

# PenTest **EXTRA** *magazine*

Vol.2 No.2 Monthly ISSN 2084-1116

Issue 02/2012(06) February

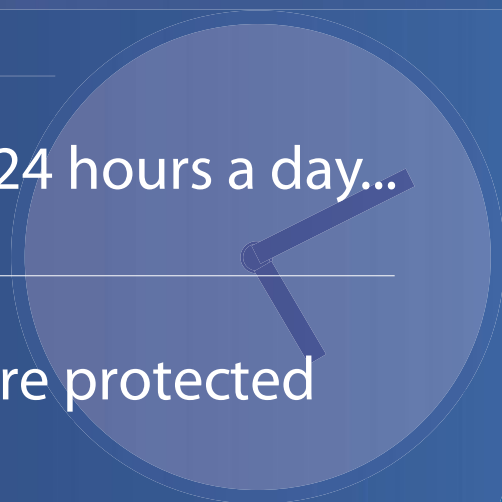
## **Social Engineering:**

**A FORMAL APPROACH  
TO EXPLOIT HUMAN INTELLIGENCE**

**INTERVIEW WITH MARSEL NIZAMUTDINOV**  
**FOOT PRINTING – FINDING YOUR TARGET**  
**SESSION HIJACKING**  
**QUALYS VIRTUAL SCANNER**  
**NT0 SQL INVADER**

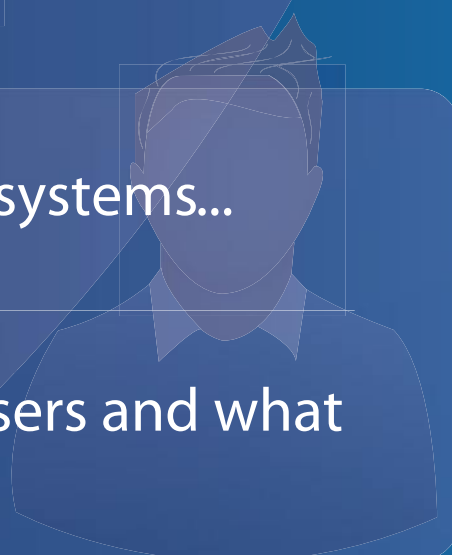
# Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...



# Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.



## **Just After Valentine's Day**

February is a beautiful month full of love and happiness. Just yesterday was Valentine's Day. Most of you are possessed with love but you have to stay focused. You can be hacked anytime. In this issue we provide useful information regarding social engineering, foot printing, session hijacking, SQL injection or Cross-Site Request Forgery. Let's look inside.

First article is on social engineering. Shakeel Ali has briefly discussed the psychological human behavior to help understand the science behind social engineering attacks, the generic attack process and methods with realistic examples, and precisely explained two well-know technology assisted tools to carry out attacks in an automated fashion. „A Formal Approach to Exploit Human Intelligence” is on page 06.

Next one provides valuable information, regarding foot printing. An intriguing title „Finding your target” shows some of the steps, tips and tricks that pentesters and hackers alike use when they start an engagement. Jump to page 10 and find out more.

Nikhil Srivastava elaborates on the issue of unauthorized access to information or services in a computer system through Session Hijacking. He mentions that the attacker does not need to find out your username and password. His target might be your session. The article can be read on page 16.

Sow Ching Shiong describes usage of NTO SQL Invader which is a SQL injection exploitation tool. It gives the ability to quickly and easily exploit or demonstrate SQL injection vulnerabilities in Web applications. If you want to learn more, go to page 26.

Cross-Site Request Forgery seems to be a frequently disregarded subject. Eugene Dokukin claims that almost all network devices are vulnerable to CSRF due to misunderstanding of this threat by developers. Therefore, attackers can conduct remote CSRF attacks on network devices, such as routers, Wi-Fi Access Points and others to do many nasty things about which you can read on page 30.

What follows is an article devoted to web application security. Matt Parsons discusses three the most common and devastating software security vulnerabilities. He looks at SQL injection, Cross Site Scripting and Cross Site Request Forgery as an attacker and offers you more secure software for your enterprise. „Web application security vulnerabilities have been prevalent the last decade” can be found on page 34.

Traditionally, we have prepared for you an interview. Our guest is Marsel Nizamutdinov. He is a Head of Research & Development Department at High-Tech Bridge SA and the author of „Hacker Web Exploitation Uncovered”. Full interview is available on page 44.

We are happy to present to you technically advanced review of Qualys Virtual Scanner. This new scanner is an alternative to Qualys' scanner appliance already in popular use by security departments and consultants and will run in as a virtual machine on VMware or VirtualBox software on a server or laptop/desktop. Jump to page 48 and read Scott Christie review.

We hope you will find this issue of PenTest Extra interesting and useful. Thank you all for your great support and invaluable help.

Enjoy reading!  
Krzysztof Marczyk  
&Pentest Team

# PenTest magazine

## TEAM

**Editor:** Krzysztof Marczyk  
krzysztof.marczyk@software.com.pl

**Associate Editor:** Aby Rao

**Betatesters / Proofreaders:** Massimo Buso, Daniel Distler, Alexandre Lacan, Michael Munty, Davide Quarta, Jonathan Ringler, Johan Snyman, Jeff Weaver, Edward Werzyn, Daniel Wood

**Senior Consultant/Publisher:** Pawel Marciniak

**CEO:** Ewa Dudzic  
ewa.dudzic@software.com.pl


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

**Production Director:** Andrzej Kuca  
andrzej.kuca@software.com.pl

**Marketing Director:** Ewa Dudzic  
ewa.dudzic@software.com.pl

**Publisher:** Software Press Sp. z o.o. SK  
02-682 Warszawa, ul. Bokszerska 1  
Phone: 1 917 338 3631  
www.pentestmag.com

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](http://smartdraw.com) program by  SmartDraw

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.

