing 5.

Much like the algorithms we previously looked at, this algorithm also loops over the encrypted text only instead of using a known encryption key, the algorithm takes a number from the user to use as a range starting from 0.

You'll also notice that we are also using a set of loops in this algorithm as opposed to before where we only needed one. Reason being, the outer loop is giving us the potential encryption key while the inner loop is using the potential encryption key on the encrypted text. Once execution reaches the inner loop, it works much like our decryption algorithm in that we are still processing character by character but

the difference is that we are storing each potentially decrypted message in a string array. Lastly the outer loop prints out each index of the string array to the console window for viewing.

Listing 6 shows a sample run using the same example as before. The list format makes it easier to determine which index contains the decrypted message.

If on running the program, the range of numbers does not turn up the decrypted text, simply increase the number previously entered and re-run the program. This process can be repeated as often as needed until the deciphered message is displayed in the list. It's by writing such software that we don't have to concern ourselves with trying each number on it's own and can more easily break the encryption.

So What?

Why care about anything we just talked about? Similarly, it's also apparent that in order to demonstrate the process of breaking encryption, we used an obviously outdated algorithm. The point to all this though is the fact that software can be written as a tool for use in cryptanalysis and ultimately the breaking of encryption. Once a software tool is written that is capable of breaking encryption, the amount of time it would theoretically require to break the cipher leaves little in the way of an acceptable deterrent. This is the case because the rise of bot nets and super-computers substantially raises the potential processing power one has to work with and as a result, the greater the processing power, the smaller the amount of time to break the encryption.

So where are we to look to find a solution to the problem? Because we face a cyclical cycle of constantly developing newer technologies to secure information, there is no clear cut solution. As we push forward into the future of information security, it's best that we do away with the oldest of encryption algorithms – merely to keep them around for theoretical purposes – and focus on those that yield the best possible strength for the current security conditions. Finally, we must not forget that the truest sense of security comes down to our treatment of the encryption key. For the advancement of cryptography is inevitable but the person in control of the keys to such systems is not.

Listing 5: Brute forcing algorithm

```
for (int i = minRange; i <= encryptedText.length; i++)
{
    for each (char currentChar in encryptedText)
    {
        currentASCII = int(currentChar);
        clearASCII = currentASCII - i;
        clearChar = char(clearASCII);
        clearText += clearChar;
    }

    cout << clearText << endl;
}
```

Listing 6: Brute forcing in action

```
uif!rvjdl!cspxo!eph
the quick brown dog
sgd#pthbj#aqnv#cnf
```

RICH HOGGAN

Rich Hoggan is currently pursuing a bachelors degree in Computer Science and plans on specializing in information and cyber security. In his spare time, Rich enjoys writing music, photography, and creating visual art with the Processing programming language.



UAT's coveted Bachelor of Science degree in Network Security is a vital national resource

One of the most prestigious Network Security programs in the country

We will teach you the concepts of security by design, and layered security to protect against exploitation of networks and data

UAT has been designated as a Center for Academic Excellence in Information Systems Security Education by the US National Security Agency

THEY SELDOM SMILE AT THE NSA. CAN YOU MAKE THEM GRIN?

Learn how to synthesize and apply these vital skills and leadership ability to succeed in the fast moving field of Network Security.

- Bachelor of Science**
 - Network Engineering
 - Network Security
 - Technology Forensics
- Master of Science**
 - Information Assurance

Program accreditations, affiliations and certifications:



⚠ CLUSTERGEEK WITH CAUTION

LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREE STUDENTS: Advancing Computer Science, Artificial Life Programming, Digital Media, Digital Video, Enterprise Software Development, Game Art and Animation, Game Design, Game Programming, Human-Computer Interaction, Open Source Technologies, Robotics and Embedded Systems, Serious Game and Simulation, Strategic Technology Development, Technology Product Design, Technology Studies, Virtual Modeling and Design, Web and Social Media Technologies

Prepare to Defend!

www.uat.edu

877.828.4335



Is Data Secure on the

Password Protected Blackberry Device?

People who have ever heard of password utility think the usage of it can protect their private data. There are, however, several ways to steal a lot of information in spite of the fact that device locked by password. These ideas are not complicated to first-time malware developer.

What you will learn...

- Noise typing can bring functional disorder
- Screen capture can make the security system pointless
- Your typing is vulnerability for the password

What you should know...

- basic knowledge about BlackBerry security

How many times have you found them in a situation that typing a complicated password you were confused, lost your train of thought and forgot on what character are you staying? And what did you do? Erased already entered 14 or 20 characters, and re-typed for a new, right? Why? Because your password hidden behind asterisks. And whether they should have?

Historically, password behind asterisks could be help to protect it from bystanders' villain who doesn't mind to steal password. So, doesn't villain know another way to steal it by key-loggers, phishing pages or trojans? More importantly, there's usually nobody looking over your shoulder when you log in to a website. It's just you, sitting all alone in your office, suffering reduced usability to protect against a non-issue.

Password masking has proven to be a particularly nasty usability problem in using mobile devices, where typing is difficult and typos are common.

Did you know?

Usability suffers when users' type in passwords and the only feedback they get is a row of bullets. Typically, masking passwords doesn't even increase security, but it does cost your business due to login failures. Providing visualizing the system status have always been among the most basic usability principles. Showing asterisks while users enter complex codes definitely fails to comply.

Keystroke emulation

Have you ever thought about touchscreen devices as a vulnerable touch technology? The underlying principle of direct interaction with screen is just emulation keystroke.

Most modern smartphones have this feature because it enhanced ways that devices to communicate to each other.

A touchscreen is an electronic visual display that can detect the presence and location of a touch within the display area. The term generally refers to touching

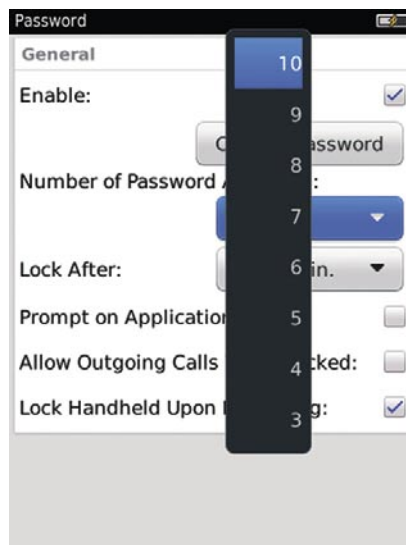


Figure 1. Password attempt quantity



Figure 2. State before unlocking

the display of the device with a finger or hand. Touchscreens can also sense other passive objects, such as a stylus.

The touchscreen has two main attributes. First, it enables one to interact directly with what is displayed, rather than indirectly with a cursor controlled by a mouse or touchpad. Secondly, it lets one do so without requiring any intermediate device that would need to be held in the hand. Such displays can be attached to computers, or to networks as terminals. They also play a prominent role in the design of digital appliances such as the *personal digital assistant* (PDA), satellite navigation devices, mobile phones, and video games.

A keystroke emulator duplicates (provides an emulation of) the functions of typing or input letters using a different system, so that the second system behaves like the first system. This focus on exact reproduction of external behavior is in contrast to some other forms

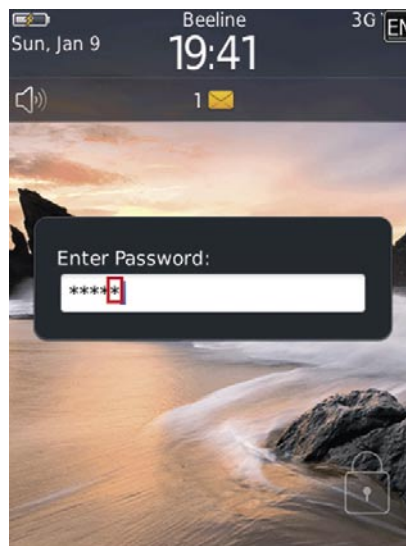


Figure 4. Noise input

of computer simulation, which can concern an abstract model of the system being simulated. Example, we are typing message *Hi, how's going...* via pressing hardware keyboard buttons and typing the same text via touching virtual keyboard buttons displayed on the screen. Outcome is the same.

Unsecure for the future

All smartphones give their owners a free choice to lock handheld by password or grant *unsecured* access. Password Strength is range of 8 up to 14-18 symbols with case-sensitive (Figure 1). The major concept in using the most complex password is main idea when you're reading BlackBerry Smartphone tutorial. You're obliged to lock your devices! You're obliged to use more complex combination! It's obliged to be randomness! But think for moment. Can you quickly say how many symbols are entered up? *No* is correct answer.

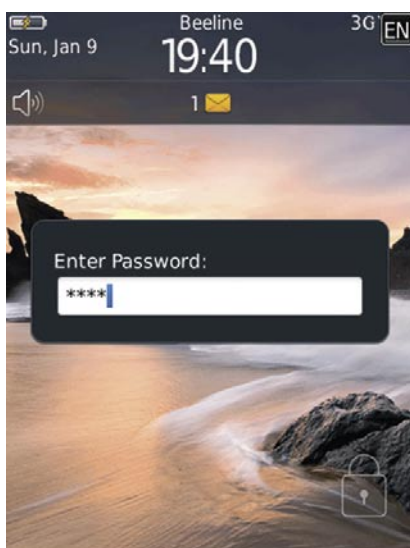


Figure 3. Typing correct password

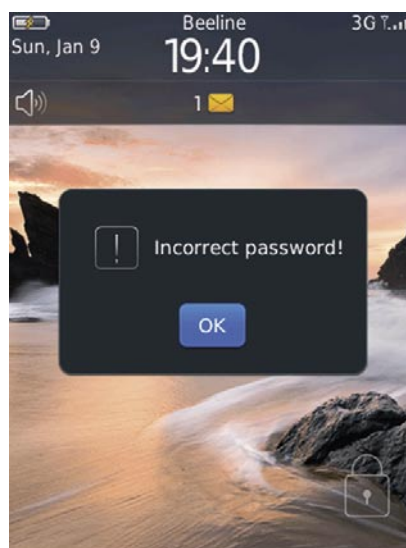


Figure 5. Error password notification

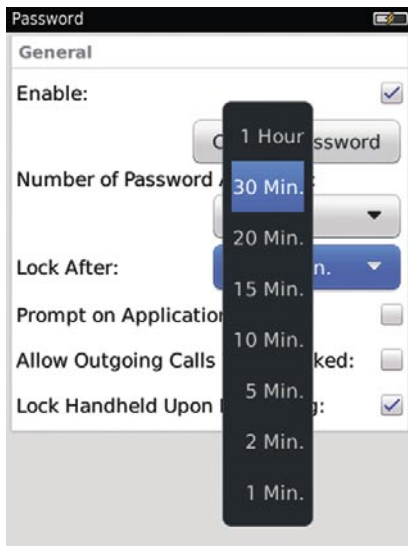


Figure 6. Device locking time span

Rub up keystroke emulation! So, just imagine malware product loaded into device memory and waits when you're going to unlock handheld by typing your *top-secret password*. After inputting is half-closed malware types just the one random letter to make senseless your unlocking action. And BlackBerry says *Wrong password! Try once again. The 2/10 attempt* (Figure 2, 3, 4, 5). Come to think of it that you never can to input correct password. What's going on 10 wrong attempts? One of several BlackBerry secured mechanism is being activated to wipe out your confidentially information. What of it! It was high time to do backup. The lesser

painful alternative is the malware typing unnecessary symbols whenever it possible. It's in case OSv4 and OSv5. In OS v6 your device is blocked for a time is various from 1 minute to 1 hour (Figure 6).

Malware Design

Ultimate goal is show what API-routines help us to design such malware. List of API classes is shall be import is presented in Listing 1.

The first public class `net.rim.blackberry.api.cradle.CradleHandlerRegistry` is need to registry for cradle handlers that are a candidate to be started when a cradle of the corresponding type is connected.

The second public interface `KeyListener` gives us the listener interface for receiving keyboard events (`KEY_DOWN` & `KEY_UP` event to simulate full key pressing).

The third class `net.rim.device.api.system.EventInjector` or gives us a character input event. So if we can use physical key injecting events, use `EventInjector.KeyCode` Event.

Did you know?

