Talking with Erick Hjelmvik

About Network Miner

Blackhat Arsenal 2012

In This Issue

Book Review Kevin Mitnick

Septembre Tools Wrap-Up
Is this a yet new magazine that addresses information security?

No. it's not.

Or at least, I want to avoid falling into this trap. I realized that there is enough various and focused IT magazines but still nothing concrete about security tools.

Perfect Timing, because I’ve invested in such task for years now through ToolsWatch.org to share and discover with community the latest infosec tools releases & updates.

So I felt the need to provide to my friends & fellas a monthly (or quarterly depends on a volunteers and effort equation to be solved) dedicated pentest tools magazine.

Similarly, this is another wonderful opportunity to meet few hackers and allow them to talk about their life & times. Because Some of them are not able to attend events & conferences to demontrate their work.

In each issue, I (we) will take time to dissect a specific tool, make an interview, write about a book and highlight the latest updates. You are also free to contribute and share your experience in infosec tools. Any help is appreciated to beautify this new mag.

Keep in mind, this is the Magazine Pilot and there is no strategy defined yet. Everything should be reviewed thanks to your comments and suggestions. So, do not hesitate a second to write me.

What else ? Great news !! ToolsWatch is selected for the 4th session to animate the Blackhat Arsenal at Abu Dhabi.

The CFT is still open and you can submit your tool via netpeas website. So, give your tool a chance to be recognized.
Mitnick at the Arsenal Tools

Archive with released tools, pictures and more at

http://www.toolswatch.org/blackhat-arsenal-us-2012-archive/

Interviews archives at

http://www.youtube.com/user/ToolsWatch/videos?query=Blackhat+USA+2012
Georgia Weidman - The SPF Geek Girl during Interview Session.

Get Ready for the next coming session at Abu Dhabi Emirates

http://www.blackhat.com

R.Harrando (@netpeas). One of the ToolsWatch & Arsenal dude

Kill me if you meet Jayson without his popular 20oz Pepsi Diet ;)

The Arsenal Effect
Digital age version of the Jack Kerouac’s «On The Road»

It is with a slight sadness that I have finished reading the latest Kevin Mitnick Best Seller “Ghost In the Wires”.

I think it is needless to introduce Kevin David Mitnick to the mere mortals. Just his name is synonymous of the legend built around him. Nevertheless, for those who believed at least knew him through the “rumors”, I recommend you warmly to read “Ghost in The Wires”.

The book is a kinda of confession written with a great sincerity.

Indeed, the book is a leap into the past which traces the life of a guy who just wanted to understand how things work out. It must be put in the context of the earlier years when Mitnick began to take an interest in Computers Industry. This was the beginning of Hacking and everything was still to be invented: techniques, methods, exploits and tools. Because there was almost nothing except a hacker’s mind presence to overcome all obstacles to achieve tremendous challenges.

If you see all today's so-called-hacking-crappy-movies, you couldn't even think that “Ghost in The Wires” goes beyond Hollywood imagination. I’ve repeatedly read few passages because I found them awesomely fantastic.

This is the story of a man who dealt with Advanced Operating Systems, Phones phreaking, Social Engineering Tricks to go to the depth of companies lingo looking for the reliable information.

I insist on word “Information”. No harm, no data deleted and no financial motivation.

Why was he doing that? That's the question; The FBI was always asking and obviously driving them crazy & mad.

The trick was all that easy: The Willingness to Learn & To Discover. Mitnick was a kind of a digital age version of Jack Kerouac.

Nowadays, an intrusion that seems common and somehow easy to perform was a great challenge at the old days.

There was no Metasploit, no Google Hacking and no ExploitDB. You wanna something, roll up your sleeves and dig for it.

When the VoIP hacking techniques could be a way to forge a fake identity, at the time «The Condor» (Mitnick alias) had to reprogram phones by modifying the source code.

How on earth? This is a long story of almost 400 pages.
The Condor reborns from the ash

All through the book, I have cursed the FBI. I damned the way they hunted & chased a man treating him as the worst criminal. One of the reasons they have highlighted and claimed was «Whistling in a Phone to start a nuclear war». I’m still rolling up my eyes !!

Kevin finally gave his side of the story about the Takedown affair. You will learn everything you need and stop asking the same boring question «Was the Movie based on real events ?». No, it wasn’t. Read the book :)

Hollywood and others made benefits from this business and earn some dough while Kevin was confined in a prison for wrongful and unfounded reasons !!

