

PentTest **FREE** magazine

Vol.1 No.1 Monthly ISSN 2084-1116
Issue 01/2012(01) July

Pentesting Attacks



**A WIRELESS (802.11) PROBE REQUEST BASED ATTACK
ZED ATTACK PROXY
PHISHING, SMISHING & SOCIAL MEDIA ATTACKS**

PLUS

**PENTESTING SCADA PLATFORM
THE ARTILLERY OF CYBER WAR**



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

support@itonlinelearning.co.uk

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



Global I.T. Security Training & Consulting

www.mile2.com

In February 2002, Mile2 was established in response to the critical need for an international team of IT security training experts to mitigate threats to national and corporate security far beyond USA borders in the aftermath of 9/11.



IS YOUR NETWORK SECURE?

**A Network breach...
Could cost your Job!**

Available Training Formats

1. F2F Classroom Based Training
2. CBT Self Paced CBT
3. LOT Live Online Training
4. KIT Study Kits & Exams
5. LHE Live Hacking Labs (War-Room)



CISSP™
C|ISSO
C|SLO
ISCAP

GENERAL SECURITY TRAINING
CISSP & Exam Prep
Certified Information Systems Security Officer
Certified Security Leadership Officer
Info. Sys. Certification & Accred. Professional



C|PTE™
C|PTC™

PENETRATION TESTING (AKA ETHICAL HACKING)
Certified Penetration Testing Engineer
Certified Penetration Testing Consultant



C|SCE™

SECURE CODING TRAINING
Certified Secure Coding Engineer



C|WSE™
C|WNA/P™

WIRELESS SECURITY TRAINING
Certified Wireless Security Engineer
Certified Wireless Network Associate / Professional



DR/BCP

DR&BCP TRAINING
Disaster Recovery & Business Continuity Planning



C|SVME™

VIRTUALIZATION BEST PRACTICES
Certified Secure Virtual Machine Engineer



C|DFE™

DIGITAL FORENSICS
Certified Digital Forensics Examiner

Other New Courses!!

ITIL Foundations v.3 & v.4
CompTIA Security+, Network+
ISC² CISSP & CAP

SANS GSLC GIAC Sec. Leadership Course
SANS 440 Top 20 Security Controls
SANS GCIH GIAC Cert Incident Handler

Worldwide Locations



We practice what we teach.....

Other Mile2 services available Globally:

1. Penetration Testing
2. Vulnerability Assessments
3. Forensics Analysis & Expert Witnesses
4. PCI Compliance
5. Disaster Recovery & Business Continuity

(ISC)2 & CISSP are service marks of the IISCC. Inc. Security+ is a trade mark of CompTIA. ITIL is a trade mark of OGC. GSLC & GCIH are trademarks of GIAC.

1-800-81-MILE2
+1-813-920-6799

11928 Sheldon Rd Tampa, FL 33626

Dear Readers!

To thank you for your support with creating PenTest community we decided to publish PenTest Free. Every month you will get five great articles that will teach and keep you up to date with IT security issues.

In the first issue you will find articles devoted to attacks. We have chosen the most popular titles and here you can read the best articles devoted to Zed Attack Proxy, internationalized, free and of great help as far as report writing is concerned. Probe Request Based Attack article is a great technical tutorial for anyone interested in wireless attacks. Can we train a computer user to be sufficiently security literate? What's the best way to defend one from phishing attacks? You can read about this in the article of Ian Moyses.

In the section Cyberwar you can read about digital frontier and the impact of cyber attacks on our lives. Are we living in the times of an ongoing cyberwar? See what our author has to say about this problem. Last but not least, we would like you to read article about pentesting SCADA written by our regular author Stefano Maccaglia.

I hope that you will find this issue a valuable compilation and encouragement to stay with us for good. If you have any suggestions for us concerning topics, problems you want to read about or people you would like to know better thanks to PenTest please, feel free to contact us at en@pentestmag.com.

Thank you all for your great support and invaluable help.

Enjoy reading!
Malgorzata Skora
& PenTest Team

ATTACKS

06 Get it on with ZAP

by Gareth Watters

Let's take a look around Zed Attack Proxy and see what it's all about, but before we go on let's emphasize some of the greatest ZAP's attributes. It's easy, it's free and open source, ZAP is fully internationalized, has extensive user guides and unlike some similar tools, has the ability to save sessions to go back to later for reports, which is an imperative requirement for pen testers as report writing tends sometimes not to be our strongest area.

14 Wireless Eurynomus: A Wireless (802.11) Probe Request Based Attack

by Hitesh Choudhary and Pankaj Moolrajani

In the recent years, the proliferation of laptop computers and smart phones has caused an increase in the range of places people perform computing. At the same time, network connectivity is becoming an increasingly integral part of computing environments.

18 Securing Users from Phishing, Smishing & Social Media Attacks

by Ian Moyses

Some experts believe one of the best solutions to thwart phishing attacks is end-user training, but can we really train every computer user to be sufficiently security literate? Will it ever be the case that anyone can distinguish a phishing message from a genuine bank email?

CYBERWAR

22 Digital Apocalypse: The Artillery of Cyber War

by Cecilia McGuire

Cyberspace is now the digital frontier of choice for executing many combat operations, by extending the medium in which greater levels of power can now be accessed by Machiavelli agents, militants and nation-states. Squads of cyber militants going under the banner of Anonymous and LulzSecare, motivated by the ease in which they can now execute high impact operations whilst avoiding detection, are just a few of the much publicized names synonymous with cyber terrorism. The multi-dimensional characteristics of cyber space have dissolved the boundaries between digital landscape and physical security, facilitating cyber-attacks that produce devastating impacts to critical infrastructure, as well as Corporate and Government assets.

SCADA

28 The Box holes. Pen Testing a SCADA platform

by Stefano Maccaglia

In the last decade SCADA systems have moved from proprietary, closed, networks to open source solutions and TCP/IP enabled networks. Their original "security through obscurity" approach, in terms of protection against unauthorized access, has fallen, together with their interconnection limits. This has made them open to communicate with the rest of the world, but vulnerable, as our traditional computer networks.

PenTest

magazine

TEAM

Supportive Editor: Ewa Dudzic
 ewa.dudzic@software.com.pl

Product Manager: Malgorzata Skóra
 malgorzata.skora@pentestmag.com

Betatesters / Proofreaders: Robert Keeler, Daniel Wood, Scott Christie, Massimo Buso, Hussein Rajabali, Aidan Carty, Jonathan Ringle, Thomas Butler, Dan Felts, Gareth Watters, Stefanus Natahusada, Francesco Consiglio, Harish Chaudhary, Wilson Tineo Moronta, Scott Stewart, Richard Harold, Ryan Obero, William R. Whitney III, Marcelo Zúñiga Torres

Senior Consultant/Publisher: Paweł 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

Publisher: Software Press Sp. z o.o. SK
 02-682 Warszawa, ul. Bokserka 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 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.

Get it on with Zed Attack Proxy

Let's take a look around Zed Attack Proxy and see what it's all about, but before we go on let's emphasize some of the greatest ZAP's attributes. It's easy, it's free and open source, ZAP is fully internationalized, has extensive user guides and unlike some similar tools, has the ability to save sessions – a great help as far as writing reports is concerned.

You can download Zed Attack Proxy from <http://code.google.com/p/zaproxy/>. Note: If you don't already have it installed, you need to download and install java <http://www.java.com>.

ZAP is at its heart an interception proxy and has to be configured in-line between your browser and your application. For instructions to configure ZAP as a proxy for all the major browsers go to [http://](http://code.google.com/p/zaproxy/wiki/HelpStartProxies)

code.google.com/p/zaproxy/wiki/HelpStartProxies.

When you open ZAP for the first time you will be prompted to create an SSL Root CA Certificate as in Figure 2. In the context of this article, we will be working with the secure login to a vulnerable web application. Therefore we shall create a SSL Root CA certificate.

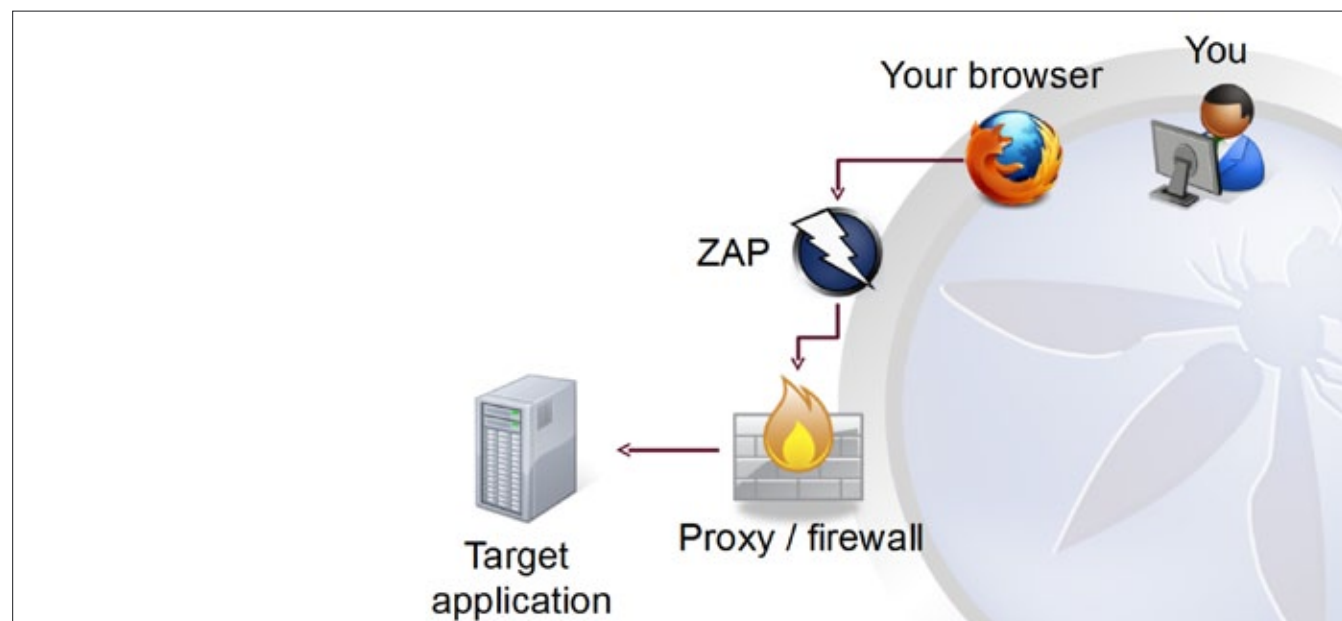


Figure 1. Setup of ZAP for use in a Penetration Test

Option Dynamic SSL Certificates

OWASP ZAP allows you to transparently decrypt SSL connections. For doing so, ZAP has to encrypt each request before sending to the server and decrypt each response, which comes back. But, this is already done by the browser. That's why, the only way to decrypt or intercept the transmission, is to do a 'man in the middle' approach.

Overview

In other words, all data sent to and received from the server is encrypted/decrypted by using the original server's certificate inside ZAP. This way, ZAP knows the plain text. To establish a SSL protected session from you (your browser), ZAP is using it's own certificate. This is the one you can create. Every certificate created by ZAP will be signed for the same server name. This way, your browser will do regular SSL encryption.

Import Certificate in to Mozilla Firefox – Firefox is using it's own certificate store. Installation and late on validation is done in the same preferences dialog:

- Go to Preferences
- Tab Advanced
- Tab Cryptography/Certificates
- Click View certificates
- Click tab Trusted root certificates
- Click Import and choose the saved owasp_zap_root_ca.cer file
- In the wizard choose to trust this certificate to identify web sites (check on the boxes)
- Finalize the wizard

Attention Risks

When adding self generated Root CA certificates to your list of trusted root certificates, anyone with the root certificate can smuggle data into your sys-

tem (browser). In other words when you're not testing in a safe environment, but on productive machines, be aware that you could be opening an additional attack vector to your system if your certificate was in the wrong hands. ZAP generates a certificate that is unique to you, so keep this certificate safe.

Next you configure ZAP's Local Proxy port: Go To Tools -> Options -> Local Proxy -> localport Settings: Localhost 8090.

Then configure your browser to use ZAP as a proxy. In this example we are using Firefox running Foxyproxy: Go To Edit -> Preferences -> Networks -> Settings -> Choose to Use ZAP for all URLs.

Now you're ready to go. All you need is your target application (Pentester) or your own Web Application that's under development (Developer). for the context of this article we will use DVWA (*Damn Vulnerable Web Application*)

DVWA – Damn Vulnerable Web App

(User: admin Password: password)

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. It's main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any working web server as it will be hacked. I recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing. <http://code.google.com/p/dvwa/>

Tip

If you fancy skipping past the installation and setup of dvwa, I suggest downloading SamuraiWTF, you will find that this great distro already has DVWA already installed setup and ready to go.

The next thing to do for a beginner new to development or pentesting is explain how ZAP's advanced components can be useful as a tools in a basic web application penetration test.

Basic Web Application Penetration Test: Recon -> Mapping -> Discovery/Enumeration -> Exploitation.

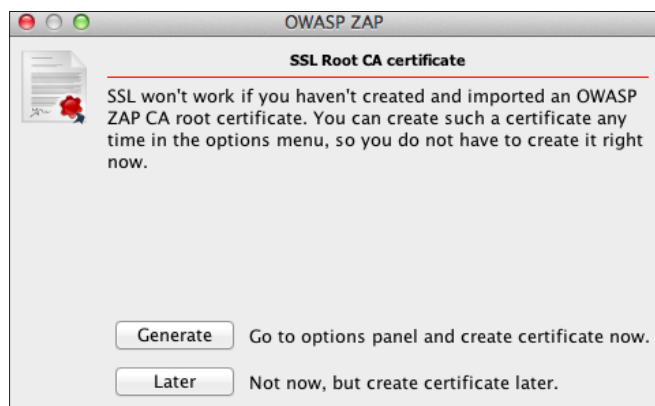


Figure 2. SSL Root CA Certificate

ZAP is useful in the Mapping context using the proxy and spider. ZAP is useful in the Discovery context with the active vulnerability scanner and fuzzer, brute forcing web directories and files with DirBuster.

ZAP is useful in the Exploitation phases when you combine it's findings with exploitation tools such as like SQLMap,BeEf and Metasploit.