## SOCIAL ENGINEERING

### 06 A Formal Approach to Exploit Human Intelligence

by Shakeel Ali

There is no formal procedure or process for social engineering attack till date. It all depends on the given situation and how would you draw the steps to initiate an attack against your target. Some of the most common steps taken are intelligence gathering, identifying vulnerable points, planning the attack, and execution. Each of these steps should remain consistent in the definite order and data collected upon their successive completion.

## FOOT PRINTING

### 10 Finding your target

by Willem Mouton

Dumpster diving, if you are up for it and have physical access to the target, means sifting through trash to get useful information, but in recent times social media can provide us with even more. Sites like LinkedIn, Facebook and Twitter can provide you with lists of employees, projects that the organization is involved with and perhaps even information about third party products and suppliers that are in use.

## NETWORK SECURITY

### 14 Session Hijacking

by Nikhil Srivastava

Session hijacking, also known as TCP session hijacking, allows a user to take control over a Web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network.

### 26 CSRF Attacks on network devices

by Eugene Dokukin

The first attack it's to turn on the remote access to the admin panel (it's off by default), to allow remote attacker to access the admin panel from the Internet and change all required settings (and this attack can be conducted in one request). Network devices which have an option to allow remote access and have CSRF vulnerabilities can be attacked in such way.



## SQL INJECTION

### 30 NTO SQL Invader by Sow Ching Shiong

NTO SQL Invader is a SQL injection exploitation tool. It gives the ability to quickly and easily exploit or demonstrate SQL injection vulnerabilities in Web applications. With a few simple clicks, a penetration tester will be able to exploit a vulnerability to view the list of records, tables and user accounts of the back-end database.

## WEB APPLICATION SECURITY

### 34 Web application security vulnerabilities have been prevalent the last decade by Matt Parsons

The main issue with SQL injection is that the programmer is dynamically generating SQL queries and not validating the input. The best way to prevent this attack is to validate all input with white list validation, use least privilege and use prepared statements or stored procedures. In Java EE it is best to use `PreparedStatement()` or in .NET use `SqlCommand()`.

## INTERVIEW

### 44 Interview with Marsel Nizamutdinov by PenTest Team

Marsel Nizamutdinov is a Head of Research & Development Department at High-Tech Bridge SA, web application security expert and the author of „Hacker Web Exploitation Uncovered” (2005).

## REVIEW

### 48 Qualys Virtual Scanner by Scott Christie

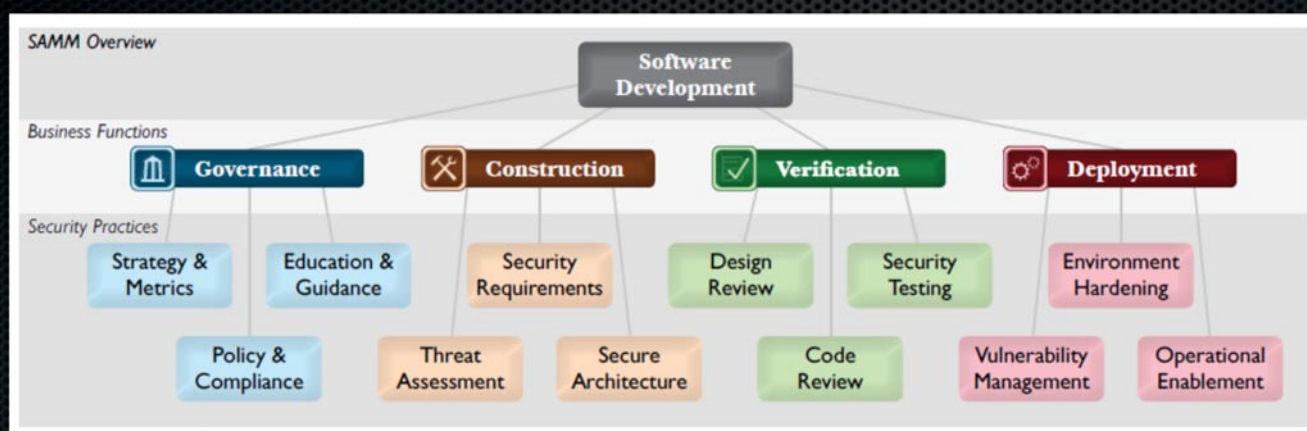
The setup of a new Virtual Scanner is not difficult. For existing Qualys customers, a change must be made to the service account to allow for the Virtual Scanners. During the change and previously owned physical scanner appliances must be online or else the physical devices can be irreparably dropped from the service account and will have to be returned to Qualys. After the account change, users will notice new menu options for the provision and download of Virtual Scanner appliances.

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



# OWASP Foundation

*“We help protect critical infrastructure one byte at a time”*



- 140+ Checklists, tools & guidance
- 150 Local chapters
- 20,000 builders, breakers and defenders
- Citations: **NSA, DHS, PCI, NIST, FFIEC, CSA, CIS, DISA, ENISA** and more..

Learn More: <http://www.owasp.org>

# A Formal Approach

## to Exploit Human Intelligence

In today's highly secured corporate environment, it is quite hard to find vulnerable systems or applications which would allow pen-tester to enter his footsteps into restricted zones. Therefore, the use of "social engineering" techniques come into practice for obtaining privileged access by exploiting human vulnerabilities.

It is a vital part of penetration testing process which allows you to wrap yourself with an art of deception when there is a lack of information available about the target. Since the humans are the weakest link in any organization's security defenses, it is the most vulnerable layer which can be exploited by various social engineering methods. These methods follow core principles and practices executed by social engineer in order to extract confidential information by manipulating human's neuro-linguistic system. The science of social engineering brings powerful weapon for penetration tester to evaluate the integrity of the organization employees and identify their social and professional weaknesses which may otherwise hard to determine. It is also an interesting fact that the practice of social engineering has been adopted by range of professionals in their daily life. These include business partners, recruiters, sales agents, telemarketers, identity thieves, private detectives, disgruntled employees, government spies and many other entities. The influence and direction under which you execute the social engineering tactics is what proves the rate of success. In this article, I have briefly discussed the psychological behavior of a human to help understand the science behind social engineering attacks, the generic attack process and methods with realistic examples, and precisely explained two well-know technology assisted tools to carry out attacks in an automated fashion.