Some API-routines need to be signed in your application by rim developer keys. If you intend to use this element, please visit <http://www.blackberry.com/go/codesigning> to obtain a set of code signing keys. Code signing is only required for applications running on BlackBerry smartphones; development on BlackBerry Smartphone Simulators can occur without code signing. You can get your develop keys til 48 hour after registration and payment 20\$

Listing 1. API-routines to design malware injector

```
net.rim.blackberry.api.cradle
net.rim.device.api.system.Characters;
net.rim.device.api.system.EventInjector;
net.rim.device.api.system.KeyListener;
```

Listing 2. Simulation piece of code without key repeating

```
VKeyIsDown = new EventInjector.KeyEvent(EventInjector.KeyEvent.KEY_DOWN, Characters.LATIN_SMALL_LETTER_V,
    KeyListener.STATUS_NOT_FROM_KEYPAD);
VKeyIsUp = new EventInjector.KeyEvent(EventInjector.KeyEvent.KEY_UP, Characters.LATIN_SMALL_LETTER_V,
    KeyListener.STATUS_NOT_FROM_KEYPAD);
```

Listing 3. Simulation piece of code with key repeating.

```
VKeyIsDown = new EventInjector.KeyEvent(EventInjector.KeyEvent.KEY_DOWN, Characters.LATIN_SMALL_LETTER_V,
    KeyListener.STATUS_NOT_FROM_KEYPAD);
VKeyIsRepeat = new EventInjector.KeyEvent(EventInjector.KeyEvent.KEY_REPEAT, Characters.LATIN_SMALL_LETTER_V,
    KeyListener.STATUS_NOT_FROM_KEYPAD);
VKeyIsUp = new EventInjector.KeyEvent(EventInjector.KeyEvent.KEY_UP, Characters.LATIN_SMALL_LETTER_V,
    KeyListener.STATUS_NOT_FROM_KEYPAD);
```

`EventInjector.KeyCodeEvent` is one of them. It's only accessible by signed applications. To simulate key pressing we have to inject a `KEY_DOWN` event followed by a `KEY_UP` event on the same key in the Listing 2. To duplicate the same character e.g. V you need to add one more injection via `KEY_REPEAT` (between `VKeyIsDown-line` and `VKeyIsUp-line`) event like presented in Listing 3.

Keystore Constants

`KEY_DOWN` – Represents a constant indicating that the key is in the down position.

`KEY_REPEAT` – Represents a constant indicating that the key is in the down position, repeating the character.

`KEY_UP` – Represents a constant indicating that the key is in the up position.

`STATUS_NOT_FROM_KEYPAD` – Status flag indicating that the inputted value is a char, and has no key association

To keep BlackBerry Smartphone user having a nightmare with typing extra secret password we should to design time span injection is one (or less) second. It's more than enough!

Our finally subroutine is accommodate `VKeysDown`, `VKeysRepeat` (optionally), `VKeysUp` and time span. `VKeysRepeat` counter is set quantity of character duplicate. Piece of code is presented in Listing 4.

Is key logger dead?

A screenshot or screen capture is a static image taken by the computer to record the visible items displayed on the monitor, television, or another visual output device.

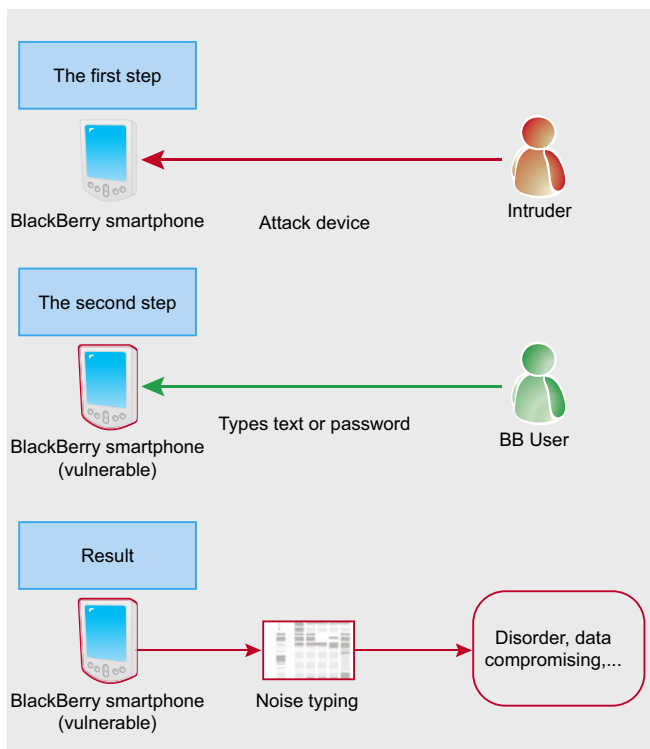


Figure 7. Key Injection Vulnerability Model

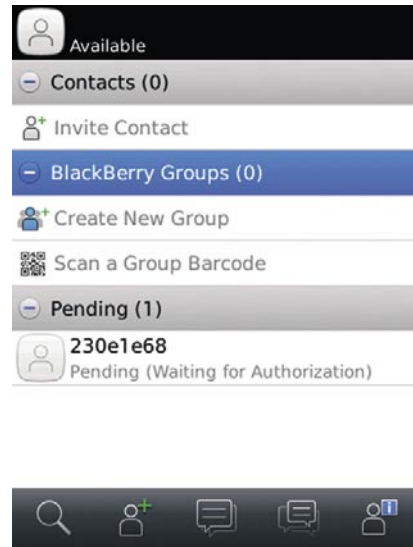


Figure 8. Stolen image of BlackBerry Messenger

In other words, it is a way of taking a snapshot, or picture, of your computer screen. Some people also call it a screen grab or screen dump.

Screen shots can be very helpful when you need to demonstrate something that would be difficult to explain in words. Here are just a few examples of situations where a screen shot can be useful and why:

- In software reviews, to show what the software looks like.
- In software tutorials, to demonstrate how to perform a function.
- In technical support troubleshooting, to show error message or software issues.

Screen shots are also useful to save snippets of anything you have on your screen, particularly when it cannot be easily printed. I use screen shots all the

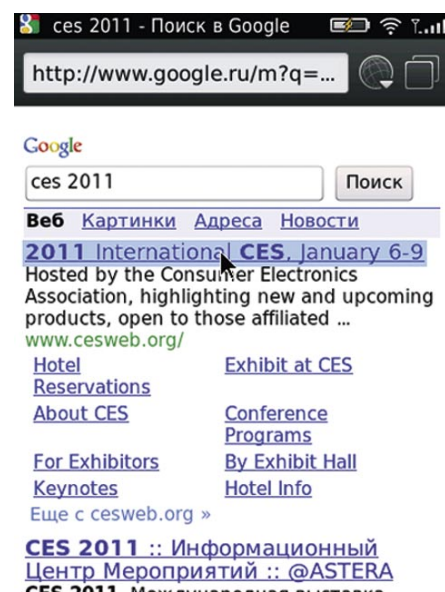


Figure 9. Stolen image of BlackBerry Browser part 1



Figure 10. Stolen image of BlackBerry Browser part 2

time for things I want to save to refer to later, but don't necessarily need a printed copy of.

Screen recording

Sometimes, it takes more than a couple of images. 25-30 images are picked up during 1 second gives us video frame. So, the screen recording capability of some screen capture programs is a time-saving way to create instructions and presentations, but the resulting files are

Listing 4. Simulation piece of code without key repeating.

```
EventInjector.invokeEvent(VKeyIsDown);
EventInjector.invokeEvent(VKeyIsRepeat); //
    (optionally)
EventInjector.invokeEvent(VKeyIsUp);
Thread.sleep(1000); // TimeSpan 1000 msec (1 sec).
```

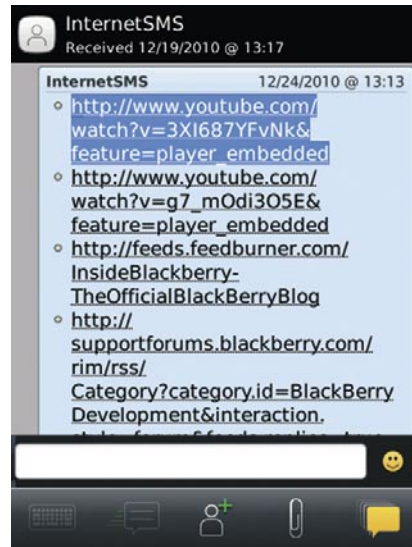


Figure 12. Stolen image of chat

often large. A common problem with video recordings is the action jumps, instead of flowing smoothly, due to low frame rate.

For many cases, high frame rates are not required. This is not generally an issue if simply capturing desktop video, which requires far less processing power than video playback, and it is very possible to capture at 30 frame/s. But it's enough to log your keystrokes.

Listing 5. API-routines to design malware photo sniffer

```
net.rim.device.api.system.Bitmap;
net.rim.device.api.system.Display;
net.rim.device.api.ui.Screen;
net.rim.device.api.ui.Ui;
net.rim.device.api.ui.UiApplication;
```



Figure 11. Stolen image of BlackBerry Browser part 3

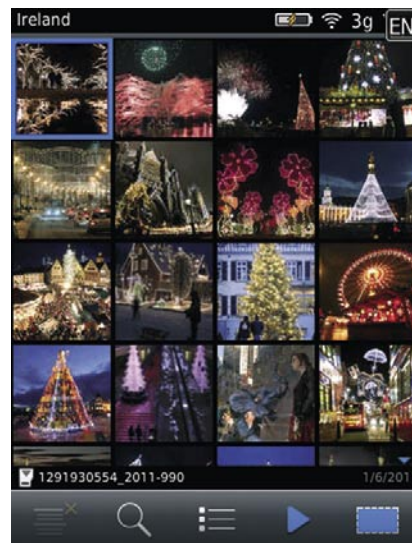


Figure 13. Stolen image of photo explorer

Listing 6. API-routines to design malware photo sniffer

```
Screen vulnerable_screen = Ui.getUiEngine().getActiveScreen();
Bitmap bitmap_of_vulnerable_screen = new Bitmap(vulnerable_screen.getWidth(),vulnerable_screen.getHeight());
Display.screenshot(bitmap_of_vulnerable_screen, 0, 0, vulnerable_screen.getWidth(),vulnerable_
screen.getHeight());
```

Keystroke logger is only allowed to his own application on BlackBerry Devices. It means you can't steal any information that user might type by keyboard sniffer. Despite this security feature it still possible to sneak your password or your messages. Try and remember uncomfortable feeling when somebody try look into your device screen. In a different way you can capture and dump screen image (Figure 8 – 14).

Malware Design

Ultimate goal is show what API-routines help us to design such malware. List of API classes is shall be import is presented in Listing 5.

The first public class `net.rim.device.api.system.Bitmap` needs to construct a blank bitmap object.

The second public class `net.rim.device.api.system.Display` provides access to the device's display when we're going to take a screenshot of a portion of the screen and saves it into a bitmap object.

Three public classes `net.rim.device.api.ui` define functionality for a user interface engine applications can use for their UI operations. As it pushes screens onto the stack, it draws them on top of any other screens already on the stack. When the application pops a screen off the stack, it redraws the underlying screens as necessary. From capture to capture we have to put

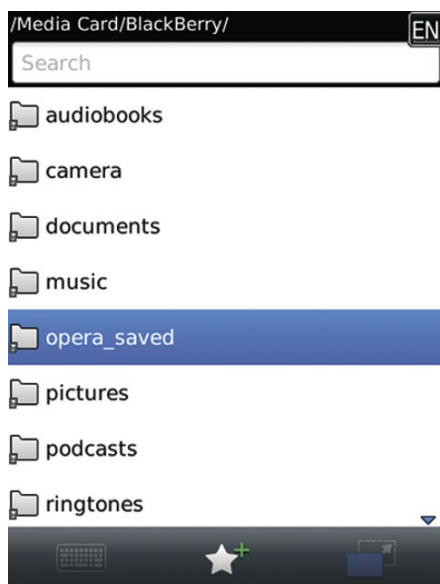


Figure 14. Stolen image of file explorer

in and put out next screen onto stack by `UiApplication.getUiApplication().popScreen(this)`, `UiApplication.getUiApplication().pushScreen(this)`.