It was the great Epic Hacking days when everything was still to be invented as i mentioned before. Actually, almost all intrusions are not stunning because the systems are interoperable, applications are more and more vulnerable and the humans are talking too much via their social networks. The perfect conditions for a successful & easy intrusions.

If the word Hacker should have another meaning, I’ll call it Mitnick.

The tide is finally turning, and Mitnick is now one of the most prominent and outstanding security consultant in the world.

His yesterday’s detractors are paying the price high to see him giving talks & keynotes and ironically taking a picture with him !

http://www.mitnicksecurity.com/
1 million iOS device IDs

One million unique device identifiers (UDIDs) from iOS devices have been posted online by hacking group Antisec, who claimed the UDIDs came from an FBI-owned laptop. The group published a file containing the UDIDs—as well as push notification tokens, device names, and more—on Monday evening, promising that there are plenty more entries where that came from. Antisec claims the original file contained roughly 12 million UDID entries—some with very personal data attached, such as full names, cell numbers, and home addresses.

Read more on Arstechnica Website

Zero-Day Season is Not Over Yet

New Java zero-day vulnerability has been spotted in the wild. We have seen this unpatched exploit being used in limited targeted attacks. Most of the recent Java run-time environments i.e., JRE 1.7x are vulnerable. In my lab environment, I was able to successfully exploit my test machine against latest version of FireFox with JRE version 1.7 update 6 installed.

Read more on FireEye Blog
http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html

New Metasploit 0day exploit for IE 7, 8 and 9

We have some Metasploit freshness for you today: A new zero-day exploit for Internet Explorer 7, 8, and 9 on Windows XP, Vista and 7. Computers can get compromised simply by visiting a malicious website, which gives the attacker the same privileges as the current user. Since Microsoft has not released a patch for this vulnerability yet, Internet users are strongly advised to switch to other browsers, such as Chrome or Firefox, until a security update becomes available. The exploit had already been used by malicious attackers in the wild before it was published in Metasploit.

Read more on SecurityStreet Blog

Events may change

Those events are not published in real time. Some could be outdated. Changes may also occur meanwhile. So, there is no need to fire me email poking about this ;). Besides, you can still follow me at @toolswatch and get informed in realtime because I myself follow great reliable infosec people.
Bulb Security LLC was founded in January 2012 by information security professional Georgia Weidman as a side venture for her research and security training. Bulb Security is here to provide your organization with the personal attention to reach your security goals. We provide personalized security training, security assessments, and research and development.

CEO G. Weidman. [http://www.bulbsecurity.com](http://www.bulbsecurity.com)

Mkit is an IT Argentinian Security Company that specializes in Penetration Testing, Vulnerability Assessments and Security training for private companies and public organizations.

Mkit also provides consulting services regarding application development security and code review.


Vega is an open source platform to test the security of web applications. Vega can help you find and validate SQL Injections, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities.

Vega is developed by an Open Source Security Canadian Company SubGraph.

CEO D. Mirza [http://subgraph.com](http://subgraph.com)

Since 2005, Stach & Liu has provided security consulting services to the Fortune 1000, high-tech startups, and financial institutions all over the world. Our mission is to help companies secure their networks and applications, and our core services include: security assessments; policy and compliance consulting; and strategic security program development.

Managing Partner F. Brown [http://www.stachliu.com](http://www.stachliu.com)
Could you introduce yourself to ToolsWatch Community?

Sure; my name is Erik Hjelmvik, I live in Sweden and I'm the creator of the network forensics tool NetworkMiner. I'm also co-founder of the network security company Netresec.

How many years have you been in the security industry?

I started out in the security industry in 2005, while working with R&D in control system security at a large electric utility company.

What motivates you to release networkminer (How comes this awesome idea?)

NetworkMiner started out as a fairly simple tool that parsed pcap files and displayed a list of all the hosts that had communicated on the network.

I built the first version back in the days when I was working with security for industrial control systems, since I wanted to see what was on the network without doing any active scanning.

This passive host inventory tool has since then evolved into a solid network forensics tool that can do stuff like extracting files, passwords, chat messages, emails etc. from sniffed network traffic.

What are the support of SCADA protocols?

SCADA systems are made up of multiple proprietary embedded systems spread across a large geographical area, such as a power grid. These embedded systems typically have very poor security logging, which makes it difficult to analyze hacked SCADA systems. Because of this we today see utility companies starting to sniff the network traffic in their control system networks.

This makes a lot of sense since these types of networks typically carry unencrypted protocols and have low traffic volumes. The problem is, of course, to understand the captured traffic, which is where NetworkMiner comes in.