### Human Psychological Behavior

The activity of a human brain depends on number of senses (hear, taste, sight, touch, smell, pain, temperature, direction, balance and acceleration) which controls the state of perception to the reality. These senses play an important role to in shaping the way we see the world. In social engineering world, any information extracted through eye movements (blinking or squinting), facial expressions (happiness, sadness, fear, anger, or surprise), body posture, gestures or feelings (anxiety, shame, or depression) of the target adds greater likelihood of success in acquisition of classified information. On the other side, effective communication techniques do result in obtaining meaningful data. The most common techniques are, interview and interrogation. Each one of these relies on other common factors like environment, knowledge, and controlling the frame of communication of a target. These factors build an important prototype for the social engineer to follow and achieve his ultimate goals. Remember that social engineering is all about building *trust* relationship. If you are able to win the trust of your target then you are successful otherwise you are most likely to fail in your mission.

### Attack Process

There is no formal procedure or process for social engineering attack till date. It all depends on the given

situation and how would you draw the steps to initiate an attack against your target. Some of the most common steps taken are intelligence gathering, identifying vulnerable points, planning the attack, and execution. Each of these steps should remain consistent in the definite order and data collected upon their successive completion. This would increase the proximity to divulge information about your target. This defined attack process of social engineering as shown in Figure 1 will improve the productivity and competitiveness of penetration tester to fulfill the given assessment.

## Intelligence Gathering

Selecting the best target to achieve your motives is the most important step in social engineering. By using various resources and intelligence, one can gather information about the organization. For instance, harvesting the corporate email addresses, collecting personal information about the employees, attending the corporate business events and conferences, identifying third-party software or hardware being used, and walk through online social media networks to gather information about employees activities. This all constitute a strong base for penetration tester to select the most valuable target (insider) for social engineering attack. The more accurate the target is, the more effective is the result.

## Identifying Vulnerable Points

Gaining the confidence and trust of your selected target is the second important step in social engineering. This can be achieved by various means, such as creating social relationship, friendliness, affection, brotherhood, sisterhood, fellowship, sportsmanship and philanthropy. It is very crucial to maintain your concealment and coyness throughout the attack process. Such that, gaining access to sensitive information held within your target should not alert him/her about your findings. Once you identified all the possible entry points, it is now time to think about targeted attack methods which would allow you to gain access to confidential information or restricted area. Remember that each successive step in social engineering attack process depends on the previous output.

## Planning The Attack

By observing the vulnerable entry points, one can determine the attack path and method. The attack can be carried out actively (face-to-face with target) or passively (by means of electronic-assisted technology such as email or phone). Based on the common factors contributing to social engineering criteria I have divided these methods into five different categories. This would

benefit penetration tester to understand, socialize and prepare the target for final engagement. Each of these methods has its unique role in the social engineering field. It is, however, necessary to understand the psychological factors which form the basis of these attack methods. The more efficient and robust your method is, the more likelihood for the success. Each method has been described with real-world example to provide more detailed direction.

## Impersonation

Convincing and pretending to be in someone else's shoes is what known as impersonation. Let's take a well-know example of *phishing* attack where an unaware corporate employee (John) received an email asking to confirm bank account information. It started when the penetration tester (Caesar) harvest the web results by executing various search queries and got John's email address. Through active intelligence and monitoring, Caesar was able to find his target's bank. Caesar then prepared the scam login page which looks and functions exactly the same as original bank website. By using the technical skills and available tools, Caesar sent a formalized email to John which seems to be originated from the bank's domain asking John to visit a link in order to confirm bank account information. This whole scenario can also be replaced by human-assisted scamming through other electronic means. Such as, calling the target directly and pretends to be the bank administrator with false identity.

## Reciprocation

Exchanging a favor to gain mutual advantage is known as reciprocation. This method requires more casual and stable relationship in order to exploit the trust level and acquire necessary information. For instance, Caesar is looking to hack into SCADA network for which he requires internal employee to execute his malicious code. After his research, he developed a jewelers shop drawing keen interest of one of their employees (Eda) by selling gold jewelry at cheap prices. Now, assume that Caesar has already walked through the internet to get her personal information including her email address. Eda started getting special offers from the website with more discount prices than usual. It has attracted her mind to visit the website and purchase jewelry on regular occasion. After building this trust, Caesar decided to pursue the final task during her business hours on the selected day by offering her free gold jewelry in exchange to download and install the game on her desktop. Without noticing its implications and



consequences, she downloaded and installed the game. It proves that strengthening the relationship by offering valuable items can be of great advantage during social engineering engagement.

### Influential Authority

A method which manipulates the target's business responsibilities is known as influential authority. Accepting and following the instructions from senior management is our regular duty. As a human this makes us vulnerable to the situations where we are forced to execute certain tasks. For example, Caesar wants remote login credentials to access *Acme Inc* network. He obtained personal information about company's CEO and Network Administrator through business partner using reciprocation method (i.e. traded valuable item for the information). Using an external call spoofing service, he manages to call Network Administrator where the number is appearing to be from CEO's phone. As such the call is from senior management it should be prioritized and answered immediately. At this point of time, Network Administrator revealed login credentials to impersonated authority. It should be noted that this kind of social engineering method may complement combination of other methods like impersonation and reciprocation.