Before our malware has got a static image of vulnerable screen it should get active screen and retrieves screen size to put it into bitmap object that's presented int Listing 6.

Also we can put timespan as 40 msec and loop it. Loop quantity is optional. Then malware needs to save static images to memory or file. For example, malware demo saves it to bytes memory array. Piece of code is presented in Listing 7.

Behind mirror

Previous vulnerabilities show how intruder can get your messages, tasks, chats (in short everything is possible to photocapture) and then block normal operation with blackberry device as far as possible. But is there no way to sneak blackberry password?

In first part I refer to attempt quantity you set in your device. It's various from 3 to 10. The second half of it

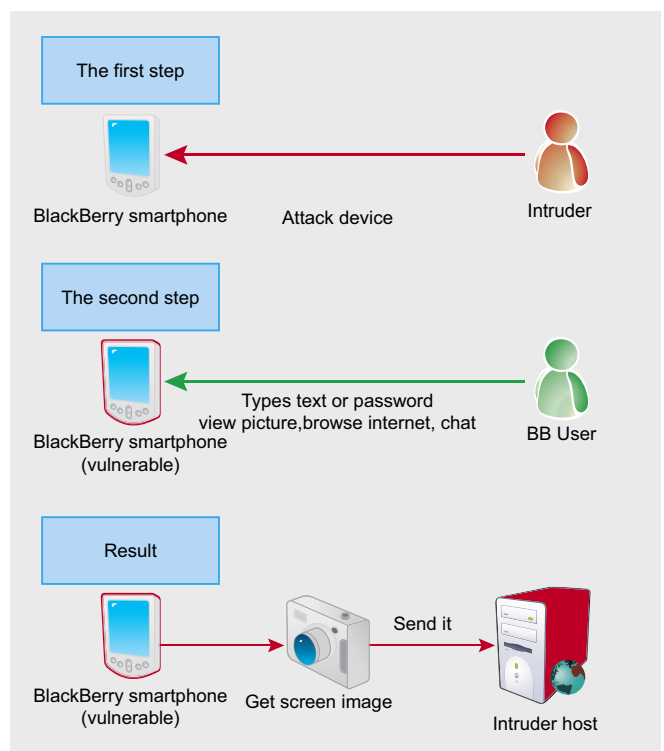


Figure 15. Photo Sniff Vulnerability Model

Listing 7. API-routines to design malware photo sniffer

```

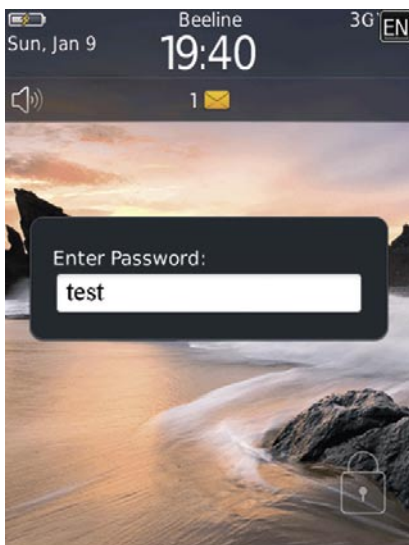
public byte[] getBytesFromBitmap(Bitmap bmp)
{
    int height=bmp.getHeight();
    int width=bmp.getWidth();

    ByteArrayOutputStream bos = new
        ByteArrayOutputStream();
    DataOutputStream dos = new DataOutputStream(bos);
    Graphics g = new Graphics(bmp);
    bmp.getARGB(rgbdata,0,width,0,0,width,height);
    for (int i = 0; i < rgbdata.length ; i++)
    {
        if (rgbdata[i] != -1)
        {
            dos.writeInt(i);
            dos.flush();
        }
    }
    bos.flush();
    return bos.toByteArray();
}

```

isn't masked behind asterisk by default. This feature corresponds to the device option *suppress password echo* (or BES IT Policy) is set in true by default. It means.

First malware (key injector) waits moment till user unlocks device then type noise symbol at that time the second malware (photo sniffer) is steal an image of device. Done! Now a violator can whatever you like, for example decipher your file backup and get your actuals (Figure 16).

**Figure 16.** Unmasked typing

Malware Design

To design this type of malware you need combine the previous pieces of code.

Mitigation

If you are BIS consumer you always check permissions when downloading an application to disable key injection or screenshot capture. Additionally you should set option *suppress password echo* to false. If you are BES consumer your administrator should check IT Policy like this:

Key Injection:

```
"Application Control Policy a Event Injection" = False
```

Device Screen Capture:

```
"IT Policy a Security Policy Group a Allow Screen Shot
Capture" = False
```

Combo Vuln

```
"IT Policy a Password Policy Group a Suppress Password
Echo" = False
```

Did you know?

Phishing kits are constructed by con artists to look like legitimate communications, often from familiar and reputable companies, and usually ask victims to take urgent action to avoid a consequence or receive a reward. The desired response typically involves logging in to a Web site or calling a phone number to provide personal information.

Fobbing off is no object!

Understanding the human factors that make people vulnerable to online criminals can improve both security training and technology. Since recently, phish email were headache task for bank consumers, online consumers, etc. Up to now, there's one more phish kit. It's called a scumware that disguised as genuine software, and may come from an official site. For example, user has just downloaded a video player. Before downloading BlackBerry smartphone asking him to set permissions for new application. Typical user allows all because he's bored with it. He's bored with think what to do – allow only Wi-Fi connection or 3G too, disallow access to PIM and any kind of messages. He waits *mega secure technology* that says: don't worry! It's video or mp3 player. There's shouldn't access to personal data. Still waits. And how! Then typical user click button with caption *Make me Happy!*. So, he gives full access for intruder application because he's tired of pop-up permissions. Then GPS location is steal, his photos or videos, his PIM, chats, etc. Afterwards he looks in wide-eyed astonishment. You don't say so! Why? I'm not to

On the 'Net

- <http://blogs.wsj.com/wtk-mobile/> – The Wall Street Journal brief research of genius spyware
- http://docs.blackberry.com/en/admin/deliverables/12063/BlackBerry_Enterprise_Server_Policy_Reference_Guide-T323212-832026-1023123101-001-5.0.1-US.pdf – BlackBerry Enterprise Server Version: 5.0. Policy Reference Guide, RIM,
- <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html> – The Wall Street Journal research of genius spyware on iPhone and Android
- http://docs.blackberry.com/en/developers/deliverables/11961/BlackBerry_Java_Application-Feature_and_Technical_Overview--789336-1109112514-001-5.0_Beta-US.pdf – BlackBerry Java Application. Version: 5.0. Feature and Technical Overview, RIM
- http://docs.blackberry.com/en/developers/deliverables/9091/JDE_5.0_FundamentalsGuide_Beta.pdf – BlackBerry Java Application. Version: 5.0. Fundamentals Guide, RIM,
- http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/8655/8656/1106255/BlackBerry_Application_Developer_Guide_Volume_1.pdf?nodeid=1106256&vernum=0 – BlackBerry Application Developer Guide Volume 1: Fundamentals (4.1), RIM,
- http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/8067/645045/8655/8656/1106255/BlackBerry_Application_Developer_Guide_Volume_2.pdf?nodeid=1106444&vernum=0 – BlackBerry Application Developer Guide Volume 2: Advanced Topics (4.1), RIM,
- <http://www.blackberry.com/developers/docs/4.2api/> – RIM Device Java Library – 4.2.0 Release (Javadoc), RIM,
- http://docs.blackberry.com/en/developers/deliverables/15497/BlackBerry_Smartphone_Simulator-Development_Guide--1001926-0406042642-001-5.0-US.pdf – BlackBerry Smartphone Simulator. Version: 5.0. Development Guide, RIM,
- http://docs.blackberry.com/en/developers/deliverables/1077/BlackBerry_Signing_Authority_Tool_1.0_-_Password_Based_-_Administrator_Guide.pdf – BlackBerry Signature Tool 1.0. Developer Guide, RIM

download Trojan! But there's just one shag to it. The salesman has already fobbed off the faulty application on him.

Sometimes events are developing in another way. According to the WALL STREET JOURNAL (<http://wsj.com>) marketers are tracking smartphone users through applications – games and other software on their phones. It collects information including location, unique identifiers for the devices such as IMEI, and

personal data. Then applications send this information to marketing companies from time to time (<http://blogs.wsj.com/wtk-mobile/>, <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>).

Conclusion

It happens that there are serious deficiencies in the numbers of suitable vulnerability survey mythicize computer privacy. Real-world example is said there have been no exploitable BlackBerry handheld vulnerabilities published since 2007 year. Even the 2007 vuln was a DoS, not taking control of the device. As a matter of fact Praetorians made a much powerful exploit (Blackberry Attack Toolkit – <http://www.praetoriant.net/>) that was present on the DEFCON 14 in July, 2006. This condition implies ability to speak well for design a botnet applications and networks that applicable to deface vital role information systems such as trading session or air reservation.

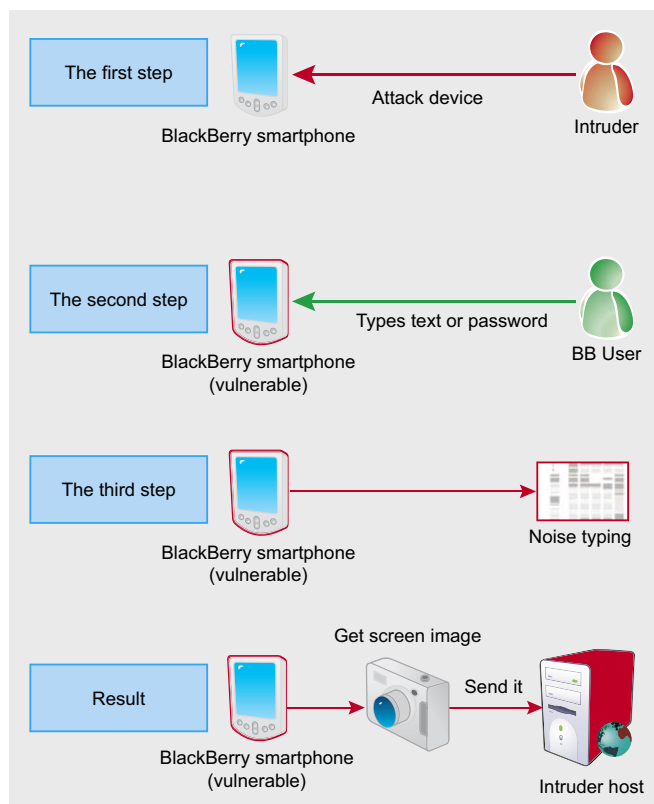


Figure 17. Combo Vulnerability Model

YURY CHERMERKIN

Graduated at Russian State University for the Humanities (<http://rggu.com/>) in 2010. At present postgraduate at RSUH. Security Analyst since 2009 and currently works as mobile security researcher in Moscow.

E-mail: yury.chemerkin@gmail.com.

Facebook: <http://www.facebook.com/people/Yury-Chemerkin/100001827345335>.

Examine your Network With Nmap

What is network Scanning?

Network scanning is an important part of network security that any system administrator must be comfortable with. Network scanning usually consists of a port scanner and vulnerability scanner.

What you will learn...

- how to examine a website or IP address for security hole
- hacker spends 90% of the time for gathering information on a target and 10% on launching the attack.

What you should know...

- basic networking skills (like Network+)

Port scanner is a software that was designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and can be used by an attacker to identify running services on a host with the view to compromise it. A port scan sends client requests to a server port addresses on a host for finding an active port. The design and operation of the Internet is based on TCP/IP. A port can have some behavior like below:

1. Open or Accepted: The host sent a reply indicating that a service is listening on the port.
2. Closed or Denied or Not Listening: The host sent a reply indicating that connections will be denied to the port.
3. Filtered, Dropped or Blocked: There was no reply from the host.

Port scanning has several types such as: TCP scanning, SYN scanning, UDP scanning, ACK scanning, Window scanning, FIN scanning, X-mas, Protocol scan, Proxy scan, Idle scan, CatSCAN, ICMP scan. Below we explain a number of these scans:

TCP scanning

The simplest port scanners use the operating system's network functions and is generally the next option to go to when SYN is not a feasible option.