Basic Web Application Penetration Test – Mapping

To do comprehensive mapping, you must navigate through your web application. Ensure to follow and explore through all of the functionality of the application. Click each link, traverse through all tabs and areas of your application. Press all buttons, fill in and submit all forms. If your application supports multiple roles then do this for each of the roles e.g. User, Admin. Note: In order to use multiple roles, it's best to save each role as a separate ZAP sessions.

Zap maps out the web application in a hierarchical manner as in the *sites* tab displayed in Figure 3.

The lower pane brings together all the tabs for web application pen. testing in a universal status bar.

Tip

In Zap – Double click on a tab and it the tab for a better view – Double click and it will revert back to the lower status bar.

- *Sites* tab – A Hierarchical representation of your application
- *History* Tab – Lists all the requests (GET/POST) and the order they are made
- *Search* tab – Search ZAP gathered information
- *Port Scan* – a basic port scanner allows you to scan and shows which ports are open on the target sites.
- *Output* tab – This shows various informational messages. These can include the stack traces of unexpected exceptions
- *Alerts* tab – Shows you any potential issues and vulnerabilities ZAP has found. (See Exploitation for more info.)

Click on entries in *Sites* or *History* – corresponding requests and responses will be visible in the *Request* and *Response* Tabs If you right-click on any item – A whole load of extra options and functionality becomes available.

Zap passively scans the Requests and Responses and reports any potential problems, but does not submit any responses on your behalf.

Spider

Can be activated by the play button on the Spider tab or Right-Click Attack on the sites tree.

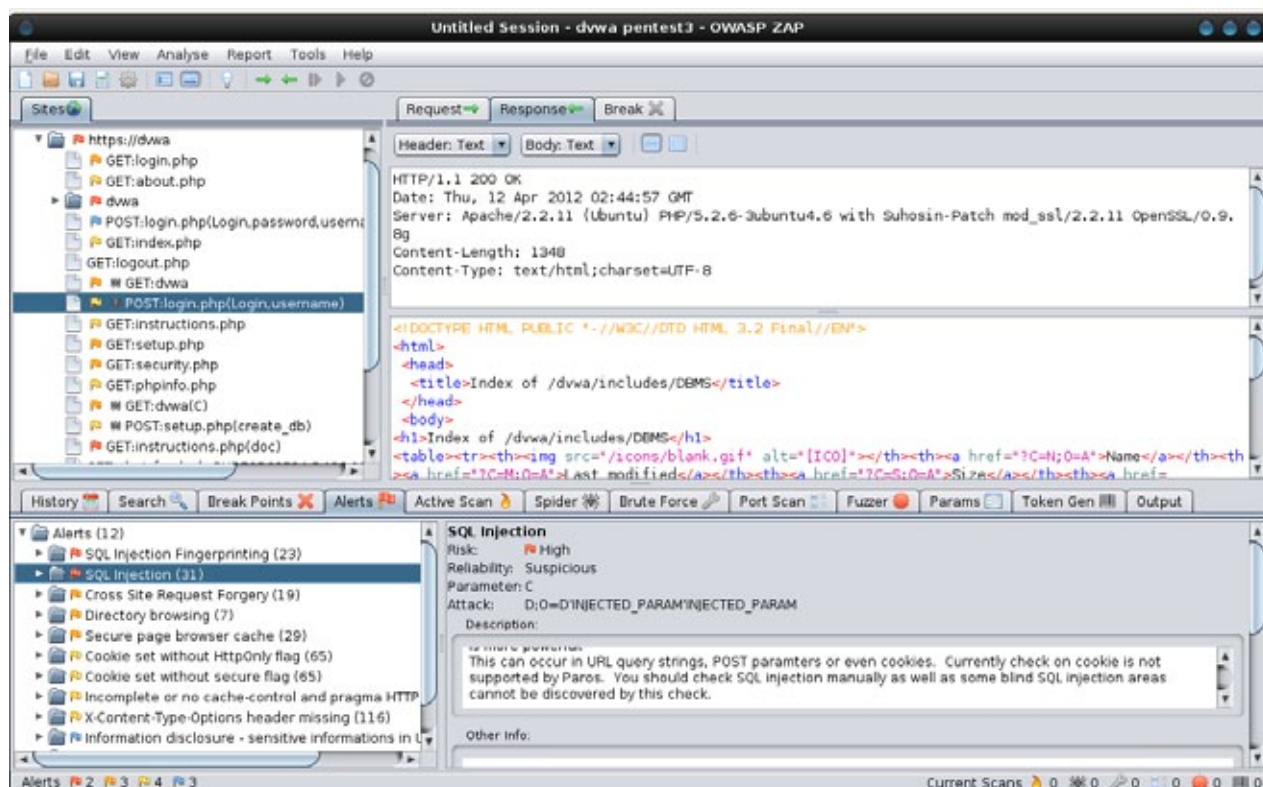


Figure 3. A completed mapping of DVWA

The spider looks for pages that weren't found in the manual recon/mapping. Running the spider, will crawl the website and find URLs that you may have missed are hidden. It places them in the Sites page with a spider icon. It is recommend to manually explore and map the web application first and then use spider. If the spider does find unseen links, revert back through the application through your browser and visit those URLs.

Tip

A good crawl will enable you to have a better active scan.

Basic Penetration Test – Discovery

Active scanner

Active vulnerability scanner attacks the application and performs a number of known attacks.

Active scanner is there to find basic vulnerabilities (*Only to be used in development environment unless explicitly permitted in writing by the Web App. owner in case of a Penetration test – It is illegal to run active scans without legal consent*).

Damn Vulnerable Web Application (DVWA) as it is aptly named is an excellent resource for viewing, and learning about vulnerabilities. Once you've completed the above steps above you should be able to see the results of the mappings and vulnerabilities in your application in the Alerts tab Immediately you can see a number of alerts for vulnerabilities found.

Brute Force

Use the brute force scanner to find unreferenced files and directories. You can use the built in or custom input files for Brute Force Scanner. ZAP Uses OWASP DirBuster and Fuzzing using another OWASP Project JBroFuzz and Fuzzdb

ZAP uses *OWASP DirBuster*, a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. DirBuster attempts to find these.

However tools of this nature are often as only good as the directory and file list they come with. A different approach was taken to generating Dirbuster. The Dirbuster list was generated from scratch, by crawling the Internet and collecting the directory and files that are actually used by developers! DirBuster comes a total of 9 different lists, this makes DirBuster extremely effective at finding

those hidden files and directories. And if that was not enough DirBuster also has the option to perform a pure brute force, which leaves the hidden directories and files nowhere to hide!

Tip

ZAP also *allows for custom files to be used*, in the SamuraiWTF training course we used CeWL (*Custom Word List generator*) by DigiNinja. CeWL is a ruby app which spiders a given url to a specified depth, optionally following external links, and returns a list of words which can then be used for password crackers such as John the Ripper. John the Ripper can aswell be used to create a wordlist that has different versions of the words that CeWL collected for example – ex@mpl3 These custom wordlists can then be imported and used by ZAP for Brute Forcing and Fuzzing.

Fuzzer

ZAP also has fuzzing capabilities through its integrated use of yet another OWASP Project JBroFuzz. *'Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems'* - Wikipedia'

To Fuzz a request string such as a password:

- Select a request in the *Sites* or *History* tab
- Highlight the string you wish to fuzz in the request tab
- Right-click in the Request tab and select 'Fuzz'
- Select the Fuzz Category and one or more of the Fuzzers
- Press the Fuzz Button
- The results will then be listed in the Fuzzer tab
- Select them to see the full requests and responses

Additional fuzzing text files are added continuously with each ZAP release and as stated earlier you can also create and import your own custom files.

Manual test

The above steps will find basic vulnerabilities. More vulnerabilities become apparent when you to manu-

ally test the application by giving it some data, trying loginsetc. In an advanced web application penetration test scenario, a number of other tools such as Nikto, Curl, SQLMap, Cewl etc would be used, See the OWASP Testing Guide for more details on comprehensive Penetration Testing at https://www.owasp.org/index.php/OWASP_Testing_Project.

Basic Penetration Test – Exploitation:

Once you have performed your basic pentest mapping and discovery, you are ready for exploitation or remediation depending on your role, developer or pentester. The considerable information that ZAP provides under the Alerts tab is key to a pentester's next move.

Alerts

ZAP provides comprehensive information relating to all alerts and vulnerabilities it finds. All the exploitation material you need is here listing active and passive vulnerabilities. Each alert gets flagged in the *History* tab, gets a Risk Rating – Informational, Low, Medium or High. Also, they get an alert reliability rating – False Positive, Suspicious, Warning.

Tip

I find it easiest at this point to review the alerts if you expand the Alert tab by double clicking it as in Figure 4.

For each alert a description is provided. You can save your own developer/pentester specific infor-

mation about a particular alert in the 'Other info' tab, and best of all there is a solution and reference material provided for the alert.

You will see *how intuitive and educationally beneficial ZAP really is* to developers/pentesters, especially ones in the early stages of their careers.

Break Points

A break point allows you to intercept a request from your browser and to change it before it is submitted to the web application you are testing. You can also change the responses received from the application. The request or response will be displayed in the Break tab which allows you to change disabled or hidden fields, and will allow you to bypass client side validation (often enforced using javascript). It is an essential penetration testing technique. You can set a 'global' break point on requests and/or responses using the buttons on the top level toolbar.

All requests and/or responses will then be intercepted by ZAP allowing you to change anything before allowing the request or response to continue. You can also set break points on specific URLs using the "Break..." right click menu on the Sites and History tabs. Only those URLs will be intercepted by ZAP. URL specific break points are shown in the Break Points tab.

Anti CSRF Tokens

Another advanced feature of ZAP that is not readily available in similar, free versions of tools in this

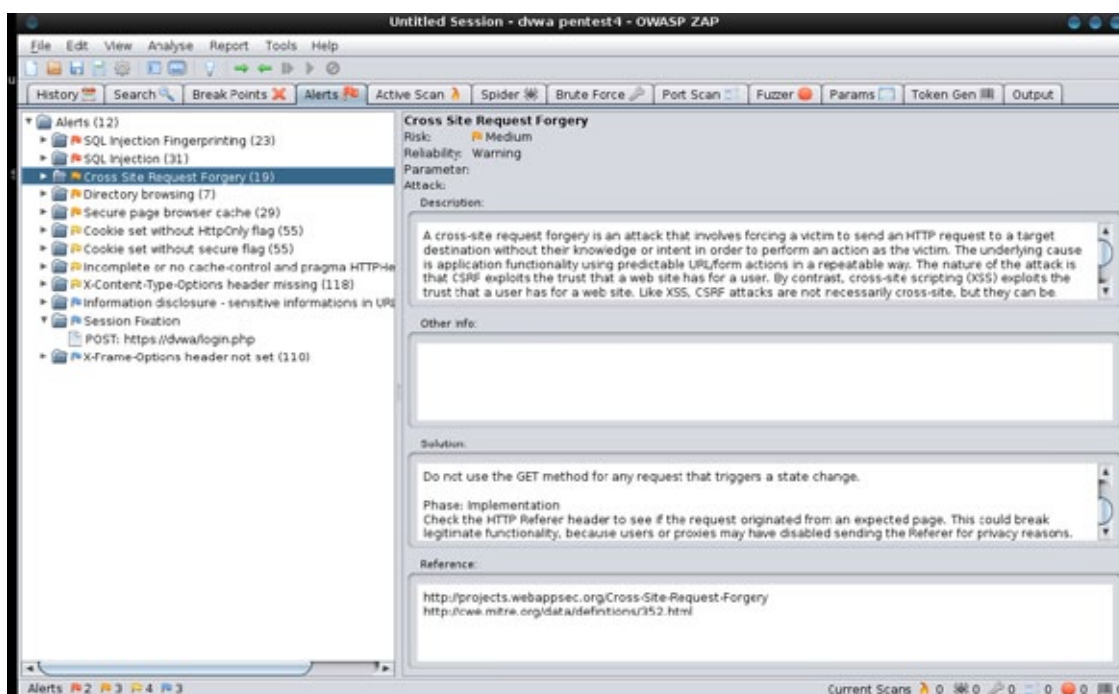


Figure 4. Alerts tab expanded

area is Anti-CSRF token handling and token generation. CSRF vulnerabilities occur by the way that browsers automatically submit cookies back to an issuing web server with each subsequent request. If a web application relies solely on HTTP cookies for tracking sessions, it will inherently be at risk from an attack like this.

Anti CSRF tokens are (pseudo) random parameters used to protect against *Cross Site Request Forgery* (CSRF) attacks.

They tokens may make a penetration testers job hard if the tokens are regenerated every time a form is requested. ZAP detects anti CSRF tokens by attribute names – the list of attribute names considered to be anti CSRF tokens can be edited using the Tools->Options->Anti-CSRF screen.

When ZAP detects these tokens it records the token value and which URL generated the token. The active scanner and the fuzzer both have options which cause ZAP to automatically regenerate the tokens when it is required. If fuzzing a form with an anti CSRF-tokens on it, ZAP can regenerate the token for each of the payloads you want to fuzz with.

If you are a developer testing your own web application make sure the names of your anti-csrf tokens are included in ZAP for ease of use.

It's clear to see that considerable effort has been embedded in Zed Attack Proxy by Simon Bennetts and Axel Neumann and also the Global community of developers and individuals contributing. ZAP

was an app built by a developer, for a developer and you can tell. It has subsequently been adopted by an international community of information security professionals.

ZAP – Fully Automated Security Tests

To conclude this extensive article, I am going to change the context of how we see use of ZAP and show how functional testing can be improved, even fully automated and with adding security in to the process. sounds good eh!

Many Web developers use applications like Selenium, Webdriver and Watir to test their Web-Applications. In this example we are using Selenium to drive the browser. Selenium records your actions in the browser such as mapping, clicking, inputs etc.. and then can re-test doing exactly the same tests while you complete iterations of say a web application under development.

Seleniumhq.org

'Selenium automates browsers. That's it. What you do with that power is entirely up to you. Primarily it is for automating web applications for testing purposes, but is certainly not limited to just that. Boring web-based administration tasks can (and should!) also be automated as well.'