### Scarcity

Giving an opportunity to the people for their personal gain is known as scarcity. Human is a curious creature which always intends to take the best available option especially when it seems scarce. This greediest nature makes human vulnerable to serious threats. *Nigerian 419 Scam* is one of the famous examples of scarcity. Let me get another example, Caesar wants to collect personal information (name, date of birth, social security number, phone number, driving license number) from

all students in the Acme University. He currently holds the database of students email addresses. As an added advantage to this information, he sends out the email message to all students offering 7-days full paid trip to Canada whoever reply back with the required information. Since the opportunity is quite rare, many students may fall into this scam. In the typical corporate environment, this method can be useful for competitors to maximize their commercial gains by obtaining trade secrets.

### Social Relationship

Creating social relation is what makes us human. We share our thoughts, feelings and ideas to express our social interaction to the loved ones. On the other side, having sexual relationship is the most common and vulnerable part of any social connection. This builds up the trust and confidence between two parties which may end up disclosing the sensitive and private information. In today's fast growing technological world it has become easier for the penetration tester to socialize with their target using online social networks like Facebook, Twitter, and MySpace. It takes up the initial efforts to create trust boundary and then exploit it to acquire the targeted information. For instance, Caesar has recently been hired by Acme Inc to get the investors information from ABC Company. He joined several social media networks and attended couple of business events where he found and interact with the easiest target *Tina* who is responsible for major business operations in ABC Company. After knowing about her marital status and personal life, Caesar found a way to create relationship with Tina. He gradually created situations where he could meet and impress Tina within social gatherings, bars, clubs, music festivals, and corporate seminars. Once he established firm relationship, business talks become

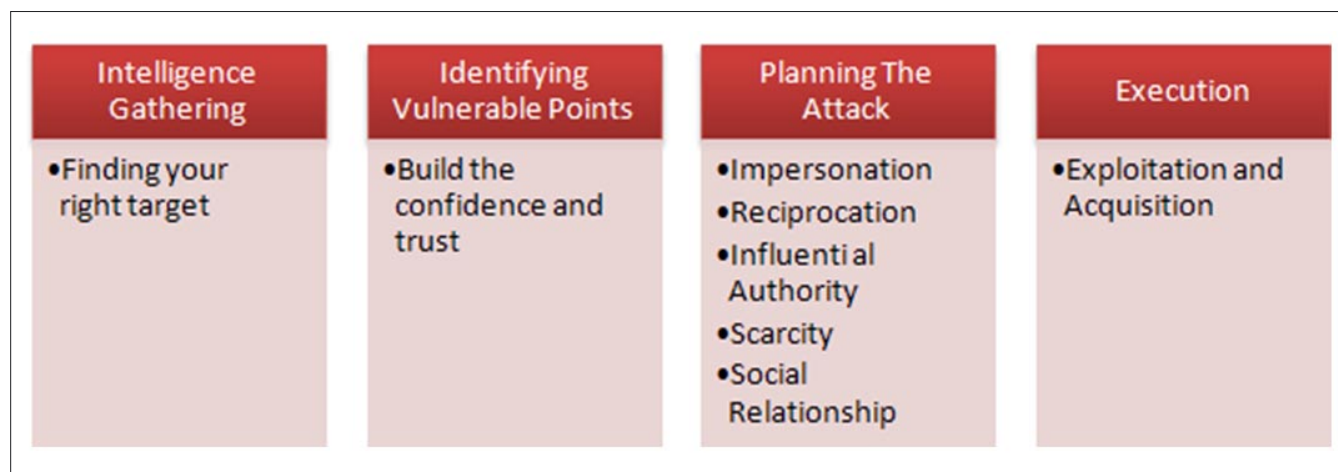


Figure 1. Social Engineering Attack Process



## References and Additional Reading

- Ali, Shakeel, and Tedi Heriyanto. BackTrack 4: Assuring Security by Penetration Testing. Birmingham, UK: Packt, 2011. Print [1].
- Hadnagy, Christopher. Social Engineering: The Art of Human Hacking. Indianapolis, IN: Wiley, 2011. Print [2].
- Social Engineering – Security Through Education. Web. 13 Feb. 2012. <http://www.social-engineer.org/> [3].

more focused and informative. This allowed Caesar to extract and gather all the required information about investors of ABC Company. It is important to note that creating trustful relation with your target would determine the success of your motives.

## Execution

The last step in social engineering attack process is the execution of the chosen attack method. Depending on the available resources and selected method, penetration tester should effectively follow the execution procedure. With confidence and creativity, the pen-tester should monitor and assess the outcome of the applied attack method. Upon successful exploitation, a social engineer would get access to privileged information. This information can help further to escalate his footsteps in acquiring other private corporate assets. During the whole attack process, it is vital to maintain patience and covertness.

## Social Engineering Tools

There are situations where you may require automating and accelerating the process of social engineering during pen-test engagement. These computer assisted tools provide platform for the penetration tester to choose the best method which should work against the target. Each of these attack methods relies on certain degree of pre-established trust relationship to execute our malicious contents. I have briefly discussed two well-know tools which may help pen-testers to automate their social engineering attack.

## SET (Social Engineering Toolkit)

The SET is a multi-functional and advanced social engineering toolset. It helps pen-tester to exploit the client-side vulnerabilities on the target machine and provides privileged access. Some of the well-known attack methods employed by SET include Spear-Phishing attack, Java Applet attack, Metasploit Browser attack, Credential Harvester attack, Tabnabbing attack, Man Left in the Middle attack, Web Jacking attack, Multi-Attack Web, Infectious Media Generator (USB/CD/DVD) and Teensy USB HID attack. Each of these attack methods require some sort of initial information gathering and reconnaissance activity before selecting the most persuasive technique which would attack the human element.

## CUPP (Common User Passwords Profiler)

The CUPP is another useful social engineering tool. The use of such tool comes into practice when you are unable to manipulate your target into disclosing confidential information or credentials. For instance, we assume that you hold target's personal information which would allow you to break the password of his email account by generating a list of possible combinations processed through his personal data. CUPP generates a list of possible passwords by profiling the target's name, date of birth, nickname, company, pet name, family member's information, lifestyle patterns, interests, likes, dislikes and hobbies. This factor contributes a great input towards dictionary-based attack against your target's email account.

