Intrusion Detection on Campus Network, the Open source approach: Accra Technical University Case Study

Victor Gbedawo
ICT Department
Accra Technical University
Accra, Ghana

Komi Agbesi
Computer Science Department
Accra Technical University
Accra, Ghana

Theophilus Adukpo
I.S Department
MTN House, Plot OER
Accra, Ghana

ABSTRACT

The computer network security landscape in recent times has become a crucial area in computer networking for both network administrators and network users such that, a compromise of this network security makes the services it provides and more importantly the data it holds, highly susceptible to exploits by malicious people for different purposes and reasons. This is particularly so for campus networks in view of the fact that, they do not only provide services to promote academic work directly but in many ways are integrated into the administrative setup of the institutions they serve. This research therefore seeks to investigate the security threats and vulnerabilities of campus networks and systems to a great extent, so as to propose interventions to resolving these threats, vulnerabilities and exploits, so as to improve the security of these networks by conducting a penetration test that simulates Intrusion Detection employing free and open source software (FOSS) tools. The research adopted "Cloppert's kill chain" Approach to Penetration Testing. The elements of the simulation included the following FOSS tools VMware Fusion (Operating System simulator), Zentyal Server (unified network server), Snort (Intrusion Detection System), Suricata (Intrusion Prevention System), Nmap (Network scanning), OpenVAS (Vulnerability Assessment Software) and Metasploit Framework (Exploitation tool). Results of the simulation revealed injection flaws to be the prevalent security vulnerability that was exploited and hence, discussed to improve computer network and application security in a rather cost effective fashion.

General Terms

Free and Open Source Software (FOSS), Simulation Approach, Intrusion detection and Prevention System, Penetration test, Campus Network, Network Operation Center (NOC).

Keywords

OWASP top 10, 'Kill Chain approach', Zentyal server, IDS/IPS, OpenVAS, NVT feed, CVE, SQL injection, Denial-of-service attack, Overt and Covert attacks

1. INTRODUCTION

At a time when the world is fast becoming a "*globalized village*" with the developed world in one breadth, taking the lead whilst the developing world in the other breadth, struggling to catch up with current trends as far as the application of Information and Communication Technologies (ICT) are concerned. The success of the highly industrialized nations like the United States of America, the United Kingdom, China and Japan to name but a few, has been possible through the computerization of both simple and complex everyday tasks which cut across different fields of engagements. The result is a quicker, more efficient and reliable way of doing things and achieving results in a world where much is demanded from very little and within very short periods of time. The face of the Ghanaian economy has improved considerably in the last few years through the use of Information Technology particularly in the banking and health sectors among others.

With critical observation and analysis, it is clear that most aspects of management can be modelled and designed into Computerized Information Management Systems (CIMS). The effectiveness of ICT as a tool for development and industrialization requires the development and effective implementation of equally highly efficient components such as databases and Database Management Systems (DBMS), servers of different kinds for a variety of purposes and computer networks of different types and sizes. The important role of these components and the current developments in the use of ICT as an indispensable tool for economic empowerment in the global market place, through its gradual integration in our daily activities coupled with the numerous existing and new vulnerabilities and security threats associated with them. Computer networks and computer networking in general, being a component of ICT provides many advantages, which rather unfortunately are closely tied with new and more sophisticated security threats and Exploits every passing day. This changes the entire security landscape of an organization. Although networking alters the risk profile of an organization, in few of the risks associated with security of computing, the general security concept remains the same for standalone computers. That is, preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.

This Research seeks to investigate the security vulnerabilities on campus networks using free and open source software with effective ways of detecting them. Thus, the research is meant to develop effective and efficient protection techniques and mechanisms for campus networks in a way that can easily be modified and ported to other networks. These techniques and mechanisms comprise a balanced combination of software and hardware solutions.

2. LITERATURE REVIEW

2.1 Attacks or Misuse

Attacks can also be referred to as unintended consequences, such as when a hapless new user overwrites a critical document with a blank page. Another misuse event could be a user mapping a drive to a file server share not intended by the network administrator. Most Intrusion Detection Systems

(IDS) are deployed to detect intentionally malicious attacks coming from external locations, but they are also proving of value within the corporate world for monitoring internal users. Security surveys often reveal internal misuse events as a leading cause of corporate data loss and an IDS tool can track internal maliciousness almost as well as external attacks. In one case, a sharp security officer working in an IT department used an IDS to catch a fellow employee cracking passwords and reading confidential e-mail [1].

2.2 Application Attacks

While network protocol attacks abound, most security threats exploit the application layer of the host. In these cases, the TCP/IP packets are constructed legitimately, but their data payload contains malicious content. Application attacks can be text commands used to exploit operating system or application holes, or they can contain malicious content such as a buffer overflow exploit, a maliciously crafted command, or a computer virus. Application attacks include misappropriated passwords, password-cracking attempts, rootkit software, illegal data manipulation, unauthorized file access, and every other attack that doesn't rely on malformed network packets to work.

2.3 Suricata as IDS

The US Department of Homeland Security in 2009, together with a group of other civilian entities, gave funding to a newly created company, the Open Information Security Foundation (OISF). The grant was to build an alternative to Snort an open source Intrusion detection system, called Suricata. Suricata was first released in 2010 as an open source software [2].