Selenium has the support of some of the largest browser vendors who have taken (or are taking) steps to make Selenium a native part of their brows-

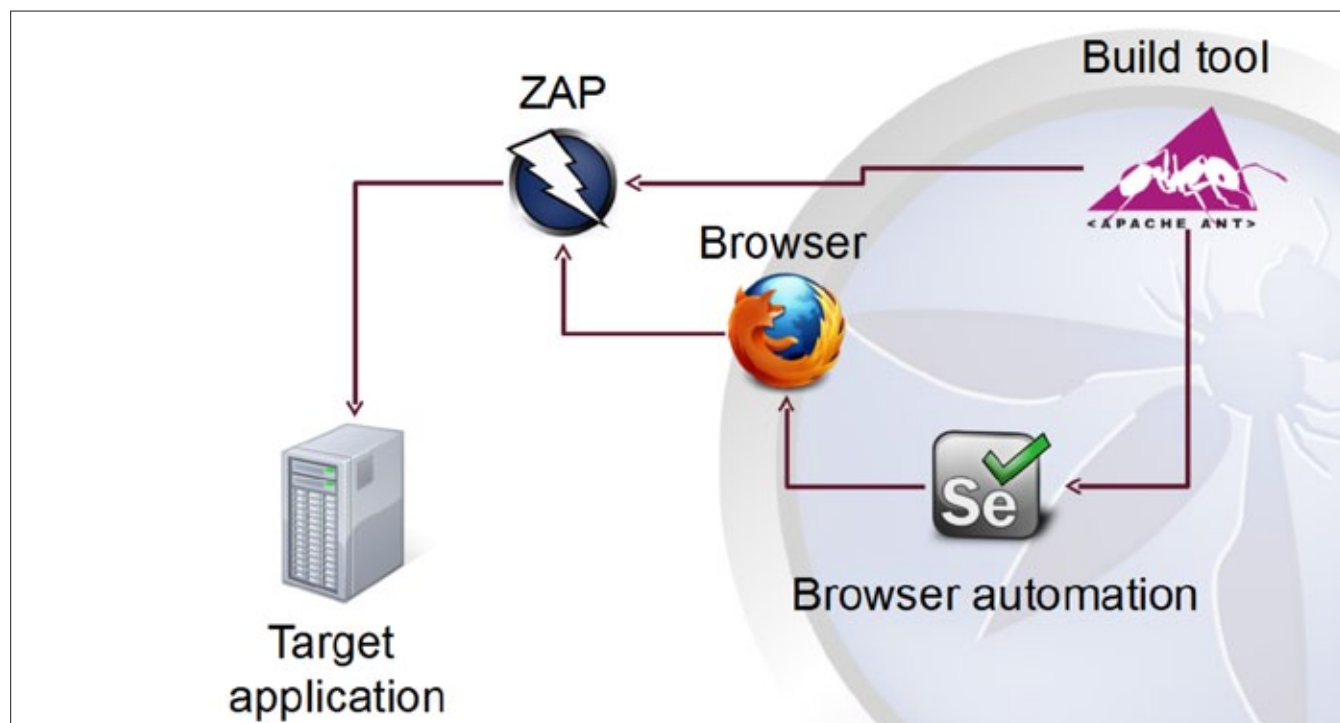


Figure 5. Example ZAP setup for fully automated regression tests with security testing

er. It is also the core technology in countless other browser automation tools, APIs and frameworks.'

A build tool such as Apache Ant can control a tool like Selenium which will drive the browser.

We can then insert ZAP as a proxy and also drive zap from the Apache Ant build tool as in Figure 5.

So selenium records and drives a browser with ZAP inserted as in intercepting proxy. This can be very useful for functional and regression tests and is a very effective way of testing web UI's. Developers can write test cases to use their apps in the way they expect users to use them and then implement and record and re-test them with Selenium.

Regression tests give you a level of confidence that any changes you have made haven't caused any issues or broken anything. They can't test everything, so you still want QA to give your application a good independent test.

In the above example we would use Apache Ant to control ZAP by the rest api, to kick off things like spider and active scanner. This gives some levels of automated security testing that you can use in your continuous integration. The mapping/spider can be set to complete first, then active scan-

ner would be run. The REST API is asynchronous and the will poll the scanner to see how it has progressed.

ZAP will detect passive vulnerabilities such as missing HttpOnly or Secure Cookie Flags whereas the active scanner finds critical XSS and SQLi other vulnerabilities. It is important to remember that there are some types of errors that can not be found with automated scanning, so its important if security is taken seriously in your organisation, to have the security team to have a review and penetration test of your application.

By using ZAP in this way, the basic vulnerabilities in your web application should have been found and then are able fixed in the early stages of the development lifecycle.

For more information and a full video example go to Simon Bennetts video tutorial: <http://code.google.com/p/zaproxy/wiki/SecRegTests>.

Summary

If you're a developer interested in security or a professional pen tester, ZAP definitely has something for you. It is a powerful tool to aid developers and QA testers with easily integrating security in to the SDLC and also serves from beginner up to advanced penetration testers in their line of duty.

It's going to take a lot of work to change the culture of Information Security. It's a risk management project on a grand scale. Get involved, educate, spread the work, take action and help change the culture.

The extensible architecture and constant development of ZAP makes for an exciting future for this Open Source project.

For full instructions and a wealth of ZAP information, see the OWASP project page:

```
WARNING Active scans must not be performed on Public
websites
without the owners written permission as it
illegal.
```

References

Thanks to Simon Bennetts (@psiinon) and Axel Neuman (@a_c_neumann), OWASP, ZAP Guide & Creative Commons Attribute Share-alike License:

- <https://www.owasp.org/index.php/ZAP>
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- <http://www.owasp.org>
- https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- <https://www.owasp.org/index.php/JBroFuzz>
- <http://samurai.inguardians.com/>
- Justin Searle (@meeas)

Google Summer Of Code 2012 Projects

There are 3 ZAP related google summer of code projects:

- Redesign of site crawler with sessions awareness – Student: Cosmin Stefan – Org: OWASP – Mentor: Simon Bennetts
- Enhanced AJAX integration – Student: Guifre Ruiz – Org: OWASP – Mentor: Skyler Onken
- Websocket Testing Tool – Student: robert Koch – Org: Mozilla – Mentor: Yvan Boily

'This is really great news – its a great opportunity for the students to work on a high profile security project, and ZAP will be significantly enhanced by their work!' – Simon Bennetts <http://code.google.com/p/zaproxy/wiki/GSoC2012>.

GARETH WATTERS (@GWATTERS) – CISSP, CISA, CPTE, MCSE, ITIL



Gareth Watters is an Information Security specialist based out of Melbourne Australia.



Virscen Technologies Pvt. Ltd., a Brainchild of a team of **IIT Kharagpur Graduates**, has been **Incubated in E-Cell IIT Kharagpur**. It is an IT Solutions & Training Company, Offering Web, Security and Network Solutions, IT Consulting and Support Services to numerous clients across the Globe.

We provide the following services:

- a. Penetration Testing
- b. Multimedia Services
- c. Web Development
- d. Training:
 - a. Corporate Training
 - b. Classroom Training
 - c. Training programs for Educational Institutions.

Our Partners:

- 1. E-Cell IIT Kharagpur
- 2. Education Project Council of India

Website: www.virscen.com

Blog : www.virscen.com/blog

Wireless Eurynomus

A Wireless (802.11) Probe Request Based Attack

In the recent years, the proliferation of laptop computers and smart phones has caused an increase in the range of places people perform computing. At the same time, network connectivity is becoming an increasingly integral part of computing environments.

As a result, wireless networks of various kinds have gained much popularity. But with the added convenience of wireless access come new problems, not the least of which are heightened security concerns. When transmissions are broadcast over radio waves, interception and masquerading becomes trivial to anyone with a radio, and so there is a need to employ additional mechanisms to protect the communications.

In this article we want to focus on some of the hidden flaws that were never taken seriously. Auto-

connect is a simple and one of the most conniving facility provided by all the clients of wireless Access Points. This feature can also be used to compromise a client and the attack is counted as one of the deadliest silent attacks.

Target Audience

This attack can affect any of the technical and non technical users of the 802.11 interface. But the technical details of this attack require usage of Wireshark, a little understanding of packet details

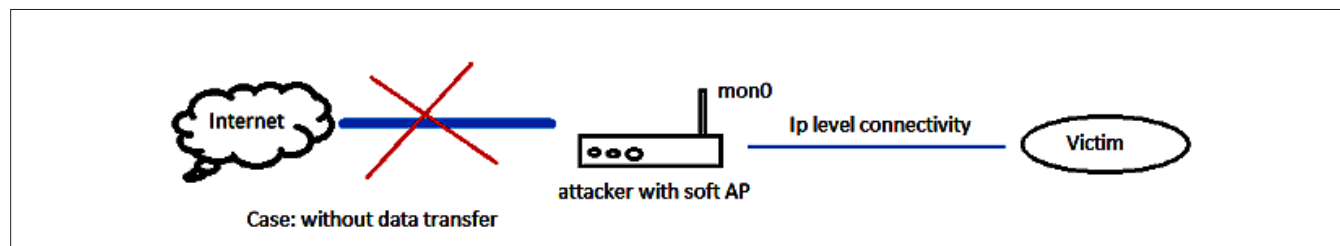


Figure 1. Non-data transfer

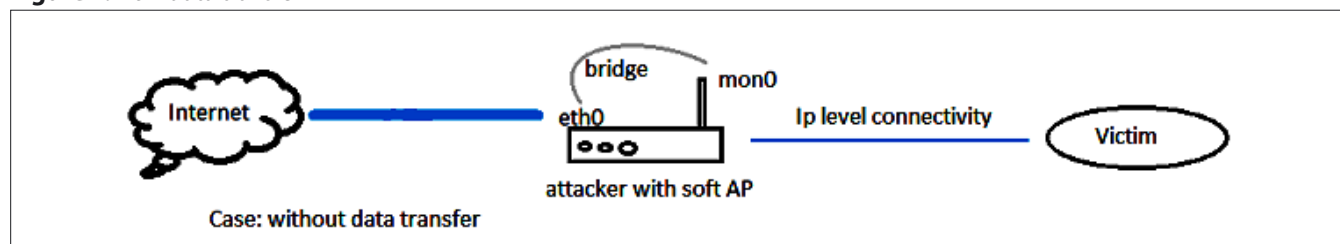


Figure 2. Data transfer to the Internet

over wireless and some of the details about the probe and beacon frames.

Scope Of Attack

This attack is almost new born to the world of wireless and the Internet. This attack is fully capable of creating an intermediate connection between any client and attacker. Talking about the scope of this attack, it can be of wide variety. For example if an attacker walks into a company premises and just by monitoring the air, he can easily find out the probes in air and can attack any laptop or he can attack any smartphone and can collect contact details of clients. This is just a simple scenario; cases can be like T.J maxx credit card incident. (http://news.cnet.com/2100-7348_3-6169450.html)

Flow Diagrams For Attacks

Case -1

Attacker just wants to have connectivity (Non-data transfer; Figure 1). In this scenario, the attacker just wants to have connectivity over the victim, after that he might be interested to do some of the post tasks like launching a Metasploit module or some of the custom coded exploits. And since the victim is only sending the gratuitous request, he will only get some connectivity to the attacker's fictitious network. After that no data transfer will happen because of lack of internet connectivity.

Case – 2

Attacker wants to have connectivity as well as data transfer to the Internet (Figure 2). In this scenario, the attacker wants the victim to connect with the attacker's machine so he could send the data packets to the Internet. In this case he only wants to monitor the data.

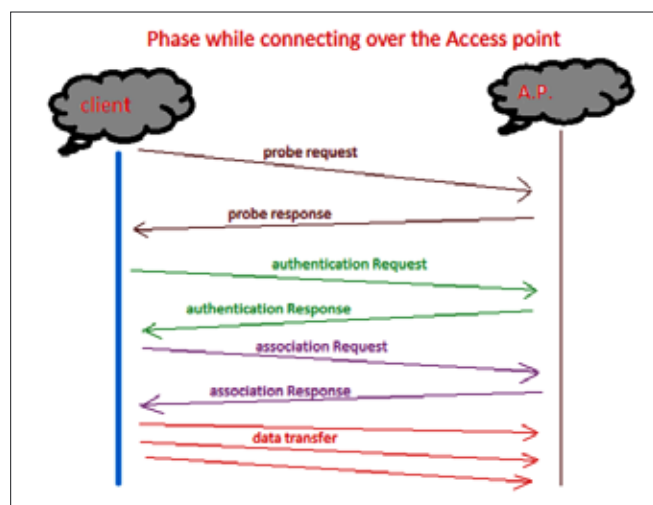


Figure 3. Connecting over the Access point

```
root@bt:~# aironet-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1045     dhclient3
1656     dhclient3
Process with PID 1656 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Realtek RTL8187L      rtl8187 - [phy0]
                      (monitor mode enabled on mon0)
```

Figure 4. Implementation

Hardware And Software Requirements

To perform this attack, we will need an entire lab setup with specific software requirements and some hardware requirements. Hardware requirements include:

- Access point
- 2 laptop (1 as attacker and 1 as victim)
- Wireless card (internal or external)
- 1 smartphone (optional requirement)

Software requirement

- Backtrack operating system (4-revision2 or higher version).
- All other required tools are preconfigured in it.

Understanding Probes And Beacons

When a client turns on its wireless interface, at the same time the wireless interface starts to send many probe requests to find if there is an access point available or not. Similarly any access point is

CH 11][Elapsed: 1 min][2012-05-15 12:37

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:14:C6:00:93:00	-22	132	125	1	11	54	OPN		ZXDSL 531B
00:0E:E9:00:00:00	-71	4	0	0	1	54	WEP	WEP	BSNL 90
E4:00:0F:00:83:00	-71	3	0	0	10	54e	OPN		comcast 90
C8:00:0C:00:96:00	-72	11	0	0	11	54e	OPN		comp128-10
E0:00:F5:00:13:00	-71	1	1	0	10	54e	WPA	TKIP	PSK kiplnetgear

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	5C:00:40:00:00:00	-43	0 - 1	0	29	
(not associated)	1B:00:F4:00:4C:00	-73	0 - 1	0	1	kiplnetgear
00:14:C6:00:93:00	C4:00:FE:00:5E:00	-1	54 - 0	0	19	
00:14:C6:00:93:00	CC:00:AF:00:65:00	-9	54 - 54	243	21	
00:14:C6:00:93:00	BC:00:37:00:82:00	-24	54 - 54	221	33	ZXDSL 531B
00:14:C6:00:93:00	C0:00:DA:00:BA:00	-33	54 - 24	217	57	
00:14:C6:00:93:00	00:00:65:00:58:00	-37	0 - 1	0	20	

probe requests by clients

Figure 5. Probe requests by clients

```
root@bt:~# airbase-ng -a 08:00:27:00:93:00 -e hitesh mon0
12:47:37 Created tap interface at0
12:47:37 Trying to set MTU on at0 to 1500
12:47:37 Access Point with BSSID 08:00:27:00:93:00 started.
```

Figure 6. *airbase-ng*

also sending the beacon frames to show its presence. Once the client gets connected to an access point, there is a facility provided by different machines to remember that access point. Whenever the client comes into the range it automatically gets connected. This is simply because the client is continuously sending probe requests in the air to find if any saved AP is available.