## SHAKEEL ALI

*Shakeel Ali is a main founder of Cipher Storm Ltd, UK. His expertise in the security industry markedly exceeds the standard number of security assessments, audits, compliance, governance, and forensic projects that he carries in day-to-day operations. He has also served as a Chief Security Officer at CSS-Providers S.A.L. As a senior security evangelist and having spent endless nights without taking a nap, he provides constant security support to various businesses, educational organizations, and government institutions globally. He is an active independent researcher who writes various articles and whitepapers, and manages a blog at Ethical-Hacker.net. He also regularly participates in BugCon Security Conferences held in Mexico, to highlight the best-of-breed cyber security threats and their solutions from practically driven countermeasures. He is also an author of two recent scholarly and professional publications, "BackTrack 4: Assuring Security by Penetration Testing" and "Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies".*



# Finding your Target...

Network foot printing is, perhaps, the first active step in the recognisance phase of an external network security engagement. This phase is often highly automated with little human interaction as the techniques appear, at first glance, to be easily applied in a general fashion across a broad range of targets.

**A**s a security analyst, footprinting is also one of the most enjoyable parts of my job as I attempt to outperform the automatons; it is all about finding that one target that everybody forgot about or did not even know they had, that one old IIS 5 webserver that is not used, but not powered off.

With this article I am going to share some of the steps, tips and tricks that pentesters and hackers alike use when starting on an engagement.

## Approach

As with most things in life having a good approach to a problem will yield better results and overtime as your approach is refined you will consume less time while getting better results. By following a methodology, your footprinting will become more repeatable and thus reliable. A basic footprinting methodology covers reconnaissance, DNS mining, various information services (e.g. whois, Robtex, routes), network registration information and active steps such as SSL host enumeration.

While the temptation exists to merely feed a domainname into a tool or script and take the output as your completed footprint, this will not yield a passable footprint for two reasons. Firstly, a single tool will not have access to all the disparate information sources that one should consult, and secondly the footprinting process is inherently iterative and continuous. A footprint is almost never complete; instead, a fork of the footprint

data provides the best current view of the target, but the information could change tomorrow as new sites are brought online, or old sites are taken offline. Thus as a datum is found that could expand the footprint, a new iteration of the footprinting process triggers with that datum as the seed, and the results are combined with all discovered information.

## Know your target

The very first thing to do is to get to know your target organization. What they do, who they do it for, who does it for them, where they do it from both online and in the kinetic world, what community or charity work they are involved in. This will give you and insight into what type of network/infrastructure you can expect. Reading public announcements, financial reports and any other documents published on or by the organization might also yield interesting results. For any organization that must publish regular reports (e.g. listed companies), these are a treasure trove of information for understanding the target's core business units, corporate hierarchy and lines of business. All these become very useful when selecting targets.

Dumpster diving, if you are up for it and have physical access to the target, means sifting through trash to get useful information, but in recent times social media can provide us with even more. Sites like LinkedIn, Facebook and Twitter can provide you with lists of

# Session Hijacking

Even if you were drunk and surfing at a Wi-Fi hotspot, you probably wouldn't stand up and shout your username and password for anyone who might want it. But an attacker does not need to find out your username and password. The attacker's target might be your session.

**S**ession hijacking is the exploitation of a valid user session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a cookies used to authenticate a user to a remote server. When implemented successfully, attackers assume the identity of the compromised user, enjoying the same access to resources as the compromised user.

Session hijacking, also known as TCP session hijacking, allows a user to take control over a Web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network.

The session ID is normally stored within a cookie or URL. For most communications, authentication procedures are carried out at set up. Session hijacking takes advantage of that practice by intruding in real time, during a session. The intrusion may or may not be detectable, depending on the user's level of technical knowledge and the nature of the attack. If a web site does not respond in the normal or expected way to user input or stops responding altogether for an unknown reason, session hijacking is a possible cause.

Because http communication uses many different TCP connections, the web server needs a method

to recognize every user's connections. The most useful method depends on a token the Web Server sends to the client browser after a successful client

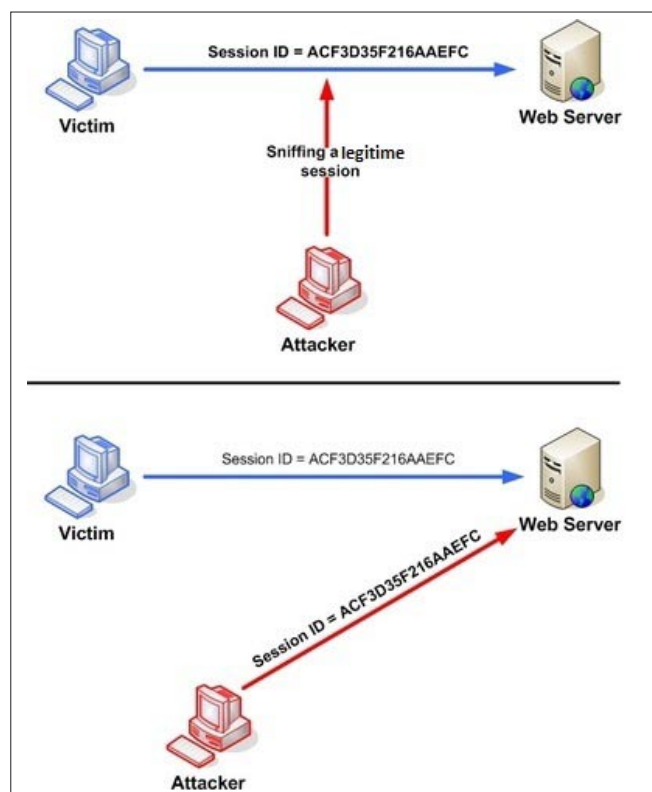


Figure 1. Session ID





# HIGH-TECH BRIDGE<sup>®</sup>

INFORMATION SECURITY SOLUTIONS

[www.htbridge.ch](http://www.htbridge.ch)

ORIGINAL SWISS ETHICAL HACKING

Digital Forensics  
Malware Analysis  
Penetration Testing  
Source Code Review  
Security Audit & Consulting







**ITonlinelearning** offers Network Security courses for the beginner through to the professional. From the CompTIA Security+ through to CISSP, Certified Ethical Hacker (CEH), Certified Hacking Forensic Investigator (CHFI) and Security Analyst/Licensed Penetration tester (ECSA/LPT).