In figure 1, each segment of the connected network, holds a network-based intrusion detection system (NIDS) monitoring the corresponding network segment. Finally, there is a management tool of IDS at LAN used to collect and organize the information received from various connected modules [3].

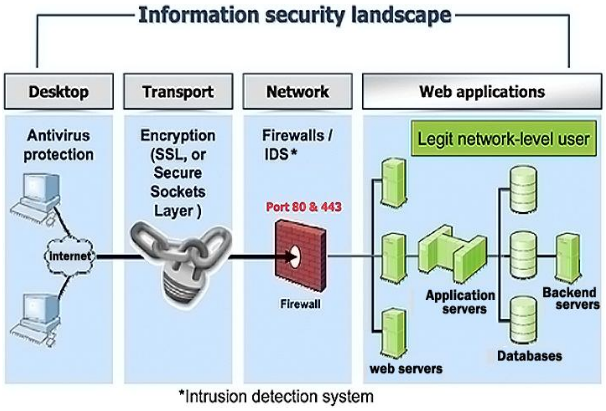


Fig 1: Example of a classic intrusion detection solution.

2.4 Zentyal as Gateway

Zentyal (formerly eBox Platform) is a program for a Linux server for small and medium enterprises (SMBs), regarded as a substitute to Windows Server and other Microsoft infrastructure products for Small and Medium Businesses. Zentyal has the ability to act as a gateway, Network Infrastructure Manager, Unified Threat Manager, office server, Unified communications server or a combination of them. Zentyal is based on Ubuntu and it can be installed either from Ubuntu repositories or from Zentyal's own installer [4].

2.5 VMware Virtualization

VMware Fusion is a hypervisor that runs on Mac OS; it enables users to set up one or more virtual machines (VMs) on a single physical machine, and use them simultaneously along with the actual machine. Each virtual machine can execute its own operating system, including versions of Microsoft Windows, Linux and MS-DOS. VMware Fusion is developed and sold by VMware, Inc., a division of EMC Corporation. The minimum hardware requirements for such a modest network simulation limited to Accra Polytechnic’s NOC should have at least, the following requirements according to table 1 [5] :

Table 1: Standard Hardware Requirements

Hardware	Minimum	Used to Build the Lab
CPU	Dual core, 6- bit	Core2 Duo
RAM	8 GB	8 GB
Hard disk	60 GB free space	Additional hard disk
Operating system	64-bit	Windows 7 64-bit
Virtualization software	VMware Player	VMware Workstation

2.6 Types of Penetration Tests

Basically, there are two main types of penetration tests: overt and covert. An overt pen test, or “white box” test, occurs with the organization’s full knowledge; covert tests or “black box” tests are designed to simulate the actions of an unknown and unannounced attacker. Both tests present advantages and disadvantages [6]. Using overt penetration testing, one works with the organization to identify potential security threats, and the organization’s IT or security team shows one the organization’s systems. The one main benefit of an overt test is that one has access to insider knowledge and can launch attacks without fear of being blocked. When time is limited and certain PTES steps such as intelligence gathering are out of scope, an overt test may be the best option.

2.7 Kali Linux for Penetration Testing

Kali Linux (Kali) is the successor to the Backtrack penetration testing platform which is generally regarded as the de facto standard package of tools used to facilitate penetration testing to secure data and voice networks. Backtrack (BT), (www.offensive-security.com) was released to provide an extensive variety of penetration testing and defensive tools that were perfect for auditors and network administrators interested in assessing and securing their networks. The same tools have been used by both authorized and unauthorized (hackers) penetration testers.

2.8 Vulnerability scanning

Vulnerability scanning employs automated processes and applications to identify vulnerabilities in a network, system, operating system, or application that may be exploitable. When performed correctly, a vulnerability scan delivers an inventory of devices (both authorized and rogue devices), known vulnerabilities that have been actively scanned for, and usually a confirmation of how compliant the devices are with various policies and regulations. Unfortunately, vulnerability scans are loud and they deliver multiple packets that are easily detected by most network controls and make stealth almost impossible to achieve.

2.9 The "Kill chain" Approach to Penetration Testing

In 2009, Mike Cloppert of Lockheed Martin CERT introduced the concept that is now known as the "attacker kill chain". These steps were taken by an adversary when they conducted an attack on a network. According to this concept, it does not always proceed in a linear flow as some steps may occur in parallel. However, multiple attacks may be launched over time at the same target, and overlapping stages may occur at the same time [7].

A typical kill chain of an attacker can be described as follows:

• Reconnaissance phase – The adage, "reconnaissance time is never wasted time", adopted by most military organizations acknowledges that it is better to learn as much as possible about an enemy before engaging them. For the same reason, attackers will conduct extensive reconnaissance of a target before attacking. In fact, it is estimated that at least 70 percent of the "work effort" of a penetration test or an attack is spent conducting reconnaissance. Generally, they will employ two types of reconnaissance:

° Passive reconnaissance – This does not directly interact with the target in a hostile manner. For example, the attacker will review the publicly available website(s), assess online media (especially social media sites), and attempt to determine the "attack surface" of the target. One particular task will be to generate a list of past and current employee names. These names will form the basis of attempts to brute force, or guessing passwords. They will also be used in social engineering attacks. This type of reconnaissance is difficult, if not impossible, to distinguish from the behaviour of regular users.