Types Of Attacks

- IP level connectivity attacks (Metasploit based)
- Relay the packets to AP (MITM based attacks)
- Depending upon the usage, attacks can be integrated and the client is still unknown.

Attack Scenario

To understand (Figure 3) this attack, the working of the Access Point must be clear. So, what we are trying to implement is, a client who is not connected to any wireless AP and having his wireless interface up and running. The wireless interface always transmits some probe request from its PNL i.e. Preferred Network List. It is just a sense of insecurity and a shocking fact that it is independent of any AP. First of all we will try to make a monitor mode interface in the air, which can accept all the packets over the air regardless if the packet



Figure 7. Connection to Hitesh network

```
root@bt:~# ifconfig -a
at0      Link encap:Ethernet  HWaddr 08:c0:ca:54:0f:c5
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:20993 (20.9 KB)  TX bytes:0 (0.0 B)
```

Figure 8. *# ifconfig -a*

is destined for it or not. This is very similar to promiscuous mode over the wired network, used for the purpose of sniffing. After finding the probes of the clients, we will create a soft AP or known as virtual AP. A soft access point is created by a set of software which continuously sends out the beacon frames to show all nearby clients about its presence. Since the client is already attempting to connect to that access point. It will automatically connect to the attacker. Now, if a DHCP is running over the attacker it will automatically receive an IP or if there is no DHCP is running then client will receive an IP of the range 169.xxx.xxx.xxx will sent gratuitous packets. Once the IP is assigned, the tap interface created by soft AP, can have IP level connectivity with the client and the best part is that the client remains unaware of the situation.

Implementation

We have used a BackTrack machine (attacker) and a I-Phone (victim) to implement our attack scenario. A monitor mode interface is being created at the top of a wireless interface, this monitor mode interface can be easily created by using airmon-ng set of tools. The wlan0 (wireless) interface is up and running (Figure 4).

```
# airmon-ng start wlan0
```

Monitor mode enabled on `mon0` indicates that the monitor mode has been created and now we can monitor the air. To monitor the air, simply `airodump` can be used over the `mon0` interface. This along

```
root@bt:~# ifconfig at0
at0      Link encap:Ethernet  HWaddr 08:c0:ca:54:0f:c5
          inet addr:169.254.28.8  Bcast:169.254.28.255  Mask:255.255.255.0
          inet6 addr: fe80::2c0:caff:fe54:fc5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:32545 (32.5 KB)  TX bytes:1014 (1.0 KB)

root@bt:~# ping 169.254.28.3
PING 169.254.28.3 (169.254.28.3) 56(84) bytes of data.
64 bytes from 169.254.28.3: icmp_seq=1 ttl=255 time=12.5 ms
64 bytes from 169.254.28.3: icmp_seq=2 ttl=255 time=7.32 ms
64 bytes from 169.254.28.3: icmp_seq=3 ttl=255 time=8.05 ms
64 bytes from 169.254.28.3: icmp_seq=4 ttl=255 time=8.05 ms
64 bytes from 169.254.28.3: icmp_seq=5 ttl=255 time=8.08 ms
64 bytes from 169.254.28.3: icmp_seq=6 ttl=255 time=7.34 ms
^C
--- 169.254.28.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/ndev = 7.328/8.563/12.523/1.802 ms
```

Figure 9. *# ifconfig at0; # ping 169.254.28.3*

References

- [1] www.aircrack-ng.org
- [2] www.aircrack-ng.org/doku.php?id=airodump-ng
- [3] www.wireshark.org/
- [4] Interception Mobile Communications, The Insecurity of 802.11 – ISAAC www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
- [5] An Overview of 802.11 Wireless Network Security Standards & Mechanisms
- [6] By: Luis Wong (posted on January 19, 2005)
- [7] Remote Access Point/IDS
- [8] By: Jared Kee (posted on April 10, 2012)

Comments

- Type of access point used for testing – a zxdsl router for this attack as a lab setup, but it will hardly matter if you use any other also, since all router broadcast same beacon frames

- Type/model of wireless cards have been used for testing – an alfa wireless external card AWUS036H series, but anyone can use their laptop inbuilt card
- Victim can have any operating system like windows xp or 7 or even linux machine, the probe request will always be sent into the air, since this is how the the wireless auto connect feature works in all operating system. I didn't tested it on MAC, and cannot say much about it. Regarding the antivirus that comes to the post exploitation task, and if any ATTACKER wants to have Man In the Middle attack to perform, then a fully patched (with antivirus and firewall) machine can be compromised. because its the victim who is trying to connect to us.
- I used a IOS4 – jail broken version for this experiment purpose.

Acknowledgment

Acknowledgment to Igneustech for providing appropriate equipment and lab environment.

with the AP will also give the details of the clients that are associated or trying to associate with the network in the surroundings (Figure 5)

```
# airodump-ng mon0
```

After finding the probe request name, the attacker can easily create a soft AP or virtual access point with any of the bssid as well as any essid. Here I have used an essid of name Hitesh just for the sake of example.

```
# airbase-ng -a <bssid> -e <ssid/name> mon0
```

The Airbase set of tools has got a lots of options, it can send responses to any of the probe requests that client is transmitting via its radio but for the sake of simplicity we have used this scenario. The interesting thing about this soft AP is that it also creates a tap interface. It's little basic that our access point always have 2 cards in it, one is wireless and other is for wired interface. This tap interface is the same clone of wired interface named as `at0`. (Figure 6). As a result of this client will automatically get connected to this "hitesh" network since there is no DHCP running over the attacker machine (Figure 7).

The client will get an IP address of the range 169.xxx.xxx.xxx and will try to send gratuitous packets. One can also use these packets as an ARP packet to send it back to the IP. So, there is can be attack at every phase. One can also verify this by using Wireshark and capturing each and every packet. These packet will show that client is again and again trying

to send DHCP request and failing so that finally it is getting an IP range 0f 169.xxx.xxx.xxx. In the mean while one can also set a DHCP and can easily transfer the packets to the Internet via its bridge interface and can perform Man In The Middle Attacks. Now the final step is to just up the `at0` interface and set the ip of the same range and same subnet that can be easily done with the `ipconfig` utility (Figure 8)

```
# ifconfig -a
```

Finally the proof of the IP level connectivity, Post that one can easily launch some Metasploit modules or other various set of attacks (Figure 9).

```
# ifconfig at0
# ping 169.254.28.3
```

HITESH CHOUDHARY



Hitesh Choudhary is a Jaipur based ethical hacker serving free to Rajasthan police to handle cyber crimes as well as pursuing his wireless research at M.I.T., California. He has completed his RHCE, RHCSA, CEH and various other security certifications.



PANKAJ MOOLRAJANI

Pankaj Moolrajani is Jaipur based security researcher at Igneustech. He is RHCE & RHCSA Certified.

Securing Users

from Phishing, Smishing & Social Media Attacks

Some experts believe one of the best solutions to thwart phishing attacks is end-user training, but can we really train every computer user to be sufficiently security literate? Will it ever be the case that anyone can distinguish a phishing message from a genuine bank email?

The volume of phishing attacks has increased, as have their variety and sophistication. Even security experts struggle to identify some of the fakes. The phishers cast their rods farther and with more efficiency than ever before. They can easily download phishing site creation tools and produce convincing messages and pages. Expecting an average PC user to beat these guys without any help is tantamount to pitting an average golfer against Tiger Woods.

It can seem at times the only people who like change are Internet attackers. And they don't just like it – they *need* it. Technology's rapid changes give cybercriminals new attack vectors to exploit, and new ways to turn a profit out of someone else's misfortune.

Internet attackers have made a profession out of rapid change of a multitude of factors – attack vector, sophistication, volume and approach. The malware market has been monetised and we are seeing the strongest ever driving forces to come up with new approaches to beat security products and users common sense.

For example, take phishing. The concept is simple: Send an email disguised as a message from a bank, PayPal, or UPS. Wait for the user to click a link in the message, and enter their private details into a phishing site, and presto! The attacker

attains financial or personal login details that can be used to commit fraud or theft. Of course, it was only a matter of time before people caught on to email scams. Users read again and again not to click on such links. Mail solutions became better at spotting phishing emails and filtering them into a junk email folder. Even free Web mail providers now catch the majority of these attacks.

Once cybercriminals noticed their traditional phishing approaches were returning lower response rates, they rapidly adjusted to new mediums. As a result, a new trend emerged: *smishing* (social media phishing and SMS phishing) became the new trend in cyber attacks.

The underlying concept is the same, but the attack mechanism is different. Instead of targeting users via email, cybercriminals use social media messaging and text messaging advertising to lure victims.

For hackers, it's the perfect opportunity. They can cheaply buy lists of Facebook login details, hack into users' accounts, and send personal-looking messages to an individual's entire friend list. The majority of users are more trusting of a post from a friend than a suspicious email in their in-box, making smishing more effective at luring users to phishing sites.

We seem to take phishing attacks for granted these days, in much the same way that we've ac-

cepted spam as a natural, and inevitable, by-product of email. Some experts believe one of the best solutions to thwart phishing attacks is end-user training, but I doubt training alone is a viable solution. Can we really train every computer user to be sufficiently security literate, such that anyone can distinguish a phishing message from a genuine bank email? I doubt its possibility, especially given how specific the details in spear phishing (phishing targeted at specific people and/or companies) attacks have become.

It used to be that thieves could satiate their hunger for evil (and money) merely through the emulation of a consumer bank or a PayPal login screen. While these low-hanging-fruit scams show no signs of abating, even following major busts of phishing rings, we've seen new types of phishing attacks that wear the mask of a Web security product, persuading users to follow through on fake spam quarantine messages, or security update alerts, sometimes using the name of real vendors. It's all very plausible.

Unfortunately, the average user is not a trained security expert – and why should he or she be? Criminals lure users into phishing and email scams in much the same way street cons lure some peo-

ple into losing their wallet at Three-card Monte. We let curiosity get the best of us, and at times can be gullible. Like street hustlers, cybercriminals aren't afraid to experiment with hacking our inclinations (or, as many security experts call it, *social engineering*). The volume of phishing attacks has increased, as have their variety and sophistication. Even security experts struggle to identify some of the fakes.

The phishers cast their rods farther and with more efficiency than ever before. They can easily download phishing site creation tools (yes they exist) and produce convincing messages and pages. Expecting an average PC user to beat these guys without any help is tantamount to pitting an average golfer against Tiger Woods (albeit a few years ago; no offense, Tiger). The criminal's job is to create online scams that work, and the returns on their investments are huge. Why would we expect non-criminally-minded users to be more adept at spotting scams, than scammers are at reeling in the users?

Technology has to step up its game. We need to continue to make it harder and less lucrative for online scammers to do their "jobs." That's really the most effective way to stop phishers from attacking our end users.

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



Web Based CRM & Business Applications for small and medium sized businesses

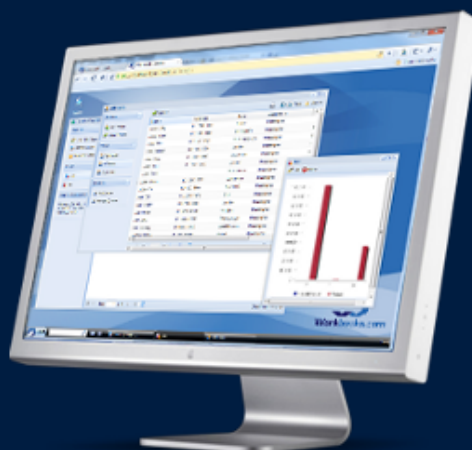
Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

Contact Us to Find Out More

+44(0) 118 3030 100

info@workbooks.com



Phishing is a good example of how the Cybercriminal utilises Social Engineering techniques combined with technology to grift money from an innocent Internet bystander. Send an email to the victim purporting to be from someone else, be it a bank, paypal or from a spyware infected machine disguising the email in the form of a genuine email from a friends address. Wait on the susceptible user to click on it believing it to be genuine, enter their private details into a fake site and hey presto the attacker has hoodwinked you and has financial or personal login details of yours. The average phishing site that stays online for an average of 5.9 days does enough damage to afford change (stat from APWG.com – the Anti-Phishing Workgroup).

Users have read again and again in articles, in warnings on bank sites, in email services and from friends not to click on such links, but they still do! Mail solutions have gotten better at discerning Phishing attacks and putting them correctly in to anti-spam filters. Even in free webmail solutions Phishing attacks are put into the junk folder the majority of the time. So users believe the Phishing mails won't reach them and they think twice before they click on a suspicious email.

So have the criminals sat on their laurels!? When they noticed the traditional Phishing approaches returning a lower response rate they rapidly adjusted to new mediums and we now have this new format of Smishing with two definitions, both harmful and both sophisticated enough to be impacting users. Variouslly termed as meaning Social Media phishing or SMS Phishing they are both a progression of attackers approaches.

Social Media Phishing means instead of sending the advert, fake link, or message in email they are utilising social media messaging and advertising to direct the user through to their fake site location. Getting a posting on to your Facebook page for example or receiving a Social Media message seemingly has more trust equity with users than email, with users believing fakes only come to them in email as Spam. On Social web sites they seemingly have entered into a different mindset of trust.