What I wanna do is to make it easier to do forensic analysis of a hacked SCADA system, or industrial control system in general, by providing an easy understandable view of the commands sent on the control system network.

Could you tell us a little about the support of SCADA protocols?

What are the plans for the next coming release?

There are many new features to be implemented, but it is not yet decided what will be in the next release. I'm always open for suggestions from the community though.

Besides, I hope to have implemented more SCADA protocols and SMB2 in a not to distant release.

Do you plan to join us the BlackHat Arsenal?

Absolutely, it would be fun to do a demo at the BlackHat Arsenal some day!
Besides hacking with NetworkMiner. What are you doing in your spare time?

Lots of stuff, like incident response and research in traffic classification.
I'm also developing a tool called CapLoader, which is built for working with large amounts of captured traffic.
I also try to spend as much time as I can together with my family.

What is your Favorite Security Tools?

A few tools I really like are: argus, tcpflow, ngrep, scapy, wireshark and of course tshark.
I also love the Linux distro “Security Onion” and the FreeBSD live CD “HeX”

Erik, I really appreciate talking with you (virtually), we’ll keep an eye on you :)

Hey thanks guys, It's always good to know that you're keeping an eye on NetworkMiner!

THANK YOU ERIK & KEEP UP THE AWESOME WORK

NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows. NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.

NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.

NetworkMiner collects data (such as forensic evidence) about hosts on the network rather than to collect data regarding the traffic on the network. The main user interface view is host centric (information grouped per host) rather than packet centric (information showed as a list of packets/frames).

NetworkMiner has, since the first release in 2007, become popular tool among incident response teams as well as law enforcement.

NetworkMiner is today used by companies and organizations all over the world.

Coverage of the latest NetworkMiner Releases could be found here
http://www.toolswatch.org/?s=networkminer

Feature requests can be submitted via SourceForge
http://sourceforge.net/tracker/?group_id=189429&atid=929293

Netresec is an independent software vendor with focus on the network security field. We specialize in software for network forensics and analysis of network traffic.

Our most well known product is NetworkMiner, which is available in a professional as well as open source version. We also develop and maintain other software tools, such as RawCap, SplitCap (a tool for splitting pcap files into one per session) and SPID (a "Port Independent Protocol Identification" tool for identifying the application layer protocol in a TCP or UDP session).
Nikhil Mittal is a hacker, info sec researcher and enthusiast. His area of interest includes penetration testing, attack research, defence strategies and post exploitation research. He has many years of experience in Penetration Testing of many Government Organizations of India and other global corporate giants.

Principal Hacker N. Mittal http://labofapenetrationtester.blogspot.fr

Peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not. The aim of this tool is to provide all the necessary components that a security researcher could need in a PDF analysis without using 3 or 4 tools to make all the tasks.

J.Miguel Esparza http://eternal-todo.com

Denim Group is a strong contributor to the larger application security community, and has been involved with the Open Web Application Security Project (OWASP) since shortly after its inception. Additionally, Denim Group was ranked in Inc. Magazine's 5,000 Fastest-Growing Private Companies in America in 2008 and 2009. ThreadFix is developed and maintained by Denim Group

Principal D.Cornell http://www.denimgroup.com
**Burp Suite v1.5rc2 released**
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and...

**CAINE The Computer Aided Investigative Environment 3.0 – QUASAR is out**
CAINE (Computer Aided INvestigative Environment) is an Italian GNU/Linux live distribution created as a project of Digital Forensics. Currently the project manager is Nanni Bassetti ...

**Tackling AETs with “Evader” The First-Ever EPS (Evasion Prevention System)**
Evader is designed to test your organization’s network security devices against Advanced Evasion Techniques that are increasingly used in sophisticated and targeted cyber attacks ...

**ExploitShield Browser Edition v0.7 released – The anti-exploit solution –**
ExploitShield protects users where traditional security measures fail. It consists of an innovative patent-pending application shielding technology that prevents malicious exploits from compromising...

**SinFP3 v1.00 The operating system fingerprinting tool released**
sinfp3.pl is more than a passive and active OS fingerprinting tool. Some examples below showing ...

**Cuckoo Sandbox v0.4.2 available (Support for VMware added)**
Cuckoo Sandbox is an Open Source software for automating analysis of suspicious files. To do so it makes use of custom components that monitor the behavior of the malicious processes while running in...

**ERPScan’s SAP Pentesting Tool v0.6 updated with 31 new modules**
ERPScan’s SAP Pentesting Tool is a freeware tool that is intended for penetration testers and security officers for vulnerability assessment of SAP...