° Active reconnaissance – This can be detected by the target but, it can be difficult to distinguish most online organizations' faces from the regular backgrounds. Activities occurring during active reconnaissance include physical visits to target premises, port scanning, and remote vulnerability scanning.

• The delivery phase – Delivery is the selection and development of the weapon that will be used to complete the exploit during the attack. The exact weapon chosen will depend on the attacker's intent as well as the route of delivery (for example, across the network, via wireless, or through a web-based service).

• The exploit or compromise phase – This is the point when a particular exploit is successfully applied, allowing attackers to reach their objective. The compromise may have occurred in a single phase (for example, a known operating system vulnerability was exploited using a buffer overflow), or it may have been a multiphase compromise (for example, an attacker physically accessed premises to steal a corporate phone book. The names were used to create lists for brute force attacks against a portal logon. In addition, e-mails were sent to all employees to click on an embedded link to download a crafted PDF file that compromised their computers.). Multiphase attacks are the norm when a malicious attacker targets a specific enterprise.

• Post exploit: action on the objective – This is frequently, and incorrectly, referred to as the "exfiltration phase" because there is a focus on perceiving attacks solely as a route to steal sensitive data (such as login information, personal information, and financial information); it is common for an attacker to have a different objective. For example, a business may wish to cause a denial of service in their competitor's network to drive customers to their own website. Therefore, this phase must focus on the many possible actions of an attacker. One of the most common exploit activity occurs when, the attackers attempt to improve their access privileges to the highest possible level (vertical escalation), and to compromise as many accounts as possible (horizontal escalation).

• Post exploit: persistence – If there is value in compromising a network or system, then that value can likely be increased if there is persistent access. This allows attackers to maintain communications with a compromised system. From a defender's point of view, this is the part of the kill chain that is usually the easiest to detect.

Kill chains are metamodels of an attacker's behaviour when they attempt to compromise a network or a particular data system. As a metamodel, it can incorporate any proprietary or commercial penetration testing methodology. Unlike other methodologies, however, it ensures a strategic-level focus on how an attacker approaches the network [7]. This focus on the attacker's activities serves as a guide to the layout and content of this study.

In figure 2, a modified; Cloppert's kill chain has been displayed to accurately reflect on how attackers apply these steps when exploiting networks and data services.

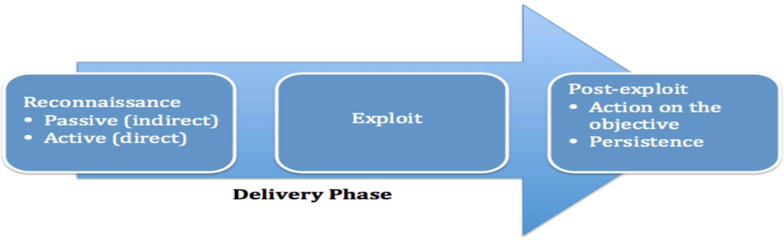


Fig 2: Cloppert's kill Chain Approach

2.10 Vulnerability Benchmark: Open Web Application Security Project (OWASP)

The Open Web Application Security Project is an open source community formed in 2001 that freely produces guidance on application security risks. OWASP maintains the OWASP Top 10 web portal, a list that identifies the most critical application security risks. Since 2004 a new list has been released every 3 years [8]:

3. METHODOLOGY

To begin with, the methodology of this study went a long way to producing consistent and reproducible results, which even had consequential benefits in the investigation of vulnerabilities in a simulated campus network. The study employed Cloppert's "kill Chain" Approach as the methodology in Penetration testing with respect to simulating the Intrusion detection and Intrusion prevention using free and open source software in a controlled environment. It was against the background of limited resources to perform this research that the overt mode of penetration was engaged. To begin with, a virtual Laboratory was built using VMware Fusion on a MacBook Pro running Mac OS X version 10.7.4 with Processor 2.26 GHz Intel Core 2 Duo.

In table 2, the available memory resource requirement used in building the penetration test was short of 4 GB. Although by inference, this limits the performance of the simulation in terms of computer resources, just about a few nodes were created, which provided a fair representation of how a larger system would have performed for which FOSS tools were used to simulate intrusion detection and prevention on campus networks.

Table 2 :Description of computer resource for Lab

Hardware	Resource Used to Build the simulation
CPU	Intel core 2 Duo
RAM	4 GB
Hard disk	50 GB free space
Operating system	64-bit
Virtualization software	VMware Fusion

3.1 Building the Simulation Laboratory with VMware Fusion on Mac OS X

The VMware Fusion installation was started by double-clicking on its executable file (which contained a 64-bit architecture). In parallel, the virtual laboratory was fully constituted with the aid of some other free open source software called Kali Linux formerly known as BackTrack, which served as the attacking agent, Metasploit Framework as the main exploitation tool, OpenVAS as the Vulnerability assessment software and above all, Zentyal server 4.2 as the unified network server. The VMware Fusion virtual machine was run on a Mac OS X host operating system. Having installed VMware Fusion, new Guest Operating systems were created and specified the ISO files of the windows 7, Kali Linux and Zentyal servers respectively as shown in figure 3.