You can cheaply buy lists of Facebook login details on the web – for example a recent site was seen offering 1000 facebook account login details for L16.50, very affordable at the worst of times. With such easy ammunition it's not a big step for someone to utilise each of these accounts and to send personal looking messages

to all linked friends of the individual, sending a 'have you see this site' message, an advert or simply a link to a fake site. Users are lulled into a greater trust of the message, having not been use to receiving this sort of message in this new more trusted medium.

SMS Phishing involves criminals switching their attacks to target a weaker link. Users are constantly educated to maintain suspicion when opening messages in email on a PC device and typically have security software running on these machines, be it antivirus, spyware protection, firewalls and other mediums of protection. Users have become rapidly more mobile and take for granted the ability to now access the internet from devices other than their PC. Text messaging has become a 'taken for granted' communications medium with many youngsters sending/receiving upwards of 100 messages a day.

Attackers have found ways to send masses of automated and believable looking text messages to users including URL links for the user to view.

Major PC based web browser software now has phishing protection built in to alert the user to suspicious sites, and users generally can hover over a link to display the true web site, but on mobile phones we are not seeing the same browsers, the same versions nor the same protection levels to help users avoid malicious fake sites.

So user beware, what you see may not always be what you get, particularly in the world of the cyber transaction. When you see a message from someone you think you know, don't assume it was them who sent it from their account, look once, think twice before you click, whether it be an email, a social media message or a text message!

IAN MOYSE



Ian Moyse has over 25 years of experience in the IT Sector, with nine of these specialising in security For the last 8 years he has been focused in Cloud Computing and has become a thought leader in this arena. He now holds the role of Sales Director at Cloud CRM provider Workbooks.com. He also sits on the board of Eurocloud UK and the Governance Board of the Cloud Industry Forum (CIF) and in early 2012 was appointed to the advisory board of SaaSMax. He was named by TalkinCloud as one of the global top 200 cloud channel experts in 2011 and in early 2012 Ian was the first in the UK to pass the CompTIA Cloud Essentials specialty certification exam.

He also sits on the board of Eurocloud UK and the Governance Board of the Cloud Industry Forum (CIF) and in early 2012 was appointed to the advisory board of SaaSMax. He was named by TalkinCloud as one of the global top 200 cloud channel experts in 2011 and in early 2012 Ian was the first in the UK to pass the CompTIA Cloud Essentials specialty certification exam.



scanning isn't enough

Cyber Security Auditing Software

- Device information remains confidential
- Settings that allow you to hide sensitive information in the report
- Low cost, scalable licensing
- Point and click GUI or CLI scripting
- Audit without network traffic

“It was refreshing to discover Nipper and to find that it supported so many devices that Cisco produces. Nipper enables Cisco to test these devices in a fraction of the time it would normally take to perform a manual audit. For many devices, it has eliminated the need for a manual audit to be undertaken altogether.”

Cisco

Business Benefits to Cisco

- Nipper quickly produces detailed reports, including known vulnerabilities.
- By using Nipper, manual testing has been altogether eliminated for particular Cisco devices.

Multi-Platform Support for



Device Auditing	Scanners	Nipper Studio
Audit without Network Traffic	✗	✓
Authentication Configuration	✗	✓
Authorization Configuration	✗	✓
Accounting/Logging Configuration	✗	✓
Intrusion Detection/Prevention Configuration	✗	✓
Password Encryption Settings	✗	✓
Timeout Configuration	✗	✓
Physical Port Audit	✗	✓
Routing Configuration	✗	✓
VLAN Configuration	✗	✓
Network Address Translation	✗	✓
Network Protocols	✗	✓
Device Specific Options	✗	✓
Time Synchronization	✗	✓
Warning Messages (Banners)	✓ *	✓
Network Administration Services	✓ *	✓
Network Service Analysis	✓ *	✓
Password Strength Assessment	✓ *	✓
Software Vulnerability Analysis	✓ *	✓
Network Filtering (ACL) Audit	✓ *	✓
Wireless Networking	✓ *	✓
VPN Configuration	✓ *	✓

* Limitations and constraints will prevent a detailed audit

Nipper Studio reduces manual auditing time by quickly producing a consistent, clear and detailed report. This report will;

1. Summarize your network's security
2. Highlight vulnerabilities in your device configurations
3. Rate vulnerabilities by potential system impact and ease of exploitation (using CVSSv2 or the established Nipper Rating System)
4. Provide an easy to action mitigation plan based on customizable settings that reflect your organizations systems and concerns.
5. Allow you to add previous reports and enable change tracking functionality. You can then easily view the progress of your network security.

evaluate

for free at

www.titania.com

enquiries@titania.com
T: +44 (0)845 652 0621

Digital Apocalypse

The Artillery of Cyber War

Cyberspace is now the digital frontier of choice for executing many combat operations, by extending the medium in which greater levels of power can now be accessed by Machiavelli agents, militants and nation-states. Squads of cyber militants going under the banner of Anonymous and LulzSecare, motivated by the ease in which they can now execute high impact operations whilst avoiding detection, are just a few of the much publicised names synonymous with cyber terrorism.

The multi-dimensional characteristics of cyber space have dissolved the boundaries between digital landscape and physical security, facilitating cyber-attacks that produce devastating impacts to critical infrastructure, as well as Corporate and Government assets.

Global security experts face the challenge of attempting to develop techniques to deter and prevent these global threats. This challenge is complicated further by the rate at which the digital paradigm continues to evolve at a rate which is often considerably faster than the ability to keep up with these developments. This disparity has, unsurprisingly, created an impression, shared throughout the cyber community, that implementing strategies to control the digital domain has become unachievable. As a result of these challenges and many others, Cyber Warfare is set to be one of the greatest challenges posed to the 21st Century.

This article will examine the characteristics of Cyber War operations in order to clarify the ambiguities surrounding these concepts. Such an examination is necessary in order to ensure that the components of Cyber War are not confused with interrelated disciplines such as Information Warfare. Real world examples of Cyber Attacks will then be discussed in order to assess the “nuts and bolts” of cyber-attack operations and to examine whether

the world is really prepared for the possibility of a “digital apocalypse”. Throughout the analysis this paper aims to emphasise that deterring Cyber War is the key to addressing this challenge.

Cyber Warfare – A Definition

Over the past few decades experts and academics have explored whether the possibility of a Cyber War was in fact a plausible threat. Early pioneers navigating through this new landscape had conjured up post-apocalyptic visions of the impact of Cyber War, bearing resemblances to scenes from a science fiction film. Today, Cyber War is no longer being examined from a theoretical perspective, as these dynamic threats have emerged throughout the global systems and networks. Experts are no longer debating the possibility of Cyber War but what can be done to stop these threats.

Despite the widespread acknowledgement of Cyber War, the definition of these threats remains under scrutiny. Experts such as Bruce Schneier have stated that many definitions of Cyber War in current circulation are flawed as they confuse a range of other computer security related concepts such as Information Warfare, Hacking and Network Centric Warfare. In order to, clarify ambiguities surrounding Cyber War, for the purpose of this discussion, Cyber War is defined as:

“Internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems – among many other possibilities.” (Rouse, 2010)

For the purpose of this discussion, the focus of Cyber War conflicts will be examined in terms of its impact to the physical realm, in particularly to its impact to critical infrastructures.

The First Warning Shots

Recorded examples of the impact of cyber-attacks on critical infrastructures have been around for over a decade. One of the earliest cyber-attacks on critical infrastructure took place in January 2000, in Queensland, Australia. Where a disgruntled former employee at a manufacturing company hacked into the organisations computer, using privileged knowledge of the system, and took control of the *Supervisory Control and Data Acquisition* (SCADA) system. The protagonist was able to maliciously attack the system causing physical pumps to release raw sewage, producing a considerable amount of damage. Although this attack is not constituted as cyber warfare, it demonstrated the possibility for a digital attack to create a detrimental financial impact and create havoc on critical infrastructures. Since this time, there have been a number of attacks classed as acts of cyber war, such as the 2007 attacks, launched against the Government of Estonia. In this example, attackers utilised a variety of different attack methods such as Denial of Services (DoS), website defacement and other malware. This was one of the earliest examples demonstrating the increased level of sophistication of cyber-attacks to be launched against a nation-state.

The Digital Artillery

The arsenal of a Cyber War attack consists of the usual suspects, such as DoS, attacks on DNS infrastructure, anti-forensic techniques, and wide-scale use of Worm, Zombies, Trojan and clichéd methods of electronics attack. However Cyber War represents much more than a DoS attack. When assessing state-of-the-art Cyber War Artillery, one name comes to mind – Stuxnet.

State-of-the-Art: Stuxnet

The ultimate state-of-the-art weapon identified in the cyber warfare arsenal, so far, is the Stuxnet

worm. First launched in to the digital landscape in June 2009, Stuxnet has become one of the heavily scrutinised, real world examples of Cyber Warfare attacks, with global security and technology communities still struggling to fully comprehend the complexities of its design almost two years on since its initial release. Stuxnet’s international attention has been achieved from the sheer sophistication in design which is composed of a comprehensive array of attack exploits and covert methods for avoiding detection. Stuxnet is the magnum opus in the malware hall of fame.

The Stuxnet worm infects computers running Windows OS, and is initially distributed via USB drives thereby enabling it to gain access to systems logically separated from the Internet. Once access has been gained it then orchestrates a variety of exploits from its toolkit designed to specifically target vulnerabilities its intelligent design is able to identify in the target host.

Stuxnet’s artillery includes uses an array of exploit methods, meticulously designed to circumvent the logical sequence security measures, one layer at a time. Exploits included Stolen Digital Certificates, Rootkits, Zero-Day Exploits, methods for evading Anti-Virus detection, hooking codes, complex process injections, network injection, to name a few. These exploits however do not affect just any old computer, aside from propagating further. The extraordinarily designed piece of malware has one solitary target in mind – Industrial Control Systems/Supervisory Control and Data Acquisition* (ICS/SCADA) and attached computer systems. With a specific ICS/SCADA being targeted in Iran, Stuxnet reprograms the Programmable Logic Controller (PLC), made by Siemens, to execute in the manner that the attack designers have planned for them to operate within.

* Bruce Schneier argues that Stuxnet only targets ICS and press releases have mis-referenced Stuxnet to also target SCADA “is technically incorrect”. For further details refer to: <http://www.schneier.com/blog/archives/2010/10/stuxnet.html>

While experts are still dissecting Stuxnet, it is apparent that the creation is the work of a team of highly skilled professionals. Some estimates have stating that it would have taken a team of 8 – 10 security experts to write over the course of 6 months (Schneier). Many are referring to Stuxnet’s creation as a “marksman’s job” due to its targeted approach and expert precision.

Given Stuxnet is considered to be one of the greatest malware masterpieces the temptation

to examine its architecture in greater detail could not be resisted. Symantec's "W32.Stuxnet Dossier Version 1.4" provides a detailed analysis delineating the technical attributes composed within Stuxnet and this 69 page document created by members of their Security Response Team is used as the basis for the following examination. The full array of technical features is outside of the scope of this article so a brief overview of Stuxnet's architectural components will be summarised below.

Breaking Down Stuxnet

The Core – .DLL files

At the core of Stuxnet is a large .dll file containing an array of resources, diverse exports as well as encrypted configuration blocks. In order to load these .dll files, Stuxnet has the capability to evade detection of a host intrusion protection programs which monitor any LoadLibrary calls. These .dlls and encrypted configuration blocks are stored in a wrapper referred to as the 'stub'. Two procedures are then employed to call Exported function. Extract .dll is then mapped into memory module and calls one of the exports from mapped .dll. A pointer to the stub is then passed as a parameter. Stuxnet then proceeds to inject the entire DLL into another process, once exports are called. Injecting processes can include existing or newly created arbitrary process or a pre-selected trusted process.

The Process of Injection

Targeted trusted processes are directed at a number of standard Windows processes associated with a range of security products, including – McAfee (*Mcshield.exe*); Kaspersky KAV (*avp.exe*); Symantec (*rtvscan.exe*); Symantec Common Client (*ccSvcHst.exe*); Trend PC-cillin (*tmpproxy.exe*) to name a few. Stuxnet then searches the registry for any indication that McAfee, Trend PC-cillin or Kaspersky's KAV (v.6-9) software is in operation. If Stuxnet is able to identify any of these technologies it then extracts the version which is used to target how to process injections or whether it is unable to by-pass these security products.

Elevation of Administrative Access Rights

Another feature of Stuxnet is in its ability to elevate access rights to run with the highest level of privileges possible. Stuxnet detects the level of privileges assigned to it and if these are not Administrative Access Rights it then executes zero-day privilege escalation attacks, such as MS10-073.

The attack vector used is based on the operating system of the compromised computer. If the operating system is Windows Vista, Windows 7, or Windows Server 2008 R2 the currently undisclosed Task Scheduler Escalation of Privilege vulnerability is exploited. If the operating system is Windows XP or Windows 2000 the Windows Win32k.sys Local Privilege Escalation vulnerability (MS10-073) is exploited.

Load Points

Stuxnet loads the driver "MrxCls.sys" which is digitally signed with a compromised Realtek certificate (which Verisign previously revoked). Another version of this driver was also identified to be using a digital certificate from JMicron.

The aim of the Mrxccls.sys is to inject copies of Stuxnet into specific processes therefore acting as the central load-point for exploits. Targeted processes include – *Services.exe*; *S7tgtopx.exe*; *CCProjectMgr.exe*.

The Target: Programmable Logic Controllers

We now arrive at Stuxnet's ultimate goal – infecting Simatic's Programmable Logic Controller (PLC) devices. Stuxnet accomplishes this by loading blocks of code and data (written in SCL or STL languages) which are then executed by the PLC in order to control industrial processes. In doing so, Stuxnet is able to orchestrate a range of functions such as:

- Monitoring Read/Writes PLC blocks
- Covertly masks that the PLC is compromised
- Compromise a PLC by implementing its own blocks or infecting original blocks.

The Grand Finale

Now that Stuxnet has finally exploited the PLC it has achieved it has reached its final destination. Where Stuxnet is then able to execute its final exploits which is to slow down or speed up frequency motors. For example when the frequency of motor is running between 807Hz and 1210Hz, Stuxnet adjusts the output frequency for shorter periods of time to 1410Hz and subsequently to 2Hz and then back to 1064Hz. These frequencies are typically used by centrifuges in uranium enrichment plants. Ultimately Stuxnet is designed to destabilize ICS/SCADA by changing the speeds in uranium centrifuges to sabotage operations, with the potential for devastating consequences.