**dSploit – An Android network penetration suite released**
dSploit is an Android network analysis and penetration suite which aims to offer to IT security experts/geeks the most complete and advanced professional toolkit to perform network security...

**hashkill v0.3.0 released**
hashkill is an open-source password recovery tool. It can recover about 45 types of passwords using different types of attacks. It has several nice features (sessions save/restore, multihash lists,...
Evil Maid CHKDSK: Steal users password with fake CHKDSK
This is a simple 512-byte MBR program that pretends to be Windows CHKDSK. It asks the user for a password, writes that password back to the media it booted from, renders that media unbootable...

AppSec Labs iNalyzer – iOS penetration testing framework
AppSec Labs iNalyzer is a framework for manipulating iOS applications, tampering with parameters and methods; no sources needed! AppSec Labs iNalyzer targets closed applications...

Onapsis SAP Bizploit v1.50-rc1 released
Bizploit is the first opensource ERP Penetration Testing framework. Developed by the Onapsis Research Labs, Bizploit assists security professionals in the discovery, exploration, vulnerability...

The Social-Engineer Toolkit (SET) v4.0.1 “Balls of Steel” in the wild
The Social-Engineer Toolkit (SET) version 4.0 codename “Balls of Steel” is officially available for public consumption. This version is the collection of several months of development and over 50 new...

BlackHole Exploit Kit 2.0 released & updated with new exploits
The Blackhole exploit kit is currently the most popular web threat, where 28% of all web threats detected by Sophos and 91% by AVG are due to this exploit kit...

Consider EMET (Enhanced Mitigation Experience Toolkit) to mitigate the IE 0day Vulnerability
From Microsoft A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has been deleted or has not been properly allocated...

Nikto v2.1.5 released
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6500 potentially dangerous files/CGIs...

Skipfish v2.09b Released
Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes..

ipv6mon v1.0 – Networks’ Address Monitoring Daemon Released
ipv6mon is a tool meant for monitoring IPv6 address usage on a local network. It is meant to be particularly useful in networks that employ IPv6 Stateless Address Auto-Configuration.
OSSEC v2.7 Beta-0 Released
OSSEC is an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active...

NOVA the Network Obfuscation and Virtualized Anti-Reconnaissance v12.6 available
The Network Obfuscation and Virtualized Anti-Reconnaissance (Nova) system is an open-source software tool developed to detect network based reconnaissance efforts, to deny the attacker access to real..

OpenDNSSEC 1.4.0b1 released
OpenDNSSEC was created as an open-source turn-key solution for DNSSEC. It secures zone data just before it is published in an authoritative name server. Why DNSSEC? Many internet protocol hinge on...

NWebsec 1.0.3 The Security library for ASP.NET
NWebsec is a security library for ASP.NET applications. It's built on the philosophy that security should be simple and maintainable. The current version includes a configurable...

Pentoo 2012.0 Beta2 Release
Pentoo is a security-focused livecd based on Gentoo It's basically a gentoo install with lots of customized tools, customized kernel, and much more. Here is a non-exhaustive list of the features...

CodeSonar® Static Analysis Tool for C & C++ released
GrammaTech makes the deepest static analysis tool for C and C++, for organizations that have zero-tolerance for defects and vulnerabilities. CodeSonar® is GrammaTech's flagship product, which...

Mercury The Android Assessment framework v1.1 is Released
A free framework for bug hunters to find vulnerabilities, write proof-of-concept exploits and play in Android. Use dynamic analysis on Android applications and devices for quicker security...

CloudShark Analyze your Capture Files in the Cloud
CloudShark is designed to work with your existing capture, analysis, and trouble-ticket tools and systems. The CloudShark API makes it simple and efficient to upload, tag, and manage capture files.

Network Security Toolkit v2.16.0-4104 in the wild
The Network Security Toolkit is bootable ISO live CD/DVD (NST Live) is based on Fedora...

360-FAAR Firewall Analysis Audit Repair v0.2.6 released
360-FAAR (Firewall Analysis Audit and Repair) is an offline, command line, Perl firewall policy manipulation tool to filter, compare to logs, merge, translate and output firewall commands for new...

Suricata v1.4beta1 released
Suricata is a rule-based ID/PS engine that utilises externally developed rule sets to monitor network traffic and provide alerts to the system administrator when suspicious events occur. Designed to...

Netsparker CE 2.3 released
Netsparker Community Edition is a SQL Injection Scanner. It's a free edition of our web vulnerability scanner for the community so you can start securing your website now. It's user friendly, fast,...