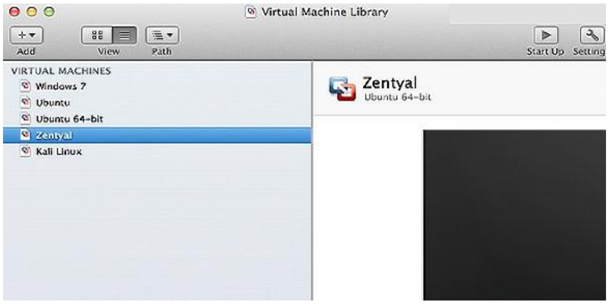
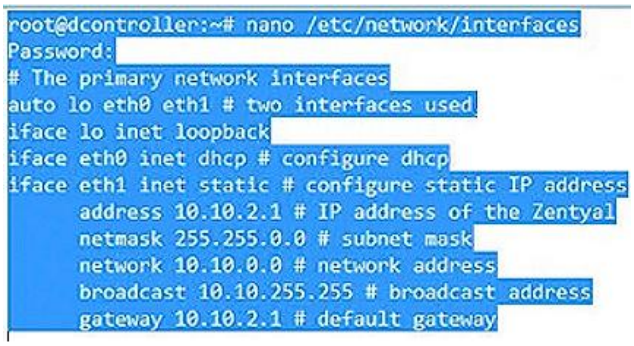


Fig 3: **VMachine showing the various guest OS**

Booting up the Virtual Machines after powering on Zentyal guest operating system and logging in using the credentials created at its installations, the Zentyal server was configured with two network interfaces. Figure 4 shows the command line processes for the network configuration in Linux. Where the IP address was set to 10.10.2.1 with the subnet mask being 255.255.0.0 on a 10.10.0.0 network.



```
root@dcontroller:~# nano /etc/network/interfaces
Password:
# The primary network interfaces
auto lo eth0 eth1 # two interfaces used
iface lo inet loopback
iface eth0 inet dhcp # configure dhcp
iface eth1 inet static # configure static IP address
        address 10.10.2.1 # IP address of the Zentyal
        netmask 255.255.0.0 # subnet mask
        network 10.10.0.0 # network address
        broadcast 10.10.255.255 # broadcast address
        gateway 10.10.2.1 # default gateway
```

Fig 4: Zentyal server network configuration

3.2 Network Configuration Service

Zentyal used ISC DHCP (Dynamic Host Configuration Protocol) Software to configure the DHCP service, which is the de facto standard on Linux systems. This service used the UDP transport protocol, port 68 on the client and port 67 on the server.

3.3 DHCP (Dynamic Host Configuration Protocol) server configuration with Zentyal

The DHCP service needed to be deployed on the interface configured with static IP address. The node with two Network Interface Cards, running the Zentyal Operating System served as the gateway machine, the DHCP (Dynamic Host Configuration Protocol) server, the webserver, the mail server, Domain controller and also the host for the Network IDS/IPS.

Each machine is assigned an IP address in the ranges of 10.10.0.1 – 10.10.2.80 as defined by the scope of the DHCP server. IPs in the 10.10… range are reserved for use on private internal networks.

3.4 Configuring Zentyal as a Standalone Domain server

Zentyal integrates Samba4 as a Directory service, implementing windows domain controller functionality and print/file sharing. A Domain, in this context, consists of several distributed services along all controllers, where LDAP directory, DNS (Domain Name System) server and distributed authentication through Kerberos are the most important. The Domain concept in Zentyal is strongly related to the Microsoft Active Directory implementation as shown in figure 5 where Accra Polytechnic's domain tree structure is clearly displayed with its corresponding user connections.

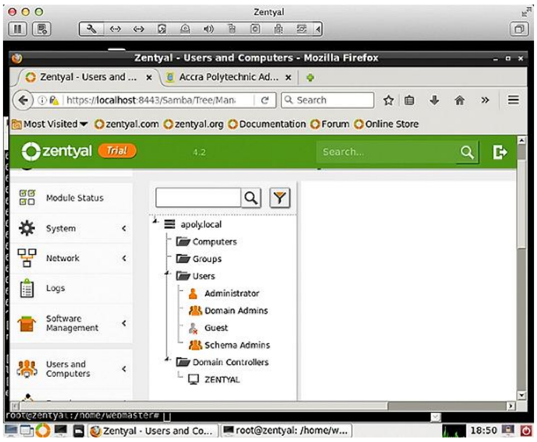
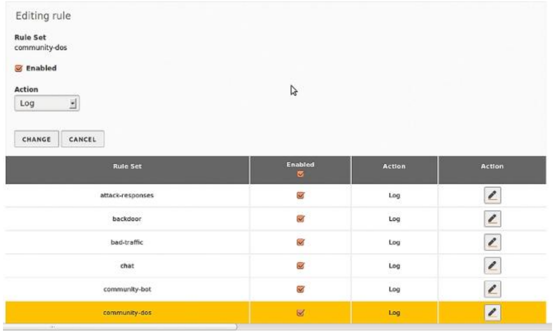


Fig 5: Zentyal related to the Microsoft Active Directory

3.5 Configuring IDS with Zentyal

The IDS/IPS module was integrated with the Zentyal logs module thus, making it possible for the different alerts to be queried. Similarly, events were configured for any of the alerts to flag notifications to the systems administrator as shown in figure 6 where the rule set for the IDS was configured to capture events like backdoor attacks, bad-traffic, Denial-of-service attack, ssh login attempts and other related events.