SYN scanning

SYN scan is another form of TCP scanning. Rather than use the operating system's network functions, the port scanner generates raw IP packets itself, and monitors for responses. This scan type is also known as *half-open scanning*, because it never actually opens a full TCP connection.

UDP scanning

UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. If a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. If a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open.

ACK scanning

This kind of scan does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered. This kind of scan can be good when attempting to probe for the existence of a firewall and its rule sets.

FIN scanning

Usually, firewalls are blocking packets in the form of SYN packets. FIN packets are able to pass by firewalls with no modification to its purpose. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand.

Nmap Support large number of this scanning.

A *vulnerability scanner* is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. It is important that the network administrator is familiar with these methods.

There are many types of software for scanning networks, some of this software is free and some are not, at <http://sectools.org/vuln-scanners.html> you can find list of this software.

The significant point about Nmap (Network Mapper) is Free and Open Source. Nmap is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) for discover hosts and services on a computer network. Nmap runs on Linux, Microsoft Windows, Solaris, HP-UX and BSD variants (including Mac OS X), and also on AmigaOS and SGI IRIX.

Nmap includes the following features:

- Host Discovery
- Port Scanning
- Version Detection
- OS Detection
- Scriptable interaction with the target

Nmap Works in two modes, in command line mode and GUI mode. Graphic version of Nmap is known as Zenmap. Official GUI for Nmap versions 2.2 to 4.22 are known as *NmapFE*, originally written by *Zach Smith*. For Nmap 4.50, NmapFE was replaced with Zenmap, a new graphical user interface based on *UMIT*, developed by *Adriano Monteiro Marques* (Figure 1).

Working with Zenmap is easy and have a good environment for work.

There are many features about Nmap, but we can not say about all in this article. I can just discuss some of the important features.

Scan a Single Target

For scanning a single target, your target can be specified as an IP address or host name.

```
Usage syntax: nmap [target]
$ nmap 192.168.10.1
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-07
19:38 CDT
Interesting ports on 192.168.10.1:
Not shown: 997 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    closed ftp
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 7.21
seconds
```

In the above example, PORT show port number/ protocol and STATE show state of port and SERVICE show type of service for the port. You can scan multiple targets with following syntax:

```
Usage syntax: nmap [target1 target2 etc]
$ nmap 192.168.10.1 192.168.10.100 192.168.10.101
```

Scan a Range of IP Addresses

A range of IP addresses can be used for target specification as in the example below.

```
Usage syntax: nmap [Range of IP addresses]
$ nmap 192.168.10.1-100
```

Scan an Entire Subnet

Nmap can be used to scan an entire subnet using CIDR.

```
Usage syntax: nmap [Network/CIDR]
$ nmap 192.168.10.1/24
```

You can create a text file that contains of your victim and give this file to Nmap for Scan, see the example below:

```
Usage syntax: nmap -iL [list.txt]
$ nmap -iL list.txt
```

Exclude Targets from a Scan

For excluding a target from scan, you can use this syntax:

```
Usage syntax: nmap [targets] --exclude [target(s)]
$ nmap 192.168.10.0/24 --exclude 192.168.10.100
```

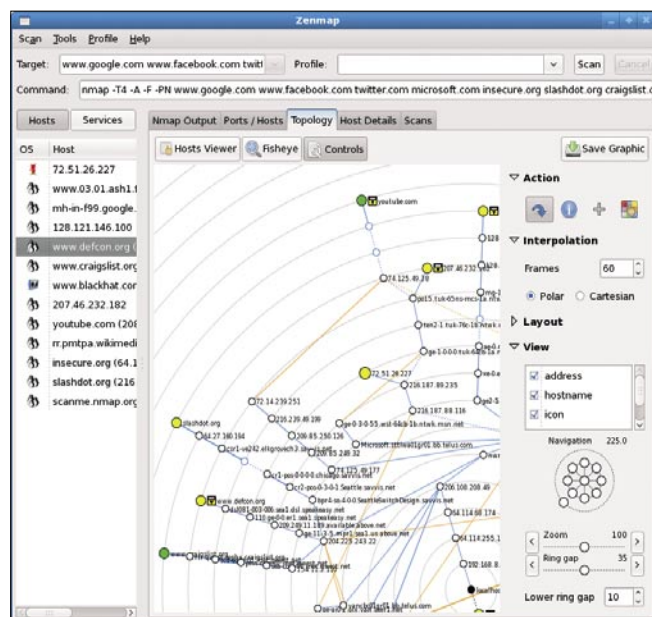


Figure 1. Phases of hacking

Scan an IPv6 Target

In addition to IPv4, Nmap can scan IPv6. The `-6` parameter is used to perform IPv6 scan.

```
Usage syntax: nmap -6 [target]
# nmap -6 fe80::29aa:9db9:4164:d80e
```

You can see a summary of some features about Discovery Options for quick read in Table 1.

In this paper we refrain from explaining details and, for example, only show general form for using.

Don't Ping

```
Usage syntax: nmap -PN [target]
$ nmap -PN 10.10.5.11
```

Other features are used similarly. Lets examine Advanced Scanning Options. Nmap supports a number of user selectable scan types. By default, Nmap will perform a basic TCP scan on each target system. In some situations, it may be necessary to perform more complex TCP (or even UDP) scans to find uncommon services or to evade a firewall. In the table below we show some option that you need to perform for advanced scanning (see Table 2).

We are just presenting the general form of scanning and some of the options that require special settings.

Advanced scanning is used like other scanning, in the below example we show you how to use options to scan target.

Note

You must login with root/administrator privileges (or use the sudo command) to execute many of the scans .

TCP SYN Scan

To performs a TCP SYN scan you must use the `-sS` option.

Table 1. Discovery Options

Feature	Option
Don't Ping	<code>-PN</code>
Perform a Ping Only Scan	<code>-sP</code>
TCP SYN Ping	<code>-PS</code>
TCP ACK Ping	<code>-PA</code>
UDP Ping	<code>-PU</code>
SCTP INIT Ping	<code>-PY</code>
ICMP Echo Ping	<code>-PE</code>
ICMP Timestamp Ping	<code>-PP</code>
ICMP Address Mask Ping	<code>-PM</code>
IP Protocol Ping	<code>-PO</code>
ARP Ping	<code>-PR</code>
Traceroute	<code>--traceroute</code>

```
Usage syntax: nmap -sS [target]
# nmap -sS 10.10.1.48
```

Other options are used in the above form, but only some of them require special settings.

Custom TCP Scan

The `--scanflags` option is used to perform a custom TCP scan.

```
Usage syntax: nmap --scanflags [flag(s)] [target]
# nmap --scanflags SYNURG 10.10.1.127
```

The `--scanflags` option allows users to define a custom scan using one or more TCP header flags (see Table 3).

Port Scanning Options

There are a total of 131,070 TCP/IP ports (65,535 TCP and 65,535 UDP). Nmap, by default, only scans 1,000 of the most commonly used ports.

In the table below, we're showing some of the options that you require to perform in port scanning (see Table 4).

For using this options we're showing some of the options that require special settings.

Do a quick scan

The `-F` option instructs Nmap to perform a scan of only the 100 most commonly used ports.

Table 2. Advanced Scanning

Feature	Option
TCP SYN Scan	<code>-sS</code>
TCP Connect Scan	<code>-sT</code>
UDP Scan	<code>-sU</code>
TCP NULL Scan	<code>-sN</code>
TCP FIN Scan	<code>-sF</code>
Xmas Scan	<code>-sX</code>
TCP ACK Scan	<code>-sA</code>
Custom TCP Scan	<code>--scanflags</code>
IP Protocol Scan	<code>-sO</code>
Send Raw Ethernet Packets	<code>--send-eth</code>
Send IP Packets	<code>--send-ip</code>

Table 3. TCP flags

Flag	Usage
SYN	Synchronize
ACK	Acknowledgment
PSH	Push
URG	Urgent
RST	Reset
FIN	Finished


```
Usage syntax: nmap -F [target]
$ nmap -F 10.10.1.44
```

Nmap scans the top 1000 commonly used ports by default. The `-F` option reduces that number to 100.

Scanning port through a name

The `-p` option can be used to scan ports by name.

```
Usage syntax: nmap -p [port name(s)] [target]
$ nmap -p smtp,http 10.10.1.44
```

Scanning Ports by Protocol

Specifying a T: or U: prefix with the `-p` option allows you to search for a specific port and protocol combination.

```
Usage syntax: nmap -p U:[UDP ports],T:[TCP ports] [target]
# nmap -sU -sT -p U:53,T:25 10.10.1.44
```

Scan Top Ports

The `--top-ports` option is used to scan the specified number of top ranked ports.

```
Usage syntax: nmap --top-ports [number] [target]
# nmap --top-ports 10 10.10.1.41
```

Operating System and Service Detection

One of Nmap's features is its ability to detect operating systems and services on remote systems. This feature analyzes responses from scanned targets and attempts to identify the host's operating system and installed services.

In the table below, we're showing some of the options that you require to perform Operating System and Service Detection (see Table 5). Use these options as well as other options listed below:

Operating System Detection

The `-O` parameter enables Nmap's operating system detection feature.

```
Usage syntax: nmap -O [target]
# nmap -O 10.10.1.48
```

Table 4. Port Scanning Options

Feature	Option
Do a quick scan	<code>-F</code>
Scanning a specific port	<code>-p [port]</code>
Scanning port through a name	<code>-p [name]</code>
Scanning Ports by Protocol	<code>-p U:[UDP ports],T:[TCP ports]</code>
Scan All Ports	<code>-p ""</code>
Scan Top Ports	<code>--top-ports [number]</code>
Perform port scanning consecutive	<code>-r</code>

Attempt to Guess an Unknown Operating System

If Nmap is unable to accurately identify the OS, you can force it to guess by using the `--osscan-guess` option.

```
Usage syntax: nmap -O --osscan-guess [target]
# nmap -O --osscan-guess 10.10.1.11
```

Evading Firewalls

Firewalls and IDS are designed to prevent tools like Nmap. Nmap includes a number of features designed to circumvent these defenses (see Table 6). We will quickly show how to use these options.

Fragment Packets

The `-f` option is used to fragment probes into 8-byte packets.

```
Usage syntax: nmap -f [target]
# nmap -f 10.10.1.48
```

Specify a Specific MTU

```
Usage syntax: nmap --mtu [number] [target]
# nmap --mtu 16 10.10.1.48
```

In the above example, the `--mtu 16` argument instructs Nmap to use tiny 16-byte packets for the scan.

Use a Decoy

```
Usage syntax: nmap -D [decoy1,decoy2,etc|RND:number] [target]
# nmap -D RND:10 10.10.1.48
```

Table 5. OS and service detection options

Feature	Option
Operating System Detection	<code>-O</code>
Trying to guess the unknown operating system	<code>--osscan-guess</code>
Service Version Detection	<code>-sV</code>
Perform a RPC Scan	<code>--version-trace</code>
Troubleshooting Version Scans	<code>-sR</code>

Table 6. Options for escape the firewall

Feature	Option
Fragment Packets	<code>-f</code>
Specify a Specific MTU	<code>--mtu</code>
Use a Decoy	<code>-D</code>
Idle Zombie Scan	<code>-sI</code>
To specify the source port to manually	<code>--source-port</code>
Append Random Data	<code>--data-length</code>
Randomize Target Scan Order	<code>--randomize-hosts</code>
Spoof MAC Address	<code>--spooof-mac</code>
Send Bad Checksums	<code>--badsum</code>

In the above example `nmap -D RND:10` instructs Nmap to generate 10 random decoys.

Idle Zombie Scan

```
Usage syntax: nmap -sI [zombie host] [target]
# nmap -sI 10.10.1.41 10.10.1.252
```

In this example 10.10.1.41 is the zombie and 10.10.1.252 is the target system. To specify the source port manually:

```
Usage syntax: nmap --source-port [port] [target]
# nmap --source-port 53 scanme.insecure.org
```

Append Random Data

```
Usage syntax: nmap --data-length [number] [target]
# nmap --data-length 25 10.10.1.252
```

In the above example 25 additional bytes are added to all packets sent to the target.