Little Brother – Duqu

In the September of 2011, researchers at the Budapest University's Laboratory for *Cryptography and System Security* (CrySyS) made the alarming discovery of a Trojan resembling Stuxnet. Their fears were confirmed after dissecting this new threat revealed components were close to being identical to Stuxnet indicating that the writers were indeed the same authors, or persons with access to the source code of Stuxnet. They labelled this new threat "Duqu" due to its design in which it creates file names with the prefix ~DQ.

Duqu is a remote access Trojan designed to steal information from the victim machine and is designed to act as a precursor to a future malware attack, similar to the Stuxnet operation. Duqu is designed to act in much the same way as a reconnaissance agent gathering intelligence from a variety of targets, and like Stuxnet; Duqu's primary targets are industrial infrastructure. Data sources collected by this Trojan include design documents, keystrokes records and other system information. Once this intelligence has been gathered by the Trojan, it is then returned to the command and control servers, over HTTP and HTTPS, positioned across global locations such as China, Germany, Vietnam, India and Belgium. This information can then be used by Duqu's creators to then launch a premeditated cyber assault against the designated target. By default Duqu is designed to operate for a set period of time (either 30 or 36 days depending on the configuration). After which the Duqu will automatically remove itself from the system. A comparison of Duqu and Stuxnet demonstrates:

- Duqu's executables were created using the same source code as Stuxnet.
- Duqu's payload resembles no similarity to that of Stuxnet. Duqu's payload is written with the intention of conducting remote access capabilities whereas Stuxnet's payload is designed to sabotage an ICS/SCADA.
- Duqu's Payload aims to capture keystrokes and system information rather than modify target systems.
- Duqu (being a Trojan) do not contain any self-propagation capabilities as found in worms like Stuxnet.
- Duqu in one example is distributed by attackers using specially crafted email containing a word document which exploits an unpatched 0-day vulnerability to

- Like Stuxnet, Duqu's utilities include stolen signing certificates for signing drivers stolen from a company in Taiwan, with an expiry date of August 2nd 2011. These certificates were later revoked on October 14th 2011.

The resemblances in design of Stuxnet and Duqu indicate that they were most likely developed by the same authors. Kaspersky Lab's Analysts examining the source code of both programs state that – "We believe Duqu and Stuxnet were simultaneous projects supported by the same team of developers".

The Launch Pad – Tilded

How did Stuxnet and Duqu manage to launch some of the most effective cyber-attacks on record so far? The "launch pad" for this cyber artillery goes by the name of Tilded.

The Tilded platform is modular in nature and is designed to conceal the activities of malicious software by employing techniques such as encryption, thereby evading detection by anti-virus solutions. By utilising the Tilded platform developers of cyber weapons can simply change the payload, encryption techniques or configuration files in order to launch any number of exploits against a range of targets. File naming conventions used by Tilded's developers employed the Tilde symbol and the letter "d" combining the two resulted in adopting the name – Tilded. The Tilded team of developers however still remain unknown.

What we do know about Tilded is that it has undergone significant changes since its inception in 2007 with subsequent revisions created through to 2010. The researchers at Kaspersky have been able to confirm that a number of projects were undertaken between this period where programs based on the "Tilded" platform were circulated in cyberspace, Stuxnet and Duqu being two examples. While other researchers have indicated another variant exists, the Stars worm (also targeting ICS/SCADA systems) resembles Stuxnet. How many other programs have also been created but may not yet have been detected remains to be determined. What is clear is that as Tilded and similar programs continue to develop, we will see enhanced prototypes being catapulted into the digital limelight.

Are We Prepared for a Digital Apocalypse?

On the May 6th 2012, the US Department of Homeland Security reported that a major Cy-

References

- Clayton, M. (2012). Alerts say major cyber attack aimed at gas pipeline industry. Retrieved 12th of May 2012 from: http://www.msnbc.msn.com/id/47310697/ns/technology_and_science-christian_science_monitor/t/alerts-say-major-cyber-attack-aimed-gas-pipeline-industry/#.T65jgesti8D
- Kamluk, V (2011). The Mystery of Duqu: Part Six (The Command and Control servers). Retrieved 12th of May 2012 from: http://www.securelist.com/en/blog/625/The_Mystery_of_Duqu_Part_Six_The_Command_and_Control_servers
- Kovacs, E. (2011). Stuxnet, Duqu and Others Created with 'Tilded' Platform by the Same Team. Retrieved 12th of May 2012 from: <http://news.softpedia.com/news/Stuxnet-Duqu-and-Others-Created-with-Tilded-Platform-by-the-Same-Team-243874.shtml>
- RAND (2009). Cyberdeterrence and Cyberwar. Retrieved 12th of May 2012 from: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf
- Rouse, M. (2010) Cyberwarfare. Retrieved 12th of May 2012 from: <http://searchsecurity.techtarget.com/definition/cyberwarfare>
- Schneier, B. (2010) Stuxnet. Retrieved 12th of May 2012 from: <http://www.schneier.com/blog/archives/2010/10/stuxnet.html>
- Symantec (February 2011). W32.Stuxnet Dossier Version 1.4. Retrieved 12th of May 2012 from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- Symantec (November 2011). The precursor to the next Stuxnet W32.Duqu Version 1.4. Retrieved 12th of May 2012 from: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
- Teksouth Corporation (2010). Cyber Warfare in the 21st Century: Guiding Doctrine and an Initial Conceptual Framework. Retrieved 12th of May 2012 from: <http://www.slideshare.net/slahanas/cyber-warfare-doctrine>
- Westervelt, R. (2012). Tilded platform responsible for Stuxnet, Duqu evasiveness. Retrieved 12th of May 2012 from: <http://searchsecurity.techtarget.com/news/2240113299/Tilded-platform-responsible-for-Stuxnet-Duqu-evasiveness>

ber Attack was being launched against computer systems used for a national gas pipeline company supplying a total of twenty five percent of the United States energy. The cyber strike has been traced back to a single source and many experts believe that this is an early indicator of a highly organised Cyber Warfare operation. Early detection of the warning signs of such an attack has instilled reassurance throughout the wider global community that adequate mechanisms are now in place to ensure, at the minimum, a wide-scale cyber-attack will be detected and deterred prior to it accomplishing any major impact.

As discussed, the dynamic and often unpredictable composition of emerging threats reveals the critical need for developing new strategies within the Cyber Security community, so that detection of these unconventional threats can be done so with greater accuracy and prior to them developing the capability to orchestrate operations. RAND Corporation has stated that as long as systems have flaws, Cyber-attacks will be possible and "... as long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk". Deterrence therefore is the key.

Despite these challenges, real progress is being made. As the nature of Cyber Warfare becomes better understood, in spite of its complexities, a

foundation for understanding these multifaceted threats is now being established. The next challenge being faced is in developing strategies/frameworks to deter the motivational factors leading to the creation of these threats whereby influencing the mindset of cyber militants will be the key defence mechanism available to preventing a digital apocalypse.

CECILIA MCGUIRE



Cecilia McGuire is a dynamic fresh thinker and quiet achiever. Like many Gen-Y's, she has spent the past decade living a somewhat nomadic existence having worked globally, expanding her awareness of international security requirements and foresight into upcoming trends. She attributes much of her influence to growing up in an unconventional family in rural Australia, amongst a blend of western and eastern philosophical paradigms. In 2010, she completed a Masters of Information Security and now lives in Sydney where she works as a Security Consultant.



Get prepared.

We are Expanding Security, a Pen Testing and Training Company. We've been preventing deer-in-headlights look since 2006. We offer Pen Testing services plus our Live On Line training classes for ISSMP, ISSAP, CISSP, and Certified Ethical Hacker. We give you online access to materials wherever you are.



You need to keep your job secure, your business strong, and your staff on top of the game. See how good and fun training can be. Our courses are current to changing technology, and our training is the fastest, easiest way to master the relevant data you need NOW.

Sign up for our free weekly PainPill and come to a free class.

<http://www.expandingsecurity.com/PainPill>

...with Freedom, Responsibility, and Security for All TM

www.ExpandingSecurity.com

The Box holes

Pen Testing a SCADA platform

Midnight.

It is hot and humid down here... Temperature is at 36 Celsius.

The temperature processor should start computing the increased level and begin to compensate.

The core is up to 84 Celsius, but in less than a minute the injectors should start their work.

Unless some problems...

"I have not heard the fan starting Abder... what's wrong?"

The voice erupts from a badly regulated radio speaker...

"I don't know Raman!...", says Abderrahim quickly moving his wheeled chair between two segment of the main panel in the control room.

Looking to the side panel Abderrahim found two minor alarms... "what's wrong?" abruptly says...

The alarms have been activated by two unauthorized attempts to access the terminal remotely...

"Hey Abder... the fan hasn't started to lower water temperature level... what's wrong?" Raman voice increases his intensity.

"Buzzer begins to signal core overheating! You must do something quickly!..." a slight sense of panic betray Raman words. A panic that Abderrahim founds appropriate for the situation.

Ok. Let's try our manual start procedure... but what means this new panel alarm? What's on the console?...

A yellow message over a black screen on other side of the panel says "Smile u been pwnd... your coffee pot should blow up your ass!"

Damn Kids! The manual start doesn't work...

"Raman! You hear me? The manual re-start of core injectors doesn't work from here... you must do something down there! Quickly!..."

SCADA platform introduction

Nobody wanna be in such condition isn't it?

In the last decade SCADA (*Supervisory Control and Data Acquisition*) systems have moved from proprietary, closed, networks to open source solutions and TCP/IP enabled networks. Their original "security through obscurity" approach, in terms of protection against unauthorized access, has fallen, together with their interconnection limits.

This has made them open to communicate with the rest of the world, but vulnerable, as our traditional computer networks.

As a result, some highly publicised successful intrusions has been told by the press, but many other attacks against energy, transportation and other industrial fields have gone unnoticed or untold.

One thing to keep in mind is that SCADA systems manage many critical infrastructures of our life, from power grids to railways, from aqueducts to airports and vulnerabilities discovered on such systems could have a deep impact on the overall security of the country.

Rest to be noted that, despite security testing has included corporate networks, systems, and software, since the advent of ICT Security, SCADA systems have been relatively new as a target for Vulnerability Assessment and Penetration Tests due to the above-mentioned historic reasons.

Testing SCADA systems is not a usual task, in terms of complexity and strategy.

In fact, every SCADA system has specific architectures and protocols and, despite the introduction of TCP/IP, other aspects are completely different from a platform to another.

Therefore, test requires different skill and different planning to be carried out properly.

In my experience, the main difference is due to the communication architecture of the TOE (Target of Evaluation) and its access model.

If the TCP/IP is widely adopted on the SCADA infrastructure and the Input System is based on a Windows or UNIX platform, then the testing strategy can be moulded closely to a traditional Pen Test.

If the TCP/IP is limited to small fraction of the environment and the Input System is a proprietary platform, then the test should be designed around different factors, such as the knowledge of the proprietary platform and the adoption of known custom scripting for attacking the environment.

This seriously affects the choice of the Team in order to fulfil the task quickly and smoothly.

In some cases, the knowledge of a very old SCADA environment is limited to few operators and some musty papers long forgotten by the original SCADA retailer.

Often the customer thinks that security through obscurity ensure a sufficient level of protection... is up to us to demonstrate that recovering those papers and studying the manuals allows an attacker to bypass the few procedures enforced on the platform... but this requires patience and competence.

In addition, despite it is not always applicable, the approach based on information gathering, scanning and exploiting continues to give satisfactory results, even on SCADA Testing.

However, do not forget our motto: "think outside-the-box" it is a foundation on SCADA testing too.

Testing the Box

Several testing techniques are available, today, in the SCADA field.

Problems arise for testers when facing custom proprietary platforms. Another important aspect is related to the testing radius.

If networking elements and platforms are included as Targets of Evaluation (TOEs) then the complexity and temporal extent of the analysis increases significantly.

In my experience, as SCADA/ATM Banking tester, I have met very complex networking infrastructures where the SCADA systems are just the part of the entire environment and testing them requires to properly planning the entire task identi-

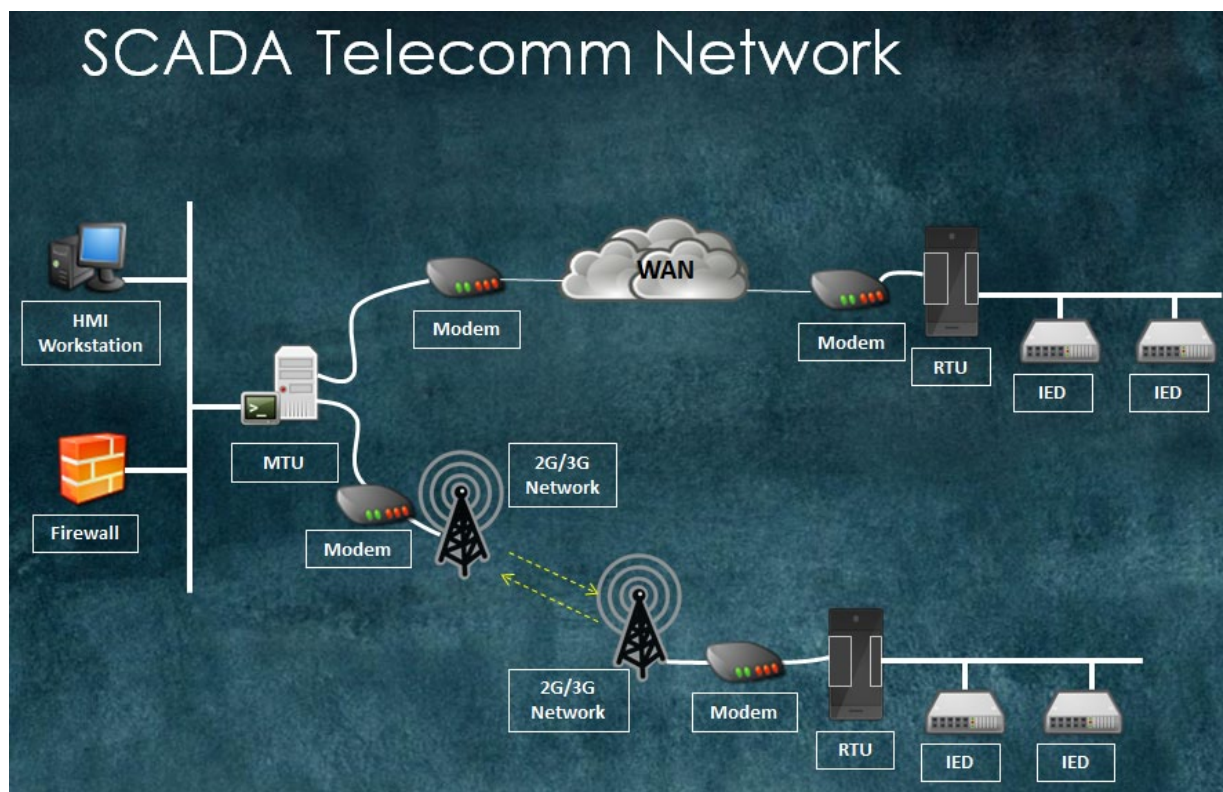


Figure 1. A typical networked SCADA Environment

fying specific skills needed to the team in order to fulfil the job.