Editing rule

Rule Set
community-dos

☑ **Enabled**

Action
Log

Rule Set	Enabled ☑	Action	Action
attack-responses	☑	Log	✎
backdoor	☑	Log	✎
bad-traffic	☑	Log	✎
chat	☑	Log	✎
community-bot	☑	Log	✎
community-dos	☑	Log	✎

Fig 6: Configured Rule set for IDS

3.6 Demonstration of the simulation involving Kali Linux and Zentyal server

Configuration of the campus network under consideration consisted of two interfaces, one Public and the other Private. It was with the Public IP address that clients within the Private network are able to have communication with other external networks. That notwithstanding, for the purpose of this simulation, two nodes n0 to n1 as shown in figure 7 was designed. In this scenario, node n0 being the attacking agent sent a broadcast message during the Fping test and Nmap sessions to node n1 being the target machine (Zentyal server). In general, all nodes connected to node n1 in turn responded to the broadcast message using simple network management protocol (SNMP) to give out sensitive information. The traffic sources were then carried by the transport layer protocols User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), respectively back to the attacking agent.

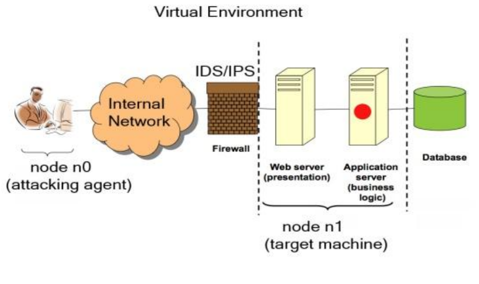

Virtual Environment
IDS/IPS
Internal Network
Firewall
Web server (presentation)
Application server (business logic)
Database
node n0 (attacking agent)
node n1 (target machine)

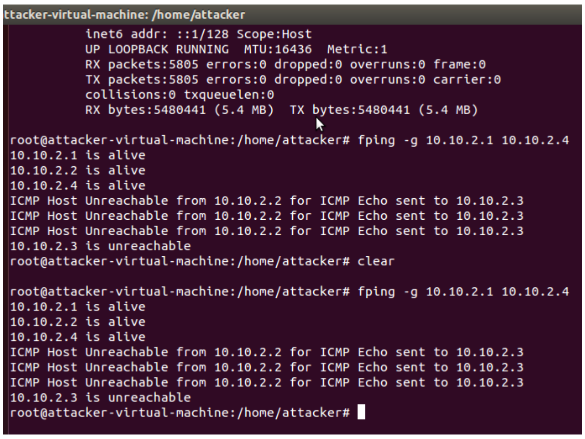
Fig 7: Proposed Network simulation attack with Distributed Intrusion Detection

3.7 Reconnaissance phase

This next step bothered on intelligence gathering and was one of the most important phases in the process, because if one missed something here, then the entire process could be compromised. The goal at this point was to understand the attacking surface and determine how to gain access to the system. To begin with, basic fping and nmap scan were performed against the targets in the virtual machine, and as a result, it was found that, port 80 was opened on the Zentyal node. Nmap's stealth TCP scan, which is typically effective in detecting ports without triggering defences was deployed. Most Intrusion Prevention Systems can detect port scans, but because port scans are so common, they are generally considered regular noise and are ignored as long as they are not very aggressive. The command in below:

root@kali:/# fping -g 10.10.2.1 10.10.2.4

was executed and the result in figure 8 revealed that three nodes were up and running.



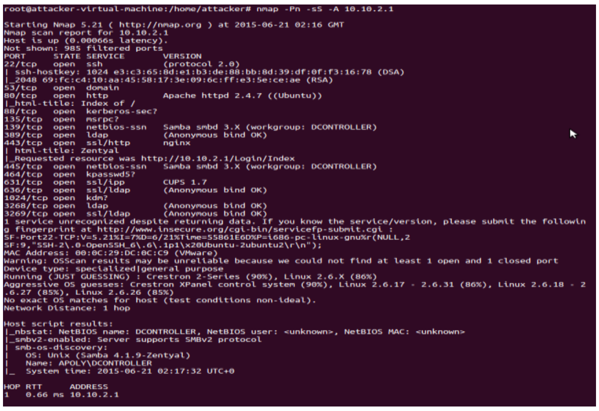
ttacker-virtual-machine: /home/attacker

```
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5805 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5805 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5480441 (5.4 MB)  TX bytes:5480441 (5.4 MB)

root@attacker-virtual-machine:/home/attacker# fping -g 10.10.2.1 10.10.2.4
10.10.2.1 is alive
10.10.2.2 is alive
10.10.2.4 is alive
ICMP Host Unreachable from 10.10.2.2 for ICMP Echo sent to 10.10.2.3
ICMP Host Unreachable from 10.10.2.2 for ICMP Echo sent to 10.10.2.3
ICMP Host Unreachable from 10.10.2.2 for ICMP Echo sent to 10.10.2.3
10.10.2.3 is unreachable
root@attacker-virtual-machine:/home/attacker# clear

root@attacker-virtual-machine:/home/attacker# fping -g 10.10.2.1 10.10.2.4
10.10.2.1 is alive
10.10.2.2 is alive
10.10.2.4 is alive
ICMP Host Unreachable from 10.10.2.2 for ICMP Echo sent to 10.10.2.3
ICMP Host Unreachable from 10.10.2.2 for ICMP Echo sent to 10.10.2.3
ICMP Host Unreachable from 10.10.2.2 for ICMP Echo sent to 10.10.2.3
10.10.2.3 is unreachable
root@attacker-virtual-machine:/home/attacker# 
```

Fig 8: Captured Fping results about machines that are alive on the network.