Randomize Target Scan Order

```
Usage syntax: nmap --randomize-hosts [targets]
$ nmap --randomize-hosts 10.10.1.100-254
```

Spoof MAC Address

```
Usage syntax: nmap --spooof-mac [vendor|MAC|0] [target]
# nmap -sT -PN --spooof-mac 0 192.168.1.1
```

The `--spooof-mac` option has the following parameters: see Table 7.

Send Bad Checksums

```
Usage syntax: nmap --badsum [target]
# nmap --badsum 10.10.1.41
```

Only a system with poor configuration, would respond to a packet with a bad checksum.

Tabela 7. Options to Spoof MAC Address

Argument	Function
0 (zero)	Generates a random MAC address
Specific MAC Address	Uses the specified MAC address
Vendor Name	Generates a MAC address from the specified vendor (such as Apple, Dell, 3Com, etc)

Tabela 8. Options for generate outputs

Feature	Option
Save Output to a Text File	-oN
Save Output to a XML File	-oX
Grepable Output	-oG
Output All Supported File Types	-oA
133t Output	-oS

On The 'Net

- http://en.wikipedia.org/wiki/Port_scanner
- http://en.wikipedia.org/wiki/Vulnerability_scanner
- <http://nmap.org>

Output Options

Nmap offers some options to generate formatted output. You can save your output in Text, Xml and single line grepable file. In the table below, we're showing some of the options that you require to generate your desired output (see Table 8). All features can be used as they are, so we just give an example.

Save Output to a Text File

For saving output as a text file we use `-oN` option.

```
Usage syntax: nmap -oN [scan.txt] [target]
$ nmap -oN scan.txt 10.10.1.1
```

Other features are like each other, but in output all supported file types option, you don't need to specify extensions.

This property is used as follows:

```
Usage syntax: nmap -oA [filename] [target]
$ nmap -oA scans 10.10.1.1
```

Another option is 133t output. It outputs only for joking. In below you can see example of this option.

```
Usage syntax: nmap -oS [scan.txt] [target]
$ nmap -oS scan.txt 10.10.1.1
$ cat scan.txt
  StaRtING NMap 5.00 ( htTp://nmap.oRg ) aT 2009-08-13 15:45 CDT
!nt3r3St|ng pOrts On 10.10.1.1:
n0t $h0wn: 998 cl0$3d p0rt$
  PORT $TATE seRV!CE
  80/tcp Open hTtp
  443/tcp Open https
Nmap DOnE: 1 Ip addresz (1 host up) $canned iN 0.48 $3c0nds
```

Remotely scan

Nmap has a version that runs online and you can scan your target remotely. Visit <http://nmap-online.com/>, enter your IP address for scanning, select your scan type, click scan now button and scanning results later will be displayed.

MOHSEN MOSTAFA JOKAR

Nmap® Cookbook The fat-free guide to network scanning



black hat[®] europe
DIGITAL SELF DEFENSE
(march 15 - 18) +2011

BARCELONA, SPAIN
HOTEL REY JUAN CARLOS

Understanding the increasingly complex threats posed to an enterprise is a daunting task for today's security professional. The knowledge to secure an enterprise against those threats is invaluable. Come to Black Hat and learn from the industry's best. Register for Black Hat Europe today at www.blackhat.com. Use the promo code **BHEUHAKIN9** and receive 15% off of Briefings registration.

Network Security – Data Breaches

There doesn't appear to be a day that passes where we don't hear about a corporate or government network data breach (<http://datalossdb.org/>) in the media. Whatever individuals or businesses do, we all fail miserably when it comes to protecting our most valued assets – personal and financial information. So what is a data breach and how will it affect businesses, government and individuals? What about the data breach threat to virtualisation (cloud computing), which is becoming part of business, general public and government strategies?

Reasons to be vigilant

In the past twelve months (January to December 2010) there have been many network breaches of corporate networks and websites. The main purpose of any data breach is to steal business and/or consumer data. Information compromise is a growing threat to businesses and in particular online e-commerce. It's also a threat for individuals who don't have any control over the data that is parsed to the businesses and is sold/rented between companies i.e. marketing agencies.

Critical proprietary data that is compromised will always be a major story if leaked to the media. So for most businesses it is very important that the threat of data breaches is reduced or in some cases removed (sensitive data held off network or accessed at specific intervals or time periods). The damage to reputation, brand and the bottom line is significant if a data breach occurs.

The black market commodity

On the black market private data is an important commodity. The critical personal and financial data can be used to obtain credit or a loan and even worse steal personal fraudulent documents. In terms of identity theft, a data security breach may involve using malicious software to collect individual information that is ultimately used to drain bank accounts or to create new credit accounts that are subsequently exhausted by the hacker or the entity that purchases the information from the hacker. This information may include government-issued identification numbers like driver's license data,

Social Security numbers, credit card and bank account numbers, and any other data that could be exploited for personal use.

Imagine what would happen if this information fell into the wrong hands? The data is quite often both personal and financial which lead to fraud, identity fraud and of course corporate and government espionage.

Data breach notifications

In the US, data breach laws are fully established in most states. Many US states opt to penalise companies that are found to have lost or had data stolen. As mentioned earlier, the loss of reputation and crippling fines isn't something a small or medium business could ignore. The financial loss could be significant. The UK will no doubt follow the US here either through its own laws or through the EU.

Data breach notifications are certainly the norm these days. Business and individuals can receive credit alerts when anything changes on their credit reports i.e. credit or loan application, mobile accounts or a new bank account is opened. If a business loses private information (whether by accident or by a hacker) they are obliged to inform individuals that their data may have been compromised. This type of data leakage normally happens in the financial industry in particular banking but has also affected government – one particular government data breach was the now infamous 2007 UK HMRC data leak where some 25 million personal and banking details were lost in transit

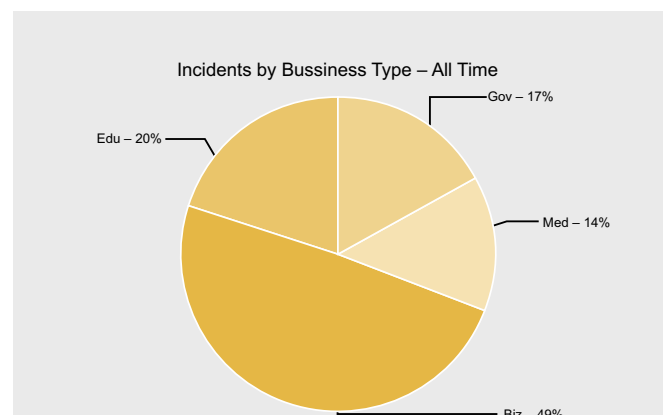


Figure 1. Incidents by Business Type – All Time (DataLossDB, 2011)

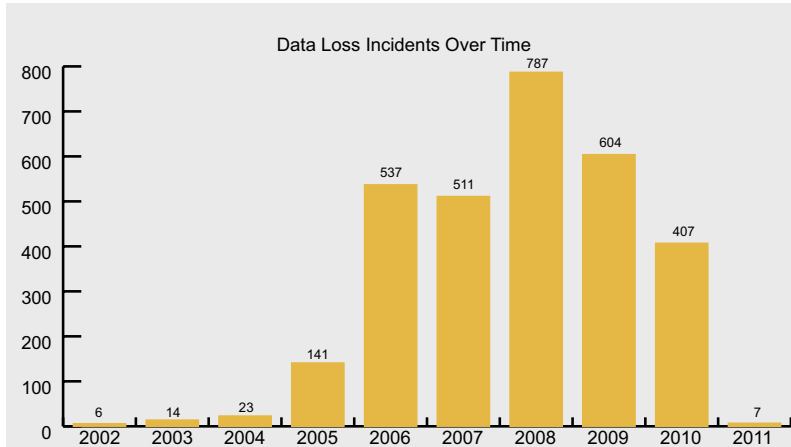


Figure 2. Data Loss Incidents Over Time (DataLossDB, 2011)*
*Figures also include data loss outside of the US i.e. UK

to the UK's National Audit Office. See Figure 1 below which highlights the incidents by business type. It shouldn't surprise you.

In the US there are strict notification laws which clearly define how companies should deal with a data breach. Most companies have to make detailed information available at a customer's request. Business and e-commerce have improved notification of fraudulent events over the past couple of years. This might include an SMS or phone call or a letter in the post (but never an email for obvious reasons).

When a database breach occurs (see Figure 2 for US data loss by year recorded by DataLossDB.org), consumer notification continues to be a public problem, and it's time for the US federal government for example to step in, Forty-six states in the US have breach-notification laws on the books, but no law is the same, and enforcement is weak.

In 2011, as malicious breaches continue and the sophistication of cyberattacks increases, Foley, co-founder of the non-profit Identity Theft Resource Center, says it's time for a national breach notification law that covers all industries and supercedes state laws. (Under the HITECH Act, healthcare organizations must report major breaches to federal authorities.) Source: ITRC, US

Of the breaches recorded by the ITRC in 2010, malicious attacks accounted for more breaches than human error. In fact, 17.1 percent of reported breaches related to hacking, while 15.4 percent related to insider theft. The ITRC expects those types of breaches to increase in 2011, as the use of mobile devices and social networks becomes more prevalent. Source: ITRC, US. Figure 2 clearly highlights that data loss has fallen since 2008.

DataLossDB

DataLossDB (<http://datalossdb.org/>) is a US research project (but also records global data losses which

include the UK and Europe) aimed at documenting known and reported data loss incidents world-wide. The effort is now a community one, and with the move to Open Security Foundation's DataLossDB.org, asks for contributions of new incidents and new data for existing incidents. This is a very useful resource for anyone wanting to find out about the latest breaches.

Click here to find out the latest data breaches in the US: http://datalossdb.org/latest_incidents. You will note that each data breach is categorized – i.e. Hack; stolen document; stolen laptop; disposal document and so on. It certainly makes an interesting read. Take a closer look at the *records stolen*

number as well – it's clear that the data loss frequency is higher but the volume of data being lost is much smaller. These data breaches vary in scale from hundreds of personal/financial records stolen to millions.

Data encryption and sandboxing

So what is an appropriate level of security? So often computers are just password protected but it's relatively easy to crack a password. Hence we hear about data encryption. This should also apply to encrypting email but in most cases it doesn't. To start with, encryption of all files whether on a hard disk or USB should be the starting point. Any loss of information would have limited damage as encryption provides a layer of security that only the persistent or top notch hacker could crack. Sensitive information should never be sent by email.

Businesses and government should also consider employing sandbox environments to every client PC. Individuals could also utilise this technology which would allow users to browse websites and run applications without ever worrying about drive-by-downloads or exploit links. Data that is encrypted isn't actually data until it is decrypted. In the US disclosure requirements are more often than not exempt if the

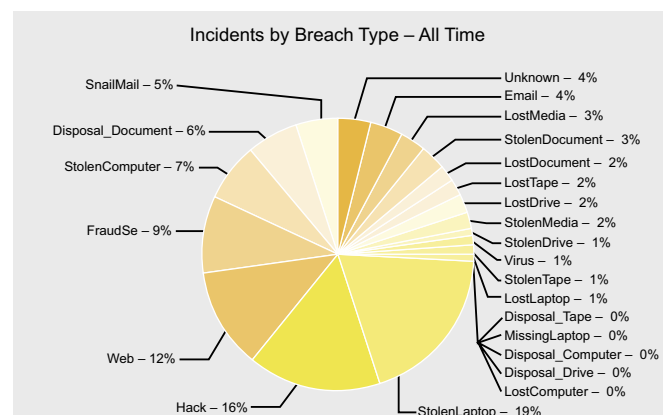


Figure 3. Incidents by Breach Type – All Time (DataLossDB, 2011)

data has been encrypted. This protects a business reputation and customer trust is retained.

OTP Authentication – online banking

To help deter a data breach, Banks (which are leading the way in the financial sector and for good reason too) have started implementing *One Time Passwords* (OTP). These passwords or keys are valid only for one login session – the OTP code can be sent to a PC or mobile phone. PC banking and mobile phone banking applications are now common place, in particular in the US, Europe and the UK.