## **e-Learning**

- ✓ Cost Advantage
- ✓ Tailored Solution
- ✓ Monitor Progress
- ✓ Flexible Study
- ✓ Certify Anywhere, Anytime
- ✓ Refresh Skills
- ✓ Explore New Courses
- ✓ Expert Help

## **Course Direction**

- ✓ Project Management
- ✓ Support
- ✓ Networking
- ✓ Server
- ✓ Security
- ✓ Database
- ✓ Developer
- ✓ Office



**Try our  
courses  
FREE**



## Tailored Advice and Discounts

0800-160-1161 or **Livechat**



Please Call one of our Course Advisors for help and Tailored Advice -during office hours  
(Mon-Fri 9am-5.30pm)

**Telephone: 0800-160-1161**

**International: +44 1795 436969**

**Email: [sales@itonlinelearning.co.uk](mailto:sales@itonlinelearning.co.uk)**

**[support@itonlinelearning.co.uk](mailto:support@itonlinelearning.co.uk)**

**Registered Office: 16 Rose Walk, Sittingbourne, Kent, ME10 4EW**



## IN ORDER TO BEAT A HACKER, YOU HAVE TO THINK LIKE ONE...

Recent major security breaches in some of the world's largest companies have proven that network security is extremely important. Companies are actively hiring Certified Ethical Hackers and Network Security Experts to help protect their customers data from malicious hackers.

Quickcert's state of the art certification training will allow you to obtain the marketability you need to take your career to the next level in 2012.

Because of this growth and demand in Network Security, QuickCert is offering you a Complimentary Two-Day Course so you can try one of our most popular security courses. If you'd like to enroll in the full class this ad entitles you to 50% off your purchase!



Call today to activate your free course – 1-888-840-2378 | Don't Delay!! Call Now

Call today and increase your  
marketability in 2012!

[www.quickcert.com](http://www.quickcert.com)  
1-888-840-2378



24703 US Highway 19 N, Clearwater, FL 33763 | [sales@quickcert.com](mailto:sales@quickcert.com) © 2012 QuickCert



# CSRF Attacks on network devices

Similar to vulnerabilities in web applications on web sites, there are also vulnerabilities in the admin panels of different network devices, including Cross-Site Request Forgery (CSRF) vulnerabilities. Which can be attack similarly to web sites – by attacking users who have access to these network devices.

**A**lmost all network devices are vulnerable to CSRF [1] due to misunderstanding of this threat by developers of such devices. So attackers can conduct remote CSRF attacks on network devices, such as routers, Wi-Fi Access Points and others, to do many different nasty things. Attackers can DoS them, disable different functionalities and change different settings, which allows them to take devices under full control (and take control on the user's traffic through these devices).

Such vulnerabilities exist in different network devices, such as Iskra Callisto 821+, D-Link DSL-500T ADSL Router and D-Link DAP 1150, vulnerabilities in which I've found and disclosed at my site. And by using CSRF attacks on these vulnerabilities the attacker can receive full control of these devices.

## Possibilities of CSRF Attacks on Network Devices

Developers of network devices don't attend enough to security (vulnerabilities in such devices are found all the time), especially CSRF, because they think that devices will reside in a LAN and will not be accessible from Internet. But it's not true, when such devices reside in a LAN, which has computers with access to Internet (CSRF attacks can be conducted via the browsers of the users at these computers). Not mentioning that there is also a threat of local attacks

– from malicious local attackers or viruses – so developers should not leave their devices with remote or local vulnerabilities.

For example routers and ADSL modems, which allow users to access the Internet, are typically affected devices. These can be attacked remotely via CSRF from the Internet. For external attackers the most interest represent such network devices as routers and other devices with router-functionality (ADSL modems, Wi-Fi Access Points, etc.). Because it's possible to setup these devices in such way, that attacker will take control of the traffic – all traffic (such as DNS requests) will be sent via his own server, allowing him to sniff confidential data and conduct phishing attacks on all users in a LAN who are using these devices to access the Internet.

## Real attacks on Network Devices

Let's see how real attacks can be conducted on example of Iskra Callisto 821+ and D-Link DAP 1150. Callisto 821+ it's ADSL Router (and similar vulnerabilities can be in all other devices from Iskra). The DAP 1150 is a Wi-Fi Access Point and router (similar vulnerabilities can be in all other devices from D-Link).

There can be different attacks created. Let's take a look at two attacks, which are very advantageous for the attackers. In the first scenario the attacker will conduct part of the actions remotely and part manually

# NTO SQL Invader

SQL Injection is an attack in which the attacker manipulates input parameters that directly affect an SQL statement. This usually occurs when no input sanitisation is conducted. Depending on permissions, an attacker may be able to read database contents or even write to the database. In this article, the author will show you how to exploit SQL injection vulnerability using NTO SQL invader.