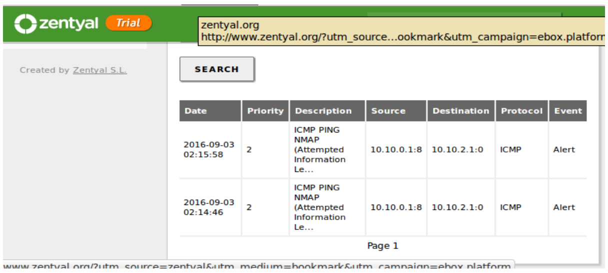
Continuing with the intelligence gathering phase, in figure 9, the nmap command: *root@kali:/# nmap -Pn -sS -A 10.10.2.1*

was executed and the resulting output displayed in figure 16 further revealed 15 opened ports and that what appeared to be running on the zentyal server was a web server. This was typical when attacking Internet-facing systems, most of which limited the ports accessible by Internet users. Port 80, the standard HTTP port was found opened and listening, Port 22, the standard ssh port was also found opened and listening. Upon further investigation, A web application in figure 11 displayed Accra Technical's Admissions online management system on browsing the IP address 10.10.2.1:80. Figure 10 shows the corresponding intrusion detection alert captured by the Distributed Intrusion Detection facility installed and configured on the Zentyal server.



```
root@attacker-virtual-machine:/home/attacker# nmap -Pn -sS -A 10.10.2.1

Starting Nmap 5.21 ( http://nmap.org ) at 2015-06-21 02:16 GMT
Nmap scan report for 10.10.2.1
Host is up (0.00066s latency).
Not shown: 985 filtered ports
PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           (protocol 2.0)
| ssh-hostkey: 1024 e3:c3:65:8d:e1:b3:de:88:bb:8d:39:df:0f:f3:16:78 (DSA)
|_2048 69:fc:c4:10:aa:45:58:17:3e:09:6c:ff:e3:5e:ce:ae (RSA)
53/tcp    open  domain
80/tcp    open  http          Apache httpd 2.4.7 ((Ubuntu))
|_html-title: Index of /
88/tcp    open  kerberos-sec?
135/tcp   open  msrpc?
139/tcp   open  netbios-ssn   Samba smbd 3.X (workgroup: DCONTROLLER)
389/tcp   open  ldap          (Anonymous bind OK)
443/tcp   open  ssl/http      nginx
| html-title: Zentyal
|_Requested resource was http://10.10.2.1/Login/Index
445/tcp   open  netbios-ssn   Samba smbd 3.X (workgroup: DCONTROLLER)
464/tcp   open  kpasswd5?
631/tcp   open  ssl/ipp       CUPS 1.7
636/tcp   open  ssl/ldap      (Anonymous bind OK)
1024/tcp open  kdm?
3268/tcp open  ldap          (Anonymous bind OK)
3269/tcp open  ssl/ldap      (Anonymous bind OK)
1 service unrecognized despite returning data. If you know the service/version, please submit the followin
g fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=5.21%I=7%D=6/21%Time=55861E6D%P=i686-pc-linux-gnu%r(NULL,2
SF:9,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\r\n");
MAC Address: 00:0C:29:DC:0C:C9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING) : Crestron 2-Series (90%), Linux 2.6.X (86%)
Aggressive OS guesses: Crestron XPanel control system (90%), Linux 2.6.17 - 2.6.31 (86%), Linux 2.6.18 - 2
.6.27 (85%), Linux 2.6.26 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: DCONTROLLER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
|_smbv2-enabled: Server supports SMBv2 protocol
| smb-os-discovery:
|   OS: Unix (Samba 4.1.9-Zentyal)
|   Name: APOLY\DCONTROLLER
|_  System time: 2015-06-21 02:17:32 UTC+0

HOP RTT      ADDRESS
1   0.66 ms 10.10.2.1
```

Fig 9: Port scan results from Nmap

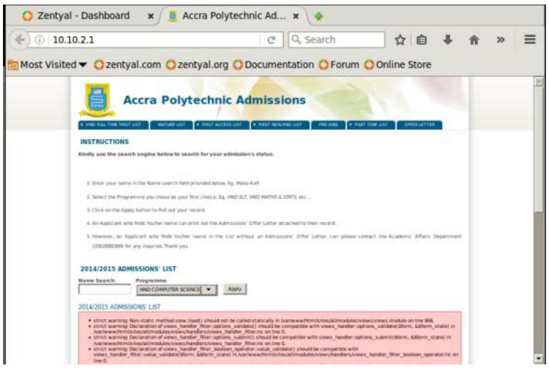

zentyal Trial
zentyal.org
http://www.zentyal.org/?utm_source...ookmark&utm_campaign=ebox.platforn
Created by Zentyal S.L.
SEARCH

Date	Priority	Description	Source	Destination	Protocol	Event
2016-09-03 02:15:58	2	ICMP PING NMAP (Attempted Information Le…	10.10.0.1:8	10.10.2.1:0	ICMP	Alert
2016-09-03 02:14:46	2	ICMP PING NMAP (Attempted Information Le…	10.10.0.1:8	10.10.2.1:0	ICMP	Alert

Page 1

www.zentyal.org/?utm_source=zentyal&utm_medium=bookmark&utm_campaign=ebox.platform

Fig 10: Nmap scan detected by IDS



INSTRUCTIONS

Kindly use the search engine below to search for your admission's status.