Statics passwords are still used by the banks which leaves individual and business banking accounts open to *static attack*. Dynamic passwords should be the only option. One solution might be to incorporate *password pattern authentication* technology into the login session – this still uses OTP which relies on a grid of numbers (say five by five) where the user has to remember a pattern rather than a passcode. Worth noting, in China, some banks use this type of authentication technology.

It's nearly impossible to crack the pattern with this type of authentication. This type of authentication could be used on PC's laptops (hard disks, USBs); data storage; network logins; mobile phones; mobile phone banking applications; ATM machines and much more.

Data storage and software patch management

More and more business are relying on electronic data storage for vital documents such as contracts, accounting, client lists and e-commerce. Some of the obvious issues surrounding data privacy include

qualifying who has access to the data and what privileges they have and when are they granted and so on. Businesses will also have to make sure they have the latest security patches deployed on every operating system including Microsoft Windows and Mac OS X as well as Java, Flash, and Adobe software.

How many software updates do businesses and individuals have to patch on a monthly basis? Most users/employees will never update Java or Flash unless enforced in a similar way that Microsoft uses its Windows Updates service. Businesses will take longer to deploy patches – using patch management systems (WSUS or 3rd party software for example) and making sure each patch installs without causing an individual system or network crash.

ENISA

The *European Network and Information Security Agency* (ENISA) has released (January 2011) new reports about the obligation to report data security breaches and about the integration of cloud computing capabilities into European public bodies. Note: This is very similar to DataLossDB.org in the US.

Its *Security and Resilience in Governmental Clouds* report examines the pros and cons of cloud services for public bodies and particularly attempts to identify potential risks involved in the processing of classified information. The report said that while commercial cloud services offer good cost effectiveness, they don't offer public bodies any control over the service; for example, to ensure that applicable laws and regulations are observed.

Consequently, it only recommends the use of such services for non-critical applications. Furthermore, it is questionable whether service accessibility and reliability is satisfactory across all EU countries, said the report. Various sample scenarios offer guidelines for decision-makers about whether using cloud services is advisable in their public body or community.

The *Data Breach Notifications in Europe* (<http://www.enisa.europa.eu/media/press-releases/new-report-data-breach-notifications-in-europe>) report examines the way telecommunications providers currently handle data breaches. Since the beginning of 2010, an obligation to report data breaches, for instance when personal data is copied following a web server break-in, has been in force across the EU.

Virtualization – the next data breach threat

Cloud network security is a virtualization service inside and outside of the firewall. This isn't a new concept. The cloud allows businesses to outsource IT functions, so fundamentally it's the same data security concerns that we see today with mature networks. The major concern for businesses is how they manage security

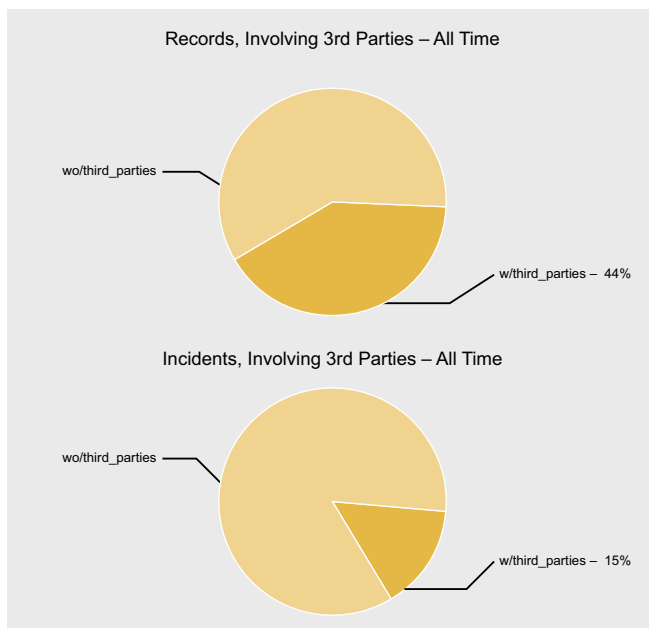


Figure 4. Records and Incidents Involving 3rd Parties – All Time (DataLossDB, 2011)

and compliance with critical IT systems and data storage being hosted out of the network and managed by a third-party.

The answer isn't straight forward. Most companies will follow Sarbanes-Oxley 9* (this Act does not apply to private companies) for security compliance. Security and compliance are two primary factors that determine whether a business moves to the cloud. *Often referred to as SOX.

Note

Sarbanes-Oxley (SOX) does not just apply to US companies – any European business listed on the US stock exchange is affected and any European company with 300 or more shareholders in the US is bound by the requirements.

The following graphs highlight a trend that indicates that data loss incidents involving third parties, on average, result in a greater number of records lost those incidents that do not involve third parties. This may be as a result of the type of data handled by third parties, the process of transferring the data between organizations, or other hypothesis, mostly all speculative as little data exists to establish one cause as dominant. The trend is, however, concerning especially if business and government move to cloud networking and storage for example.

So what is the cloud? The cloud has many types – Public clouds i.e. Amazon Web Services, Newservers; Private clouds – these are data center architectures owned by businesses; Community clouds – this is when infrastructure is shared by several organisations and supports a specific community that has shared concerns; Lastly we have Hybrid clouds – this is the composition of two or more clouds i.e. private, community, or public) that remain unique entities but are bound together by standardised or proprietary technology.

The cloud does throw up some interesting compliance issues for businesses – how do businesses document and audit access, storage and management/security of critical data that are handled by a third-party? More importantly the data management/security is not under the control of company owner – so who will be accountable in the event of a data leakage – the business owner or the third-party?

Service Level Agreements (SLAs) are common place where companies want compliance. The SLAs hold the third-party company, which manages the cloud as the accountable partner, when there is a data breach or violation of the SLA. The main problem here for business is that SLAs are rarely enforced and when they are they are difficult to enforce full stop. The cloud is an on-demand location and doesn't have a fixed infrastructure.

Added to this, the cloud provider will not want an organisation to have full visibility of their network operations – after all they are providing a customer service operation. You can now see some of the issues facing businesses who want to move into the cloud.

Final thoughts – the security policy

Business and government should consider a viable up-to-date security policy. One of the major problems for business and government is that the security policy only address yesterday's threats. Good communication policies are also imperative as are an understanding of what the sensitive data is and safeguarding it. Monitoring and maintaining a *privilege* system whereby users and applications have minimum access to restricted sensitive data is also essential. Monitoring the database for SQL injection attacks and other malicious activity, with real-time monitoring and regular auditing of the network and policies is probably the most important defence as this is where the core data is stored.

It may come as a surprise to know that some companies and government departments don't regularly pen / intrusion test their networks and devices looking for weak passwords and 'vulnerable to exploit' configurations. How many times have we seen default admin passwords never changed on first installation? Remove weak passwords and adopt encryption and sandbox technology on the network and across multiple platforms i.e. PCs, removable media, laptops, smartphones etc and organizations will immediately reduce the data loss threat.

Strong network (this includes wireless) encryption should also be made standard avoiding weak encryption standards and using IPsec, WPA2, SSL and SSH for example. Last but not least there is the social engineering threat which should also be incorporated into any security policy – after all, the main weakness in any organisation isn't the network it's the people that use it.

JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect. IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.

What is Good Enough Coverage?

Everything we buy, build, or test in the security space calls itself full coverage, complete coverage, or all you'll ever need. But we all know no product could possibly say they can be full coverage, as in they'll cover every threat you could be faced with.

Even in just the genre that product runs you can't say it'll get everything. But, are we starting to just accept that everyone can't possibly protect us from everything, so whatever they can do is just fine, as long as it's fast?

I believe we need to as consumers realign what we read into those marketing phrases, and reconsider what we should allow to be acceptable for the rhetoric. When the vendors come in to your organization and start with the usual *We'll solve all your IDS problems, nothing gets by us* we should be really challenging them on these statements. We all know, it's extremely common knowledge, that NO security product is 100%. I'd argue that most security tools at the absolute best will get about 70% of your badness.

Lets talk IDS and IPS for example. That's near and dear to my heart as the Emerging Threats.net guy and now CEO of Emerging Threats Pro (.com). We've just gone through launch, and have spent a lot of time developing our marketing slang. We purposely chose to use the term *comprehensive* to describe our ruleset. My reasoning in this was to make it clear that the ET Pro ruleset is not something that should be combined with another ruleset like the ET Open ruleset should. The open ruleset does not cover all of the major vulnerabilities, but is more malware and current events focused. The ET Pro ruleset is complete and stands on it's own. So we call it comprehensive to make it clear this was as good or better than every other ruleset, but it won't get everything. (We do believe it to be significantly better than anything else out there, but that's a different article).

We did not choose to use the term *Complete*. I don't think any security product can nor should give the impression that they'll catch everything. Our ruleset will catch more, but that's because our focus is different than any other ruleset. So what is *good enough* for IDS/IPS coverage? NSS labs has some great testing standards. And even the best vendors get out of NSS with a 70% accuracy rate or less and call that spectacular, as long as

they can boast some big throughput numbers. Accuracy is a tough thing to define, and NSS I think focuses far too much on hitting a signature for every CVE out there while leaving malware and other issues off to the side.

An effective IDS ruleset HAS to cover malware. Not just the exploits and drive by downloads (which most commercial rulesets don't cover at all). They need to cover the command and control channels. There will be infections on your network, no matter what. It will happen. But you're not going to catch every infection at the point of attack. Many of those will not happen while the computer is on your network, so you have to go with the other indicators of infection, the CnC channel. Every infection has one, and there isn't that much variance, so lets catch them there!

So that's what we focus on in the ET Pro ruleset, the CnC channels as well as the exploit vectors, and we're far more effective at catching malware than any other ruleset. But we're still not 100%. We get that demonstrated to us every morning when we come in and go over our sandnet statistics for the previous night. We sandbox about 120k pieces of malware a day and make sure we have signature coverage. And every day, EVERY SINGLE DAY, we have at least 5-20 new malware strains we didn't catch. We cover those if it's possible, and then move on to the next day. So we will never have complete coverage, and I'd argue that we will have the closest to complete coverage but I'd not venture to say we will get everything. It'd be irresponsible to say so!

What do most vendors intend to build then when they put a product to market? Well we all of course strive to make the best thing we can as security researchers. But, depending on the size of the organization building the product they may also be striving for the most marketable product, or the most profitable product. So to get most marketable, or the highest profit margin something else has to decrease. You're not going to get the most effective security tool and the highest profit margin at the same time. You're not going to get most marketable and

What is Good Enough Coverage?

most secure at the same time. Often the most effective tools are so technical and difficult to deploy that they're a nightmare to sell, so they don't make it to market.

We have to decide what we're really looking for in our security products. Lets stay with IDS/IPS. You can have high throughput, reliable, secure, manageable and inexpensive. All of those exist, but not at the same time. You can have a few of those five qualities at a time. Generally you don't get high throughput and highly secure at the same time. Usually you have to sacrifice ruleset coverage to get faster. You don't get easily manageable and inexpensive at the same time. It takes a lot of effort to build an effective management suite, and that's not cheap.

Every organization needs to decide what of the five qualities are most important to them. Personally, I choose reliable, secure and manageable. Those mean the most to me. I'll spend more money, and I'll put in more devices to cover the same traffic. As a security guy I cannot make that choice to spend less to get less security. I think that's dereliction of duty to make any choice to be less secure when more secure is available and feasible.

Where do you sit on the subject? Will you sacrifice secure for cheaper? When you buy an IDS do you ask where they get their ruleset? How often they update it? How they cover malware? How they cover the mainstream vulnerabilities? How fast do they get MS Patch Tuesday bugs out? Do they cover zero-days discussed on bugtraq before they get a CVE?

My advice, if you ask about ruleset coverage and the sales guy sends you a list of the CVEs they cover, run away. That means they are going to cover just enough to keep a nice long list of CVEs, but still keep the ruleset small enough to have a high throughput number. That means they aren't going after the things that are kicking your network's butt every day, the malware, zero-days, etc. CVEs don't steal data from your network, CnC channels do.