This means that, unlike traditional pen testing, in this case the test should be organized around a very peculiar team made by properly skilled and experienced developers and Sysadmins, with specific platform knowledge.

In other words in a proprietary SCADA test you should prepare a fire-and-forget team, with at least one expert of the target platform.

During a funny, but important analysis made few years ago, on a public transportation platform, where the distributed control RTU was an old and “forgotten” SCADA proprietary platform, my team has been rounded up with an old retiree, the only person we have found with skill good enough to ensure a proper testing of the environment.

The retiree has been a key person in the test, identifying several critical vulnerabilities. The fun was the discovery of a vulnerability affecting toilet service on the system... worst, with specific commands, once the platform was under attacker’s control, the automatic toilet flush could be reversed (with a result that anyone can imagine...)

However, environment complexity does not necessarily mean testing complexity.

Some SCADA platforms are just custom Windows Operating Systems, mainly Windows CE, 2000 or XP, with tons of common vulnerabilities. They are usually not patched by the vendor because patching could affect operation availability of the platform, or because updating them means a very long job or because it has not been included in the maintenance contract.

In these cases, the SCADA platform is composed of a distributed system with a central “knowledge” that manages and monitors endpoint operations. The SCADA platform is over the OS layer, as an application running on core devices with a limited part of it running on endpoints (Figure 1).

Testing strategy heavily depends on the characteristics of the platform and its ecosystem.

In case of Windows boxes a traditional approach could be applied, at least in specific areas, otherwise a specific attack strategy must be developed for the task. In particular it is very important to understand the communication mechanism and the networking protocol involved, especially if they rely on proprietary protocols and interfaces.

Often, the goal of system exploit could be reached through very simple and effective strategies by adopting “out-of-the-box” attacking scheme.

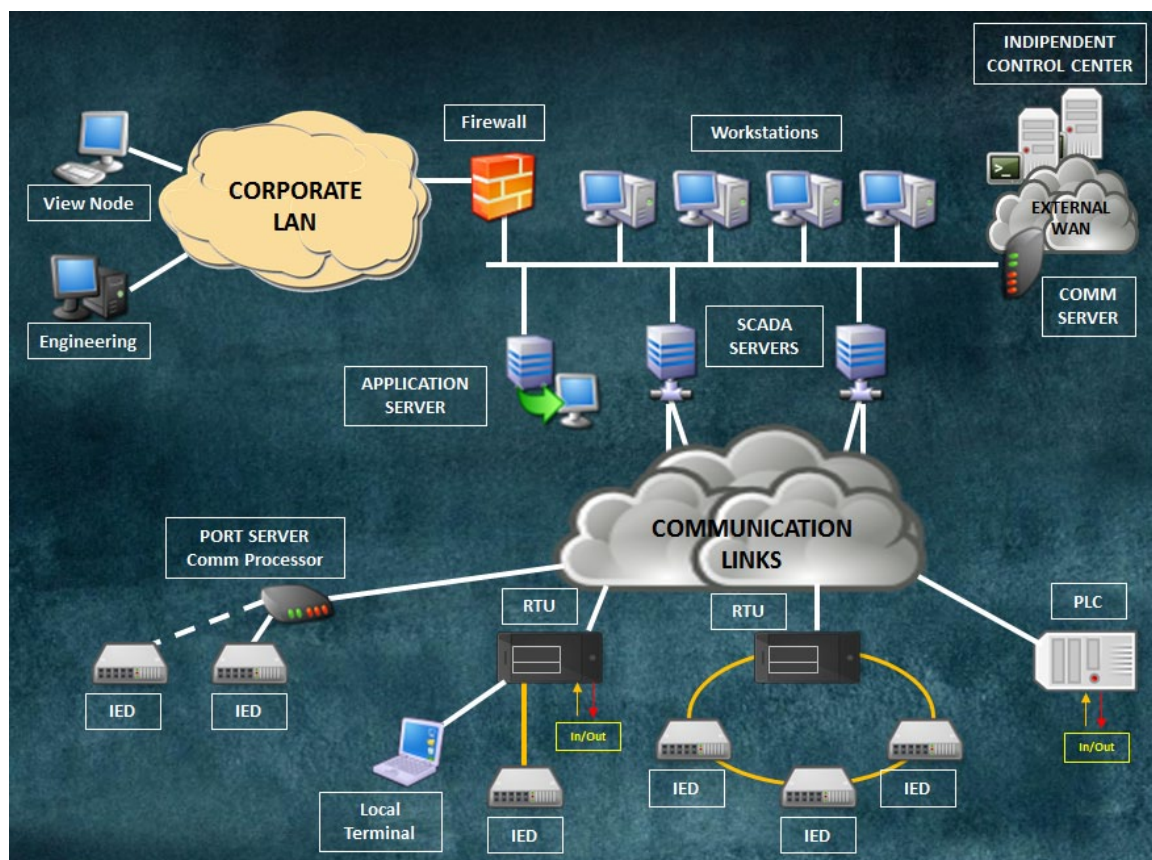


Figure 2. A complex SCADA environment

In other cases, for example during some SCADA banking tests, the resort of “physical” electronics devices could be the best way to achieve the objective. Nevertheless, all this means to study and customize the testing job accordingly and avoid relying on commercial or open source scanners. Use your brain instead.

Obviously, the scanner is a valuable tool, but the tester must know how to use it accordingly to the analysis goal.

In fact, the result taken from a scanner, if not properly verified, could lead to false positive or false negative evidences, thus lowering the cogency of the report.

This is particularly true in SCADA testing.

As a general recommendation a SCADA Security assessments should be bounded by a detailed assessment plan that specifies a schedule and budget, targets and goals, expected deliverables, hardware and resource requirements, rules of engagement, and a recovery procedure.

It is of capital importance that the team assigned to perform the assessment should be involved in the development of the assessment plan (Figure 2).

Exploiting the box

As stated previously, attacking a SCADA platform is an action full of consequences, in particular on production systems based on proprietary software and protocols.

One of the most concerning aspect is related to the possible interruption of service.

To avoid the risk, experience and competence are essential factors.

An experienced operator can predict the platform behaviour, a competent tester can, then, adapt the attacking pattern in order to avoid predictable malfunctions without a too conservative approach that could thwart the testing results.

Only experience and competence can help the team to identify a correct attack sequence with a correct exploit selection and this is of capital importance when the analysis goes deep and imposes to pwn the platform.

Often the platform complexity, in terms of number of elements, hides the simplicity of the code and its easy exploitability. But sometimes the lack of information about the proprietary software, or about custom specific customization, leads the entire team into the sea of doubts, where a move in a wrong direction could be devastating.

In one of my first experience in this field our team, during a test for a network replay attack against a Siemens System, wrongly define the number of replay packets sent against the TOE creating a devastating Denial of Service for the System's CPU forced to replay the same action for eleven times in a row.

In another test, during an attempt to force authentication on a MTU unit the tester, ignoring the presence of a limit on the attempt per seconds, has triggered a system reboot for overflow condition. Unfortunately, lately we have discovered that the password was very easy to guess...

In another task we have successfully intercepted authentication by a MitM, but we have ignored that the system does not support double authentication with same credential thus leading to the isolation of the MTU from the rest of the environment when our team have logged to verify the intercepted credentials.

This is where experience and competence are the sole chances to fulfil the task.

As you can imagine there are many ways a system can be penetrated.

Some rely on the same principle adopted in a traditional testing, for example MitM for password stealing or Drive-by attacks against system's users. For example, if we attack a laptop used to program the PLC.

Another potential way is to prepare an USB driver and give it to internal personnel working on SCADA system. This trick has been used by Stuxnet to attack Iranian WinCC systems in 2010.

Another interesting attack pattern relies on dial-up modems and wardialing.

In fact, many SCADA producers provide remote access to their platform so technical support staff can access the devices remotely. Remote access provides administrative level access to a system.

By using a war dialer, or programs that dial consecutive phone numbers looking for modems, and with password cracking software, it is possible to gain access to systems. Last but not least, passwords used for remote access are often common to all implementations of a particular vendor's systems and may have not been changed by the end user.

Other techniques depend upon platform-related vulnerabilities, for example web-related exploits.

This is a recent trend. Many SCADA producers have integrated Web Services inside their products in order to offer more flexible options to connect and manage their platform. Obviously a vast

majority of them has decided to adopt Apache as a webserver, thus paving the way to Apache-related attacks or other exploitation techniques based on traditional web attacks.

To define the best attacking strategy initial knowledge based on experience and information gathering are invaluable.

But let's plan a SCADA Test

First of all, SCADA test is not noob friendly and cannot be learned in Lab.

This means that to put your hands on a testing environment you should be an experienced pen tester.

Nobody wants to risk a production platform putting it at mercy of an inexperienced tester, isn't it?

Usually behind SCADA rely an industrial production line or worst a public service such as aqueducts, railways or nuclear power plants... The team must be confident and very experienced on pen testing.

Normally SCADA testing cannot be practically made as black box testing, too much risks are at stake.

Therefore, it should be done as grey box or white box test.

In my experience, going black box could be done only if potential compromise of the platform does not risk to block a critical infrastructure, but the opportunity is very remote.

However, the first step should aim to characterize the platform in terms of software, firmware and architecture. To do this, in black box, extreme caution must be enforced on all the operative tasks.

Normally it is good to collect information from Internet through search engines and social engineering.

Looking to company information should suffice.

In case of difficulties in finding reliable information, a social engineering test on company operators could be a valid next step.

Many SCADA operators are field technicians and engineers without security experience.

In a task on a water extraction SCADA platform, by talking with a pipeline designer has been sufficient to identify all component of the platform in terms of hardware type, firmware version and problems recorded in the past. The engineer was eager

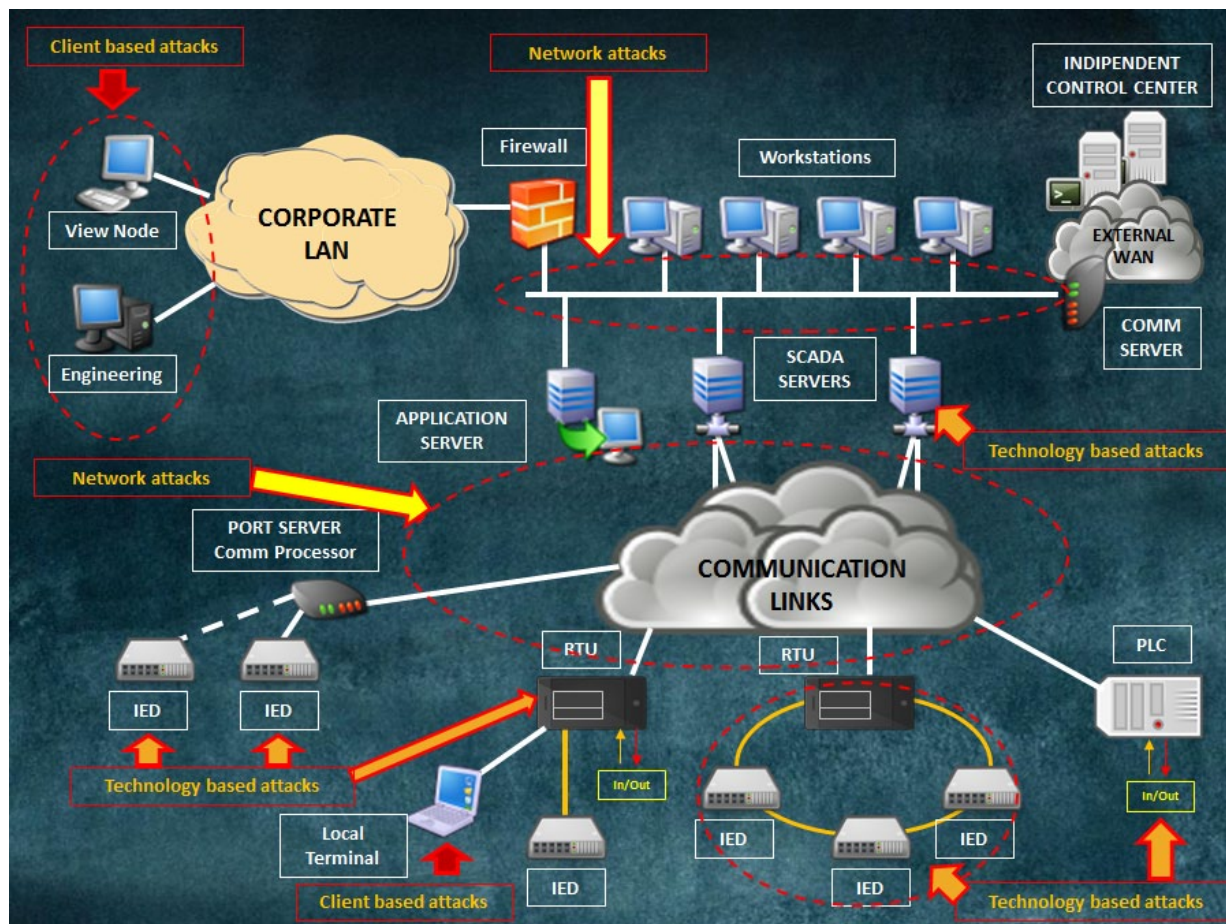


Figure 3. Different attack types and targets

to share a technical talk with an outsider showing all his ability in overcome problems.