1. Enter your name in the Name search field provided below. Eg. Manu Kofi
2. Select the Programme you chose as your first choice. Eg. HND SLT, HND MATHS & STATS, etc...
3. Click on the Apply button to Pull out your record.
4. An Applicant who finds his/her name can print out the Admissions' Offer Letter attached to their record.
5. However, an Applicant who finds his/her name in the List without an Admissions' Offer Letter, can please contact the Academic Affairs Department (0302680309) for any inquiries. Thank you.

2014/2015 ADMISSIONS' LIST

Name Search: Programme: HND COMPUTER SCIENCE Apply

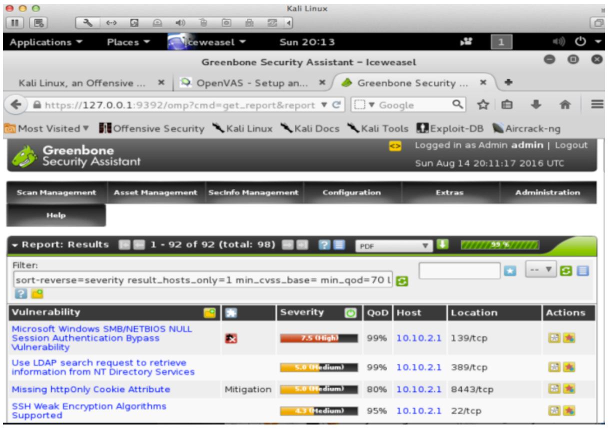
2014/2015 ADMISSIONS' LIST

- strict warning: Non-static method view::load() should not be called statically in /var/www/html/sites/all/modules/views/views.module on line 906.
- strict warning: Declaration of views_handler_filter::options_validate() should be compatible with views_handler::options_validate($form, &$form_state) in /var/www/html/sites/all/modules/views/handlers/views_handler_filter.inc on line 0.
- strict warning: Declaration of views_handler_filter::options_submit() should be compatible with views_handler::options_submit($form, &$form_state) in /var/www/html/sites/all/modules/views/handlers/views_handler_filter.inc on line 0.
- strict warning: Declaration of views_handler_filter_boolean_operator::value_validate() should be compatible with views_handler_filter::value_validate($form, &$form_state) in /var/www/html/sites/all/modules/views/handlers/views_handler_filter_boolean_operator.inc on line 0.

Fig 11: The detected HTTP protocol with port 80 running the web application

3.8 Active Reconnaissance and Vulnerability Assessment

At this point, OpenVAS which is an open source initiative of vulnerability assessment was launched and its web-based (Greenbone security assistant) interface was logged into. OpenVAS was then configured to search for a set of network vulnerabilities by just typing in the IP address of the targeted machine. OpenVAS then scanned the targeted system against the list of known vulnerabilities included in its NVT Feed as shown in figure 12. Once completed with the vulnerability scanning steps, the knowledge necessary to attempt to launch exploits against targeted system had been established. Moving forward, the Metasploit Framework was employed to exploit the known vulnerabilities of the targeted machine thus, further scaling down to specific and critical vulnerabilities. By which time, the Intrusion detection system which had been installed and configured on the targeted machine was already up and running.

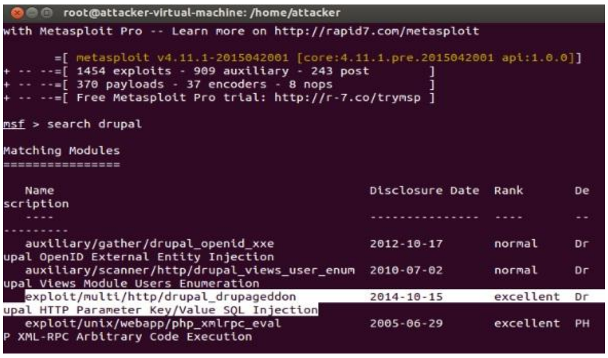


Filter:
sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70 l

Vulnerability		Severity	QoD	Host	Location	Actions
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	☒	7.5 (High)	99%	10.10.2.1	139/tcp	
Use LDAP search request to retrieve information from NT Directory Services		5.0 (Medium)	99%	10.10.2.1	389/tcp	
Missing httpOnly Cookie Attribute	Mitigation	5.0 (Medium)	80%	10.10.2.1	8443/tcp	
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	10.10.2.1	22/tcp	

Fig 12: OpenVAS search report

In this phase, all the identified vulnerabilities were examined to verify if those vulnerabilities were exploitable or not. It was not possible to exploit all threats identified as vulnerabilities, hence, only vulnerabilities that were publicly available to the Metasploit database, were exploited using the Metasploit Framework. Figure 13 clearly shows the vulnerability using metasploit framework and subsequently the intrusion detected from the attack shown in figure 15 respectively. Msfconsole command was used to launch the metasploit framework in kali linux. Figure 13 shows the Metasploit console. Msfconsole which was used to launch exploits, load auxiliary modules, search exploits, perform enumeration against the target host. The Search command was used to search for the exploit using the keyword "drupal" as a search parameter by way of guessing. Figure 13 also shows the four matching modules for the search parameter, of which one of them was of a drupal sql injection value. This module was used to carry out the exploit.