So what is good enough coverage? Everyone has to decide on their own. But please do NOT let security or accuracy be sacrificed for anything. Don't go for the magical 10gig box just to get 10gig. Look at it's security. 10gig is possible, several vendors are putting out 10gig Suricata boxes that are dirt cheap and can run a full ruleset as well as other analysis processes. Suricata is multi-threaded, this is changing the game. We can do large scale on normal hardware!

I'm very interested in what you think. Please send me your thoughts, jonkman@emergingthreatspro.com. Get your copy of the new ET Pro Ruleset, <http://www.emergingthreatspro.com> and support open source security!

MATTHEW JONKMAN

Matt is the founder of emergingthreats.net, the only open and community based intrusion detection ruleset, and is also president of the Open Information Security Foundation (OISF). The OISF is building Suricata, an next generation ids funded by the US Department of Homeland Security.

Join

hakin9 team!



If you would like to help our team in creating hakin9 magazine you can join our authors or betatesters today!

All you need to do, is to send an email to:

editors@hakin9.org

and give us a brief description of your field of interest.

We look forward to hearing from you!

Exploring GCIH certification

for fun and employability

Do you remember the time when you used to read everything you got on Internet from underground e-zines to README files? How many years of professional experience do you have? This really counts. Enhance your skill set by challenging this certification exam! There's no more room to discuss whether it's good or bad being certified. The market needs it.

What you will learn...

- Basics of GIAC certification process
- Practical tips for earning GIAC certs, especially GCIH

What you should know...

- Information Security certification market

Most readers know about the certifications provided by the SANS Institute, better known as GIAC – *Global Information Assurance Certification*. These certifications are among the most respected in *Information Security* (IS) market as well as stand out for being vendor neutral, that is, whose content is not restricted to just one product or manufacturer.

Among the technical certifications listed on the certification portal, here are some of them:

- Firewall Analyst – GCFW
- Intrusion Analyst – CGIA
- Unix Security Administrator – GCUX
- Penetration Tester – GPEN
- Forensic Analyst – GCFA
- Incident Handler – GCIH

The latter will be the target of this article. Later, I will provide valuable tips for future candidates, even for those who could not attend SANS training or conferences.

If you are already familiar with GIAC certification process you can skip directly to the section *Facing the challenge*.

Does GCIH really matters?

Incident Handling is by far one of the most discussed topics in IS community right now. When you hear about

new kind of attacks or even about new worms (got Stuxnet?), all of these are likely to be revealed during an incident handling process.

Knowing what to do (formal procedure) when such events happen is essential for any organization that deals with valuable data. Thus, it's easy to note that this knowledge has not to do with only tactical or operational teams, but strategic too.

The process of studying for – any – certification will give you, at least, a different approach to solve problems that one can face. In this case, time is running against the defender, so knowing what (and how) to handle an incident will make the difference.

SANS has made a great job regarding IS certification development. Many institutions have recognized this effort, including DoD and other dot-gov agencies, since they are requesting for GCIH and other GIAC certified individuals as a requirement to join their CSIRT or SOC teams.

OK, enough said for motivation! In my opinion, this type of certification is challenging and can increase your opportunities, professionally speaking.

What topics are covered in the exam?

The topics are based in a SANS course (Hacker Techniques, Exploits & Incident Handling, SEC-504) and the candidate must answer correctly at least 109 of 150 questions, which represents 73% of all questions. Here is the list of topics covered:

- Backdoors & Trojan Horses
- Buffer Overflows
- Covering Tracks on Systems
- Covering Tracks on the Network
- Covering Tracks with Steganography
- Denial of Service Attacks
- Exploiting Systems using Netcat
- Format String Attacks
- Gaining Windows data through null sessions
- General Trends in the Hacker Underground
- Incident Handling and the Legal System
- Incident Handling Defined
- Incident Handling Phase 1 Preparation
- Incident Handling Phase 2 Identification
- Incident Handling Phase 3 Containment
- Incident Handling Phase 4 Eradication
- Incident Handling Phase 5 Recovery
- Incident Handling Phase 6 Lessons Learned
- Intellectual Property Incidents
- IP Address Spoofing
- Kernel-Mode Rootkits
- Network Sniffing
- Password Attacks
- Reconnaissance
- Scanning: Network Mapping, Port Scanning, and Passive Fingerprinting
- Scanning: Wardialing and Wireless discovery
- Scanning: Network and Application Vulnerability scanning and tools
- Network Devices (Firewall rules determination, fragmentation, and IDS/IPS evasion)
- Session Hijacking, Tools and Defenses
- Types of Incidents (Espionage, Unauthorized Use, and Insider Attacks)
- User-Mode Rootkits
- Virtual Machine Attacks
- Web Application Attacks
- Worms, Bots & Bot-Nets

For a detailed explanation of each of the topics above, please visit the certification bulletin page:
<http://www.giac.org/certbulletin/gcih.php>

Gold x Silver

Many candidates, who passed through the certification process before mid-2005, were displeased with the current model, a process that does not require the preparation of a paper prior to obtaining the certification.

Previously, there was no such distinction (Gold/Silver). The certification process was as follows: exam registry was done using portal credentials; candidate picked up a subject for development and a technical paper should be prepared to be assessed by SANS, if approved, the candidate went to the next stage:

objective online exam, which could be done at home, using internet connection.

In the end, if the required score was obtained (generally, around 80%), the paper and the score were published on GIAC website with candidate's name and new credentials.

Nowadays, the process is different. To obtain the Gold certification, the candidate must pass the objective exam (multiple choice questions), which is held in a supervised internet environment. Successfully passing this step, grants the candidate Silver credential.

After obtaining Silver certification, if the applicant wishes to challenge the Gold credential, he must submit a paper for evaluation, following the same procedure already described above.

Furthermore, GIAC has recently published another top IS certification program, it's called GSE – GIAC *Certified Security Expert*, which also involves lab exercises in order to get certified. Visit the following URL to read about the requirements to make it (really hard work!):

<http://www.giac.org/certifications/gse.php>

Investment or Cost?

If you pass, it's an investment; otherwise, the investment is increased almost twice as you will try again, don't you?

Currently, the objective exam (challenge exam) needed to achieve Silver certification costs of \$899, whereas the paper submission for Gold certification costs \$299.

Note that if the candidate buys a certification exam in conjunction with a SANS course, exam cost gets lower. For more details about courses and retake policy, visit the following websites:

<http://www.sans.org/security-training.php>,

<http://giac.org/retakes/>

Validity and Recertification Policy

Generally, certifications are valid for 4 years. Passed 2 years after the credentials publication, it is provided an interface at SANS portal where the user can fill out with



evidence information that will be converted into points (CMUs – *Certification Maintenance Units*).

To get CMUs, a list of actions can be taken, including:

- Participation in training, both as a student or as an instructor;
- Contribution to the Information Security community (forums, magazines);
- Publication of books, either as author or a contributor;
- Gold certification achievement, in the case of Silver certification renewal;
- Publication of papers or articles, including books review;
- Professional experience.

Clearly, there was a big change regarding the recertification process, since in the past the only path was going through the whole certification process again.

Note that there is a cost to do it, which can vary between \$199 and \$399 depending on the number of certifications to be renewed in a given period of time. More details about the process of recertification can be found here:

<http://giac.org/certification-renewal/>.

The exam

As any other IT certification exam, the amount of questions can vary, however the subjects are the same. So, if you already have understanding or good hands on experience with the topics covered, all you have to do is become comfortable with the exam approach.

Want to see a good example? Can you imagine now, without trying to read ahead, what are the six stages of the Incident Handling cycle (regarding Computer Security, of course)?

You may enumerate them by using your own words or terms. But to pass, you must know the exam's ones. Try ordering the following terms in time of occurrence: eradication, identification, lessons learned, preparation, containment, recovery. Click here (http://www.sans.org/reading_room/whitepapers/incident/incident-handling-process-small-medium-businesses_1791) to find the answer.

I bet you answered right, maybe just one error (containment – eradication?). That's what I mean: you already know a lot about it, but with practical tasks in mind (maybe part of your daily job).

Exam is mostly made of questions with multiple-choice answers (4 or 5). Depending on the scenario presented, the examiner may ask you to analyze a

piece of code or a log/packet trace, network drawings and so on.

Self-studying or SANS training?

Without any doubt, if you have a chance to participate in a SANS training session or conference, it will be very valuable to your career. It's wrong expecting only technical skills improvement when attending this type of event or courseware.

Any event, whether it's a conference, mentoring session or a 40 hours course, it will provide you more than you initially imagined. Just to clarify, let me list just a few advantages:

- General Networking
- Knowledge about other students' cases and experiences
- Deep and detailed explanation of complex topics
- Complete vision of topics covered and what to focus on (weaknesses)

OK, but this option is not available for most of us, mostly because of the cost. And what about the *hacker spirit* of self learning things? I do prefer this preparation mode.

Facing the challenge

Now, I will assume that you already have decided to make it, that is, you have already registered for the challenge exam and have access to all candidate's resources at SANS portal.



Note that you need to have 109 correct answers (out of 150) questions. The exam engine will immediately stop your session if this score is no more reachable (fear!). But the good news is if you reach the final question, then you can assume that you have correct answered – at least – 108 questions.

Refer to this links to read more about the exam format:

<http://www.giac.org/exams/>,

<http://www.giac.org/feedback.php>

Some tips here will apply for *any* GIAC certification exam based on multiple-choice answers.

Should I bring any books?

The exam is open book, but with internet access restricted to SANS examination portal. Four hours as a timeframe will give you little more than 1 1 minute to answer each question. This means you won't be able to book check all questions, of course.

If you already got a seasoned position in the security industry maybe you can jump ahead. But it may be a good idea to read the following books before the examination, just to have a general idea of the topics covered, especially about the attacks methodology and tools usage.

Also note that Ed Skoudis is the main instructor of the SEC-504 training, so his book may cover a wide range of exam's subjects. Here's the list:

- *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* – By Ed Skoudis and Tom Liston
- *Hacking Exposed: Network Security Secrets and Solutions* – By Stuart McClure, Joel Scambray and George Kurtz

Many books will apply here, as they may have similar contents. After reading them, you can make your own index of interesting and relevant pages. Remember about the index (not the ToC) at the end of the books, they will help you with that.

Cheat sheets are great

Commands parameters and syntax are very well organized in some documents called *cheat sheets*. The idea here is to create your own sheet. But try starting from the available ones:

- What's in Your Folder: Security Cheat Sheets Collection: <http://blog.securitymonks.com/2009/08/15/whats-in-your-folder-security-cheat-sheets/>
- Lenny Zeltser Blog: <http://zeltser.com/cheat-sheets/>; Lenny is also a SANS contributor and instructor.
- SANS material: Google for (*pocket reference OR cheat sheet*) [site:sans.org](http://site.sans.org) – Lots of material here!

Please note that using printing optimization features will help reducing the amount of paper (go green!) and can optimize your searching time.

Increasing your chances

Four or five possible answers give you 20-25 percent of chances to choose the correct one. Sometimes it will be easier eliminating wrong answers instead of trying to find the right one.

It's a good strategy to take a look (not in detail) at the answers before reading the question, which sometimes may have 10+ lines long. Why? You can face something like this:

- NMAP
- Snort
- Nikto
- Nessus
- LANguard

Please note that this is just an EXAMPLE. What can you infer from that? All options except the letter *b* are scanning tools, right? So, the question will be something like *By using the promiscuous mode (...), one of the tools used to capture network traffic is:* Got it?

Another example is:

- X
- Y
- Z
- K
- ~X

There will be a big chance (not 100%, as everything in IS world) of choosing the right answer by shorting your options to letters a and e, as they are opposite (~sign) to each other. Think as an examiner.

So, make sure you have these tips in mind as time is running against you during the exam session.

The tip of gold for silver certification

As you register for the exam challenge, you will be enabled to evaluate your skills by making use of two practice tests. This is the most important phase of your study cycle.

I picked out this piece of text directly from GIAC website:

“GIAC Practice Tests should be used as a study tool to help ensure you have a clear understanding of what to expect from the exam system, as well as the content that will be covered on the examination. Utilizing GIAC Practice Tests significantly improves your chances for success.

Want to know more?