**N**T O SQL Invader is a SQL injection exploitation tool. It gives the ability to quickly and easily exploit or demonstrate SQL injection vulnerabilities in Web applications. With a few simple clicks, a penetration tester will be able to exploit a vulnerability to view the list of records, tables and user accounts of the back-end database. It has been designed to assist a penetration tester in demonstrating the impact of SQL injection vulnerability in a web application penetration test. NTO SQL Invader has the following features:

- Easy to use – The graphic user interface of the tool enables a penetration tester to simply paste an injectable request found by a web application vulnerability scanner or feed a detailed request straight from a web application scan report. He/she can then control how much information is gathered.
- Clearly presents evidence – Unlike other SQL injectors that provide all data via command line, NTO SQL Invader provides the data in an organised manner that is useful for executive meetings as well as technical analysis and remediation.
- Enables easy transport of logging data – All of the data gathered from NTO SQL Invader can be saved into a CSV file so the reports can be included as penetration evidence as part of a presentation or proof of concept.

NTO SQL Invader is available from: [ntobjectives.com](http://ntobjectives.com). Once you have executed the program, the following screen will be displayed: Figure 1.

## Setting Up

For this example, we are going to use NTO SQL Invader to exploit SQL injection vulnerability in a vulnerable web application – *Exploit KB Vulnerable Web App*. Exploit KB Vulnerable Web App is a PHP/MySQL web application that designed as a safe, legal environment to study and perform common attacks on web applications. You may get a copy from here: <http://exploit.co.il/projects/vuln-web-app/>.

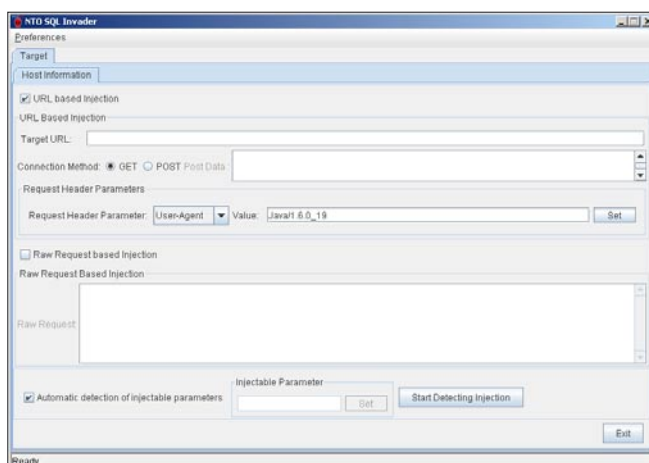


Figure 1. NTO SQL Invader main screen

# Web Application

## Security Vulnerabilities Have Been Prevalent The Last Decade

Where companies have been good at protecting the outside of the company with fences, fire walls and network defenses. Port 80 and Port 443 has been a great attack vector for malicious attackers. This article will discuss the three most common and devastating software security vulnerabilities. SQL injection, Cross Site Scripting and Cross Site Request Forgery.

We will look at each of these vulnerabilities from the outside as an attacker would as well as inside the source code where they reside and your developers program them. We will then offer solutions on how to fix them and offer more secure software to your enterprise.

Many of my colleagues participate in black box testing rather than white box testing. Black box testing is also known as zero knowledge testing where the testing team is provided no knowledge of the resource to be tested and has to acquire information on its own.

The purpose of this article is to discuss white box testing or having full knowledge of the source code and how the application works. I believe this is important when doing a penetration test to get a full threat picture of the application that you are looking at.

Another point to bring up is the earlier that this is completed in the software development life cycle the cheaper it is to fix as well as lower attack surface your application has.

To understand these commands more fully it is important to understand the TCP/IP handshake process. TCP/IP is a stateless protocol sending response and requests through GET, POSTS and HEAD. Cookies often times store state data as well as authentication and tracking data that may or not be sensitive.

With a proxy tool like Burpe Suite, <http://portswigger.net/burp/>, Open Web Application Security Framework Web Scarab [https://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project) Or Tamper data <https://addons.mozilla.org/en-US/firefox/addon/tamper-data/> all client side validation can be bypassed and direct commands can take place on the server through a man in the middle proxy.

For this basic understanding now we can completely understand how SQL Injection, Cross Site Scripting and Cross Site Request Forgery work.

SQL injection is a web application security attack that can be devastating to an application. SQL injection at its most basic level is mixing code and database commands to extract, modify or delete data in the database.

SQL injection can allow an attacker to bypass login functions or extract data. One of the simplest SQL injection attacks to bypass authentication is `' or 1=1--` (Pasted from <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>).

The source code for this would look something like this.

### Select \* From User Where

The problem with this code snippet whether it be in Java, .NET, PHP or any language that you chose is that the value of the USER is not validated and the



# Interview with Marsel Nizamutdinov

*Marsel Nizamutdinov, Head of Research & Development Department at High-Tech Bridge SA, web application security expert, author of „Hacker Web Exploitation Uncovered“ (2005).*



**Your book, „Hacker Web Exploitation Uncovered“ was written in 2005, are you planning a 2nd edition?**

**Marsel Nizamutdinov:** Not in the near future, as I am quite busy now. From time to time I write articles about new trends in web security, but a second edition of the book would be a very serious and time-consuming project.

**Besides your book, what other learning resources would you recommend for people new/interested in web application security?**

**MN:** In learning, the most important part is practice. Nevertheless, Wikipedia and OWASP websites are perfect ways to begin.

**What would you consider to be the largest threats to web applications today?**

**MN:** I would say that the largest threat is coming from people that underestimate the risks of web-based

vulnerabilities. Being unable to understand the risk or the attack vector of Script Insertion in admin panel for example, or some incompetent people who deny the dangers of the vulnerability, which quite often leads to total system compromise. The situation is even worse if people, who are not able to understand the impact of certain web-based vulnerabilities, work in the security industry and pretend to be *security experts*. They simply mislead people and pose a danger to the industry.

**What should be the first thing a penetration tester should focus on in web application testing?**

**MN:** It is difficult to give a *one size fits all* recommendation here. Every web application penetration test is unique. Personally, in most of the cases I try to understand web application logic and schema. Which script is doing what, which parameters does it accept, how does it process and store them, etc.