In white box testing all that information should be collected before the definition of the test.

Once the team has the platform data it is good to proceed to the following steps:

- Reconnaissance
- Scanning
- Protocol dissection
- Exploit

The final step (Exploit) identifies the direct or indirect approach to the Target Systems.

Usual attack pattern could be Client based, Network based or Platform related.

Client based attacks could be performed against traditional Client or Server Systems with SCADA application running in them. The attack strategy, in this case, relies on Operating System or Application specific vulnerabilities and it is similar to traditional pen testing analysis.

Microsoft Windows is extremely popular as a Client OS so we will not cover this part, as it is very similar to usual testing techniques.

In SCADA Network, we can use several traditional tests such as MitM, but we have the chance to identify Maintenance Port or to use Spoofing, an uncommon technique nowadays.

Therefore, we can describe the attacks:

- Man-in-the-Middle (MITM)
 - To intercept, alter, and relay a communication message
- Maintenance port
 - To install a malicious program

- Spoofing
 - To masquerade as another in order to initiate an unauthorized action
- Replay
 - To record and retransmit valid data (manipulating time variable) to trigger unpredictable results

Clearly, it could be possible, for an attacker, to perform DoS also, but usually the tester only evaluates it as a possibility.

In my experience, only few customers ask you to go further by blocking a service. Rest assured that in some environments a DoS could be practical for a cybercriminal in order to delay or block the flow of information.

Attack patterns in this case are defined by

- physical destruction – but can be detected through fault-handling programs.
- Communication jamming – no effective countermeasures exist.

Platform related attacks are dependent from the technology in use and from the quantity of known vulnerabilities. Obviously not all the vulnerabilities disclosed are usable or reliable but a good scanner could give us some good hints. The rest is up to our Customer to let us try those vectors against his infrastructure.

The security community has identified lot of vulnerabilities. Nessus and other scanners have integrated scan modules for SCADA systems, but if you want to look to a good and reliable source, you can point your browser to: <http://scadahacker.com/vulndb/ics-vuln-ref-list.html>.

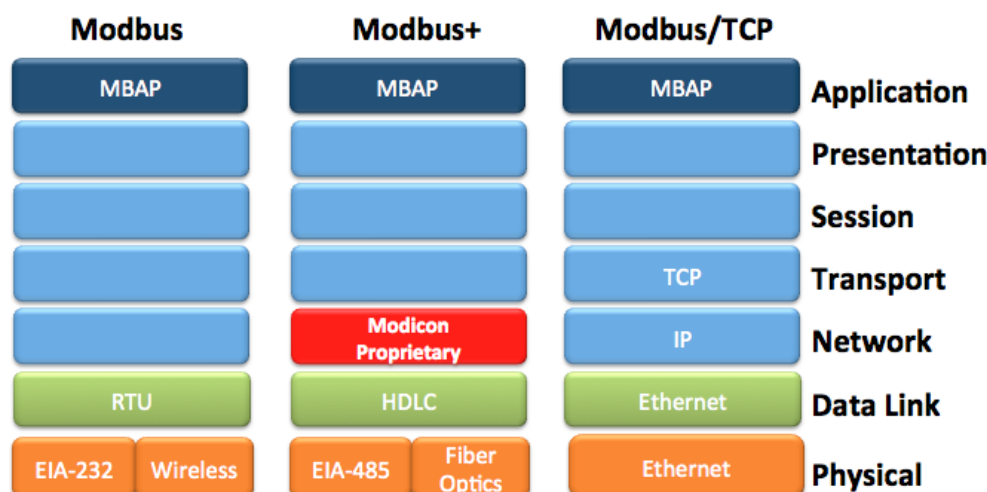


Figure 4. The MODBUS protocol family OSI stack representation

Payload and persistence

In case of plain exploitation of a system, we can conclude our task by adopting a custom payload.

This is where our fantasy could express itself.

Traditionally a payload is used to describe the action that will be performed once vulnerability has been exploited. Usual persistence options are:

- Backdoor. In Windows end points a reliable backdoor can be installed quickly. In my experience CyberGate RAT or DarkComet are the weapons of choice.
- Platform setting modifications. By activating a newest user profile with network access or by modifying configuration settings (some reverse engineering may be needed).
- Spoofing system operators. This attack pattern requires dumping platform user database and breaking cryptographic protections, which is a very time consuming, and challenging process.
- Changes to instructions and commands (requires a skilled operator in the team).

Protocol manipulation, vulnerability exploitation and the man-in-the-middle attacks are among the most popular ways to manipulate insecure protocols, such as those found in control systems.

However we must note that vulnerabilities and payloads, sometimes, are due to the burden of monitoring and keep update all system software on all of the devices in the network.

A real live one: Attacking ModBus communications

The MODBUS is a serial communications protocol created in the 1970's by the Modicon Corporation for use with its programmable logic controllers (PLCs).

The protocol's simplicity and efficiency, combined with the publishing of its specifications by Modicon caused it to become widely adopted throughout the industrial controls and SCADA world as a de-facto industrial standard.

The original MODBUS system was a simple two-layer communication stack running on top of a serial EIA-232 link.

As different physical layer options became available (see Figure 4), it was subsequently marketed as a number of different of network products, the best known of which are MODBUS, MODBUS+ and MODBUS/TCP.

The common element in all of these MODBUS networks is a client-server command structure commonly known as the MODBUS Application

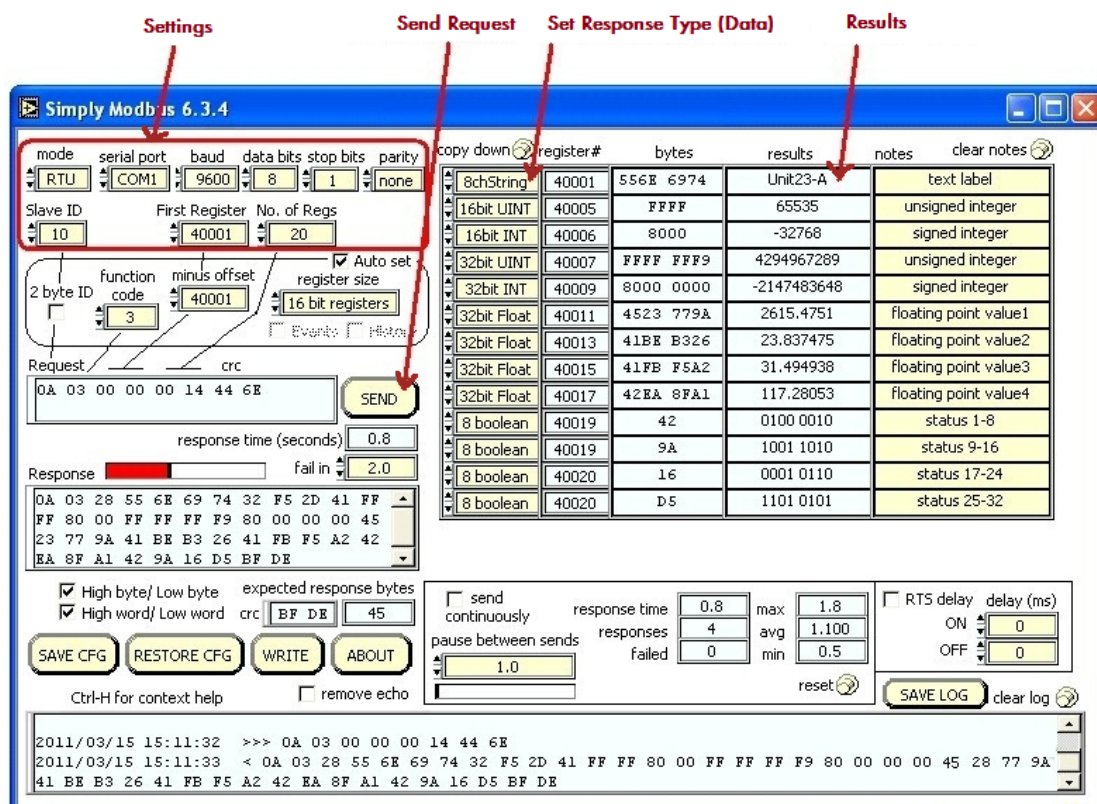


Figure 5. Simply ModBus

Protocol (MBAP), a layer-7 protocol in the Open Systems Interconnection Reference Model (OSI/RM).

In ModBus Architecture are defined two kinds of devices:

- *ModBus Master*: is the device requesting the information.
- *ModBus Slaves*: are the devices supplying information.

In a standard Modbus network, there is one Master and up to 247 Slaves, each with a unique Slave Address from 1 to 247. In addition the ModBus Master can also write information to the Slaves.

The official Modbus specification can be found at: www.modbus-ida.org.

A simple request-reply scheme is used for all transactions. The network communications follow this scheme:

- The ModBus Master device initiates a request and the slaves replies.
For example, when a Human Machine Interface (HMI) workstation requires a value from a PLC it sends a request message to start the data transfer process. In response the PLC then sends the requested information. In our case, the device running the HMI will act as the client/master and the PLC act as the server/slave.
- Each message contains a function code that is set by the client/master and indicates to the server/slave what kind of action to perform. Function codes are the same for requests and responses since the server simply reflects the function code back to the client.

There are 127 possible function codes that fall into three general categories:

- *Public* function codes.
- *User Defined* function codes.
- *Reserved* function codes.

In order to define multiple actions or to allow future enhancements, other *Sub-codes* are added to some function codes.

The MODBUS protocol was not initially designed with cybersecurity in mind; hence it lacks the mechanism to avoid the classical information security threats. The protocol does not include a way

of ciphering the traffic, check the integrity of messages, and authenticate client and server

On our scenario an attacker could send packets to the control network either from inside or outside and by doing this he could reset connection, send commands to the slaves (RTUs) or cheat masters (HMI) with fake data pretending to be the PLCs.

He could also sniff traffic and retrieve information about memory addresses or common operations performed on the system.

But how to do this?

The answer is by collecting a Modbus simulator:

- <http://www.modbustools.com/>
- <http://www.brothersoft.com/simply-modbus-117531.html>

and by interconnecting our PC with a serial interface.

The configuration of the messages is very easy, once we know what message or instruction to transmit.

The following pane shows Simply ModBus interface: Figure 5.

We can also try to intercept and replay ModBus streams in TCP/IP network, for this goal Cain&Abel, Wireshark or Ettercap are a good tool to start with.

Once we collect and replay the streams we will be able to exploit the communication thus completing the initial goal. Of course, by studying the request/response mechanism we can force the platform to perform our will.

Next time we will discuss more option on SCADA testing, but also some mitigation techniques.

UP THE IRONS!

STEFANO MACCAGLIA

Develop for the Next Big Platform!

Attend the Windows Phone Developer Conference and get the best developer training!



The Windows Phone Developer Conference

October 22-24, 2012

Hyatt Regency
Burlingame, CA

www.WPDevCon.net

Learn from the top experts at the Windows Phone Developer Conference, including 12 Microsoft MVPs!



Darrin Bishop



Michael Cummings



Nick Landry



Jose Luis Latorre



Chris Love



Colin Melia



Walt Ritscher



Lino Tadros



Kelly White



Shawn Wildermuth



Chris Williams



Chris Woodruff

50+ Classes and Workshops

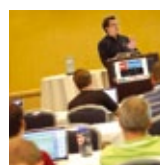
focus on a variety of important topics:

- Design implementation
- Location intelligence services
- Rich data visualization and implementation
- Cloud-based mobile solutions
- Development leveraging HTML5
- User experience
- Application design
- HTTP protocol
- Building reusable components
- Microsoft push notification service
- Creating custom animation
- and many more!

Visit WPDevCon.net for a full list of speakers, bios, classes, workshops, and special events!



Learn, network,
and seize the
opportunities
that
Windows Phone
represents.



Register Early
for the
biggest
discounts!
at
www.WPDevCon.net

WPDevCon™ is a trademark of BZ Media LLC. Windows® is a registered trademark of Microsoft.

Produced by **BZ Media** **SDTimes**

@WPDevCon

In the next issue of

PenTest

magazine

FREE

Malware

IS Risk Assessment
Measurement

DDoS Attacks

Metasploit Penetration
Testing

Available to download
on **August 20th**

If you would like to contact PenTest team, just send an email
to en@pentestmag.com. We will reply a.s.a.p.

PenTest Magazine has a rights to change the content of the next Magazine Edition.

MOBILE SECURITY

ONLINE SUMMIT

LIVE 11th JULY

Join this free summit to hear industry experts and experienced practitioners share how your business can profit from the mobile phenomenon without being exposed to threats such as data leakage, malware attacks and unauthorised data access.

FIND 8 thought leadership webinars

LEARN about the latest industry trends

SHARE the knowledge

To register for free and view the full lineup go to
<http://www.brighttalk.com/r/rmC>

BrightTALK™

PANNONE

CYBER CRIME LAWYERS

Pannone are one of the first UK firms to recognise the need for specialist cyber crime advice. We can both defend and prosecute matters on behalf of private individuals and corporate bodies.

We are able to examine material or secure evidence in-situ and will then represent your needs at every step of the way.

Our team has a wealth of experience in this growing area and are able to give discrete, specialist advice.

Please contact David Cook on

0161 909 3000

for a discussion in confidence or email

david.cook@pannone.co.uk

www.pannone.com

DIGITAL FORENSICS / MAGAZINE

Keep up to date on the latest developments in the
world of digital forensics

Read **Feature Articles** on:

- / Training and Certification
- / Management issues
- / Tools and Techniques
- / eDiscovery/eInvestigation
- / Incident Response/First Response
- / Hardware and Software
- / Network Forensics
- / Cyber Forensics
- / and much more...

Apple Autopsy:

- / A Digital Forensics look at all things Apple

From the **Lab:**

- / In depth technical articles on products and techniques

Legal Section:

- / In-depth articles on legal matters affecting Digital Forensics along with the latest legal news from around the world

VISIT DIGITALFORENSICSMAGAZINE.COM

for the latest news and views from the
digitalforensic community with special
articles for **registered users**.

***NEXT ISSUE OUT SOON
SUBSCRIBE NOW***

Prospective authors should contact editorial@digitalforensicsmagazine.com
for information on submissions.