- GIAC website: <http://www.giac.org>
- SANS website: <http://www.sans.org>
- Full brochure about GIAC certs and procedures: <http://www.giac.org/cert-brochure.pdf>
- GIAC code of ethics: <http://www.giac.org/overview/ethics.php>
- GIAC FAQ: <http://www.giac.org/overview/faq.php>

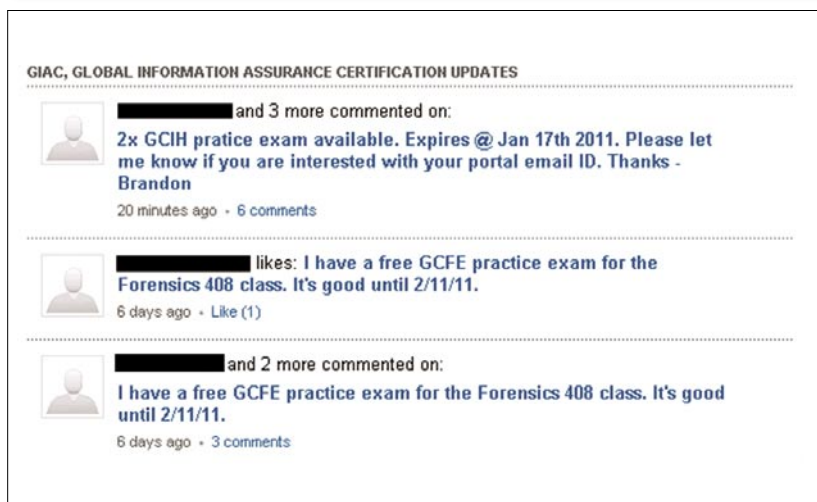


Figure 1. Group members offer practice tests

(...)

Practice test questions are written by the same authors who compose GIAC exam questions, so you can be confident that the range of your results will be similar to the actual exam. During the practice test, each time you choose a wrong answer, you will be shown the correct answer and an explanation that will help to reinforce the subject matter presented in the question.

Source: <http://giac.org/exams/practice.php>
(date of access: 12/17/2010)

So, the first lesson from this is: before you start studying for the exam, try taking – at least – one practice test. That's right. Why reading an entire book without knowing what will be asked during the exam?

The second lesson is: find a way to get as more tests as you can. More tests equal more chances and thus more knowledge about the exam, which will increase your chances. My tip here is to get involved with Infosec communities focused on IS certifications.

Another way is to buy them. Each additional practice test costs \$99.

Do you already have a LinkedIn account? If not, it's time to join it. Here's a little example, when group members are offering practice tests for free. See Figure 1 as an example.

At the beginning of this year, I was happily gifted with one GCFA practice test by a member of a LinkedIn group. It was a great experience, without

any cost but the generosity of one security professional around.

Of course, community engagement is much more than that. I discourage people to join the groups only for getting practice tests, so please adopt this with care.

So you got a Practice Test (remember, two sessions are included in the package). Now what?

Marking the wrong answer gives you the correct one and an explanation. So the final tip is: make it all WRONG! That's it. During the practice session, take notes of your answers. Here's the process:

- Choose your (right) answer, take note;
- Choose an answer that has a great chance of being wrong and mark it;
- Read the entire explanation and take notes, if needed.

Your final score will be terrible, but we are trying to learn. At the end, check your real score (your notes) and see what you will have to focus on.

The challenge exam is very close to the practice test. Please note that this is my approach, this may not work for some people. If this helps, feel free to give me feedbacks (my contacts are below) and good luck in your exam!

ALEXANDRE TEIXEIRA

Alexandre Teixeira works as Security Architect in a private bank based in Sao Paulo, Brazil. He has 10+ years of experience in IS field including many hours of self-studying for earning some IT certifications: GCIH, GCIA, GCUX, SSCP, CCNA, RHCE, LPIC-2, among others. He is also post-graduated in Computer Forensics at Universidade Presbiteriana Mackenzie and blog writer at foren6.wordpress.com.

Twitter: @ateixe

LinkedIn: <http://br.linkedin.com/in/inode>



EMERGING THREATS PRO

the comprehensive ruleset

emergingthreatspro.com

The complete ruleset, focused on malware just like you are.

- Complete Ruleset
- The Best Malware Coverage
- Suricata and Snort Versions
- Cost Effective
- Site Licensing
- Customization

The Emerging Threats Pro is a complete, stand-alone ruleset that draws upon numerous sources of intelligence as well as the EmergingThreats.net open source project to provide up to the minute rules for your network. The rules are updated daily as the threats are identified. No delays, no obfuscated rules.

Emerging Threats Pro will detect more malicious content in your network. Every network has some and most IDS rulesets don't cover it well. The research required to keep up to date on the bots and command and control channels in use is massive. But we've been doing that for ten years now...we've got you covered.

Snort and Suricata versions. We're not tied to any one platform or engine, so we don't have to make the choice not to cover a threat to avoid making a platform perform poorly. We know you can manage your

sensors, so we let you make the decision as to which threats are most important.

Customized Rulesets. Every network is different, and for most organizations all the coverage they need can be found in the Pro ruleset. But for others, the threats they face are very specific and require custom rules to be developed specifically to meet those needs. The in-house Pro research team specializes in creating custom rulesets and working with clients to create optimum network security.

We offer site licensing discounts for larger sensor networks. We know you need a predictable cost per year and nobody wants to spend time counting sensors. Let us know about how many sensors you have and we will work out a competitive price you can rely on.

If you need comprehensive coverage for the vulnerabilities and malware that threaten your network then Emerging Threats Pro is the ruleset for you.

	Emerging Threats	Emerging Threats Pro	The Other Guys
Suricata Support	YES	YES	—
Snort 2.4 to Current Support	YES	YES	—
Serious About Malware	YES	YES	—
CnC/Data Exfiltration Focus	YES	YES	—
Community Intel/Support	YES	YES	—
Hardware/Platform Neutral	YES	YES	—
Load Rated Rulesets	YES	YES	—
Complete Major Vuln Coverage	—	YES	YES
Known Bad IP Lists	—	YES	—
IP Reputation Support	—	YES	—
Full Time Research Team	—	YES	YES
Research Partnerships	—	YES	YES
24x7 Email Support	—	YES	—
24x7 Phone Support	—	YES	—
Custom Rulesets	—	YES	—
Other Formats	—	YES	—
Site Licensing	—	YES	YES

Certification Smart?

A job in computers is a position of experience; if you don't have experience the next best thing is a computer certification.

Starting at the Top

Most animals are born with ninety percent of their knowledge through instinct and acquire the other ten percent learning from their environment; we are not one of those creatures. No human is born with working job experience; with the slight exception of politicians. Everyone that has ever taken a job, at least one time in their career has done so without experience. So worrying whether or not you can get a job with no experience is foolish; we all start out the same. What is equally foolish is to worry about not being hired at a high paying salary and at the top position with no experience; because you're going to be. Many people have been convinced that if they get a degree or certain certifications they will obtain a top-paying job in a company of their choosing. *God bless your naive little souls.* I am not saying that it is not possible. With the *right* last name and from the *right* school, you could be president of the United States, but you had better have great connections, because a corporation is not as likely to start you at the top, as an elected office will. Even Bill Gates and Paul Allen started at the bottom. I mean, granted they started from a higher altitude, but it was still a bottom position. Because I hear so many IT managers complain about a young, just out of school candidate, or someone with a boot camp certification, enter an interview with a list of demands, I feel it is an important issue to address. I even interviewed a young man one time, with no experience, first time job. When I asked if he had any questions, he replied that he wanted a new laptop, a credit card, and asked about a company car. I saved him the embarrassment of failing the company drug test.

Overlooking Inexperience

If you have experience, a certification tells your potential employer; *I am serious enough about my career to take*

the study of my position as many levels as I can. If you don't have experience, a computer certification tells your potential employer; *I have studied the best I can on my own to prepare myself for a position with our company.*

Product knowledge is the key to overcoming lack of experience. Computer programs create computer careers. Software companies create programmers, network administrators, SQL programmers, and router administrators. Inexperience is secondary if you know the product. In other words, product knowledge is an acceptable replacement for experience. Product knowledge can be described as knowing an operating system, a programming language, a router OS, or an SQL language inside and out. While studying C++, I was talking to a Vice President at Microsoft, and he asked me how well I knew C++? He needed C++ programmer's right then. He knew I had no programming experience but he was willing to overlook it, if I was eager and knowledgeable enough to use the product. I was not, and subsequently he did not pursue it any further. You can also gain knowledge from self-experience. (I know; self-experience sounds a lot like what lonely people do), but in this context, self-experience can be setting up networks and servers at home or in a lab and obtaining computer certifications.

Product knowledge is the most important tool you can have when looking for a job, whether you are a seasoned professional or just starting out. A degree in computer science is a nice adornment on a resume, but it does little to help you get a job without some type of software knowledge. Every time that you install a network operating system, create a user account, or set up a DNS, DHCP, WINS, or Print Server, you have that knowledge to use at a later time.

Beware of Promises from Certification Schools

There are many schools out there that promise a quick job if you earn a certain set of certifications.

You must ask yourself how many jobs there are in the world that starts out with an inexperienced worker at the top, not very many.

Look at the employment section of your local paper and tell me how many legitimate jobs are listed that state:

Wanted: no experience necessary. With only 6 weeks of education to pass a test, we will hire you to manage all the servers, workstations, and network in our company. You only need to apply with a certification and a note from your instructor that states you were a good test taker.

Be cautious when people tell you what certifications can do. The certification freight train has already left the station. A great deal of money has been made by companies that promised a computer certification would get you a great job, and because of this, they saturated the market with unskilled, highly certified workers that cannot find work.

Without work experience, certifications only compliment your actual product knowledge. Most IT job interviews include a technical interview that includes very specific questions about your product knowledge. If you cannot answer basic questions or perform specific tasks, you will not pass the interview. I know network managers who will end the interview immediately if someone answers technical questions with, *I'm certified in it, aren't I?* Very few people are capable of faking a technical interview.

During an interview, you should tell the interviewer just what you know, how you earned it, *that you have done all you can to teach yourself, and now you are looking for an opportunity to learn first hand.* Network Managers and IT Directors are so gun shy, that if you cannot answer their questions, then this is the only answer they want to hear. A certification will not hold up in a job interview, if you did not retain the data necessary to pass the course.

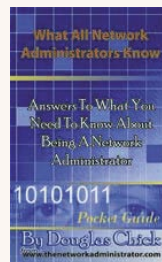
If reading this makes you nervous, you need to go back to the books and set up as many different networks as you can. At the bare minimum, you must at least be able to do what you have listed on your resume. If self-experience is the only thing you can offer, you had better be good at it. Network Analyst, System Analyst, and Helpdesk Technicians are all positions that are available without prior experience. These positions give you an opportunity to gain first

Douglas Chick. MCP MCSE CCNA

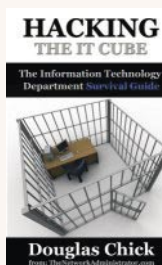
Creator of www.TheNetworkAdministrator.com

Author of:

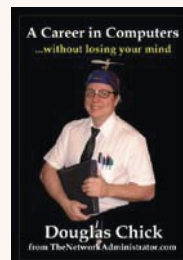
What All Network Administrators Know ISBN: 0974463000



Hacking the IT Cube: The Information Technology Survival Guide ISBN: 0974463027



A Career in Computers...without losing your MIND ISBN: 0974463035



hand experience on a network server, workstations, and even in the server room.

DOUGLAS CHICK

Douglas Chick is a Director of Information Systems for a large company in the Orlando FL area. Although he introduces himself as a Network Engineer/Administrator. As with many computer people, Doug holds an MCSE and CCNA certification. Doug first became known on the Internet in May of 2000 for a series of articles about Microsoft retiring the NT4 MCSE that were published on over 30 Internet Magazines. With his humor and insightful look into the world on computer professionals, he receives a great deal of attention from other computer professionals around the world. And is proud to admit that less than one percent are in response for his many typo's and mis-spellings. For more visit: www.TheNetworkAdministrator.com.

In the next issue of **HAKING** magazine:

- **The Best Way to Learn and Apply Cryptography**
- **Secure Env for PT**
- **Identity Thefts**

Available on February 28th