Hacking<sub>of</sub>  
Financials.

Theft<sub>of</sub>  
Data.



# Sense of Security

## Compliance, Protection and Business Confidence

At Sense of Security, Information Security and Risk Management is our only business. Our consultants are experts in their fields; our specialists are always ahead of the curve.

By engaging Sense of Security, our clients ensure they are protected, their information is safe from threats from both within and outside the organisation, they meet their regulatory requirements and their employees, partners and suppliers can conduct business in complete confidence.

[info@senseofsecurity.com.au](mailto:info@senseofsecurity.com.au)  
[www.senseofsecurity.com.au](http://www.senseofsecurity.com.au)

# Qualys Virtual Scanner

Tentatively scheduled for Q1 2012, Qualys will release their Virtual Scanner out of beta and make it available for purchase. This new scanner is an alternative to Qualys' scanner appliance already in popular use by security departments and consultants, and will run in as a virtual machine on VMware or VirtualBox software on a server or laptop/desktop.

The setup of a new Virtual Scanner is not difficult. For existing Qualys customers, a change must be made to the service account to allow for the Virtual Scanners. During the change and previously owned physical scanner appliances must be online or else the physical devices can be irreparably dropped from the service account and will have to be returned to Qualys. After the account change, users will notice new menu options for the provision and download of Virtual Scanner appliances.

Provisioning a new Virtual Scanner is an easy task including choosing a consultant or enterprise solution and obtaining a personalization code. The personalization code is later used in the initial confi-

guration of a new Virtual Scanner. Once provisioned, a decision about hosting virtualization software must be made. Virtual Scanner images are available for VMware Player/Workstation/Fusion/ESXi, VirtualBox, or vSphere (Qualys Enterprise only). The virtualization solution used will depend on the needs of the environment. VMware Player, Workstation, Fusion, and VirtualBox are excellent solutions for consultants running the Virtual Scanner on a laptop. The ESXi and vSphere solutions work better for server installs in data center environments.

From the Qualys online platform, downloads of the Virtual Scanners are available for the previously mentioned virtualization solutions.

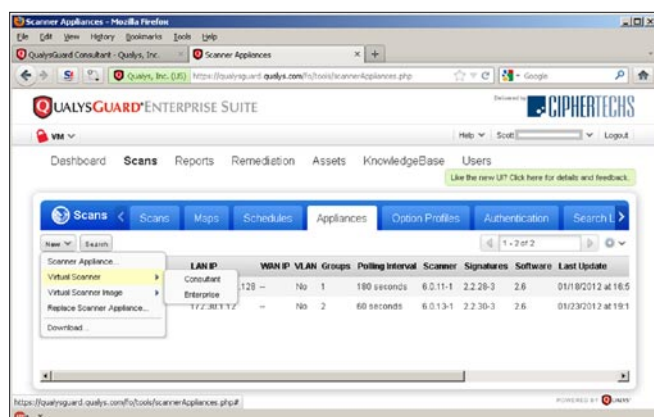


Figure 1. Provisioning a new Virtual Scanner from the Appliances tab

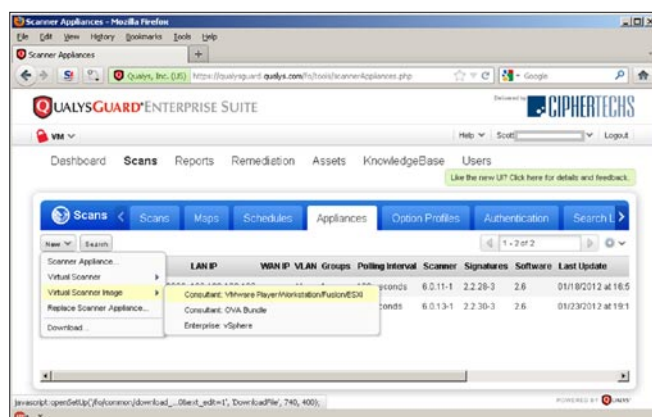


Figure 2. Selecting Virtual Scanner type to download



In the next issue of

# PenTest **EXTRA** *magazine*

## **PenTest Market!**

Available to download  
on **March 15<sup>th</sup>**

**New Magazine will bring only benefits:**

- New people interested in pentesters services will join our community
- You will find out what do employers expect from pentesters
- You will know how does pentesting market work
- Recruiters will reveal how are they looking for pentesters
- We will bring you fresh information on new products/tools for pentesters

and more...

If you would like to contact PenTest team, just send an email to [krzysztof.marczyk@software.com.pl](mailto:krzysztof.marczyk@software.com.pl) or [maciej.kozuszek@software.com.pl](mailto:maciej.kozuszek@software.com.pl). We will reply a.s.a.p..



Get the best real-world  
Android education anywhere!

Attend

# AnDevCon

The Android Developer Conference

May 14-17, 2012

San Francisco Bay Area

AnDevCon is the biggest,  
most info-packed, most practical  
Android conference in the world!

"AnDevCon was an informative and comprehensive presentation of Android development concepts, tools and techniques."

—Patrick Burrell, Sr. Research Scientist, Amway

"The conference is worth the time and expense. It's a great place to meet talented people in the Android industry."

—Keith Collins, CTO, Neusoft

"AnDevCon is great for networking, learning tips and tricks, and for brainstorming innovative, new ways to create apps."

—Joshua Turner, Software Engineer, Primary Solutions

- Choose from over 65 Classes and Workshops!
- Learn from the top Android experts—including speakers straight from Google!

Register Early  
and SAVE!



 Follow us: [twitter.com/AnDevCon](https://twitter.com/AnDevCon)

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

A BZ Media Event

Register NOW at [www.AnDevCon.com](http://www.AnDevCon.com)