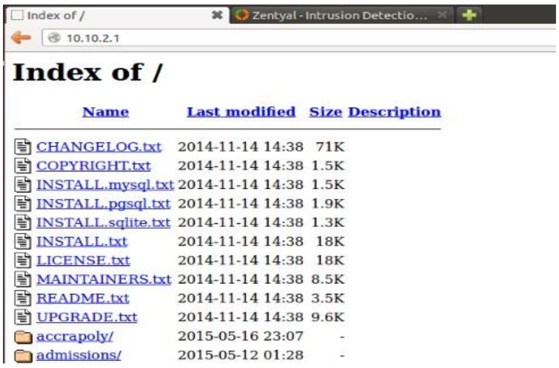


```
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015042001 [core:4.11.1.pre.2015042001 api:1.0.0]]
+ -- --=[ 1454 exploits - 909 auxiliary - 243 post        ]
+ -- --=[ 370 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search drupal

Matching Modules
================

   Name                                          Disclosure Date  Rank       De
scription
   ----                                          ---------------  ----       --
---------
   auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Dr
upal OpenID External Entity Injection
   auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Dr
upal Views Module Users Enumeration
   exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  Dr
upal HTTP Parameter Key/Value SQL Injection
   exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  PH
P XML-RPC Arbitrary Code Execution
```

Fig 13: identified Vulnerability in web application

In bid to exploiting the vulnerability, a reverse handler on 10.10.2.1:4444 was initiated to test the page and consequently created a new user and password combination and enabled the PHP filter module which escalated its privilege to the admin user's profile and finally the meterpreter session opened to allow privilege commands to be executed exposing the web files in the web root to further exploits.

The privilege commands allowed, thus *pwd* which means to print working directory, *rm –rf* Which means to delete the specified file, *rmdir* means to delete directory and many more. In the long run, was executed to delete the index file in the webroot thus resulting in the defacing of the web application in figure 14.

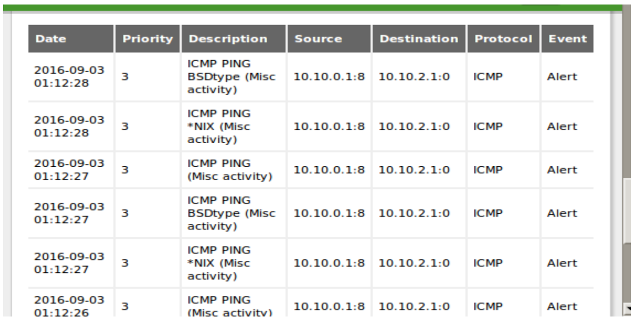


Index of /

Name	Last modified	Size	Description
CHANGELOG.txt	2014-11-14 14:38	71K	
COPYRIGHT.txt	2014-11-14 14:38	1.5K	
INSTALL.mysql.txt	2014-11-14 14:38	1.5K	
INSTALL.pgsql.txt	2014-11-14 14:38	1.9K	
INSTALL.sqlite.txt	2014-11-14 14:38	1.3K	
INSTALL.txt	2014-11-14 14:38	18K	
LICENSE.txt	2014-11-14 14:38	18K	
MAINTAINERS.txt	2014-11-14 14:38	8.5K	
README.txt	2014-11-14 14:38	3.5K	
UPGRADE.txt	2014-11-14 14:38	9.6K	
accrapoly/	2015-05-16 23:07	-	
admissions/	2015-05-12 01:28	-	

Fig 14: Successful defacing of web application

Figure 14 shows the defaced web application exposing the
various directories in the web server whereas in Figure 15 the
intrusions had been captured by the IDS.



Date	Priority	Description	Source	Destination	Protocol	Event
2016-09-03 01:12:28	3	ICMP PING BSDtype (Misc activity)	10.10.0.1:8	10.10.2.1:0	ICMP	Alert
2016-09-03 01:12:28	3	ICMP PING *NIX (Misc activity)	10.10.0.1:8	10.10.2.1:0	ICMP	Alert
2016-09-03 01:12:27	3	ICMP PING (Misc activity)	10.10.0.1:8	10.10.2.1:0	ICMP	Alert
2016-09-03 01:12:27	3	ICMP PING BSDtype (Misc activity)	10.10.0.1:8	10.10.2.1:0	ICMP	Alert
2016-09-03 01:12:27	3	ICMP PING *NIX (Misc activity)	10.10.0.1:8	10.10.2.1:0	ICMP	Alert
2016-09-03 01:12:26	3	ICMP PING (Misc activity)	10.10.0.1:8	10.10.2.1:0	ICMP	Alert

Fig 15: Detected Intrusion by IDS

In conclusion, SQL injection attack was the prevalent vulnerability attack, discovered at the end of the penetration test.

4. RESULTS AND DISCUSSIONS

After performing the experiments using the Cloppert's "Kill chain" Approach of penetration in the methodology, this part of the report seeks to fully discuss the outcomes of the experiments. Generally, free and open source solutions were used for the simulation of intrusion detection on campus network. Once the target systems were tested for vulnerabilities and weaknesses using OpenVAS, these vulnerabilities were exploited by using publicly available exploits. Metasploit framework was used for vulnerability exploitation to determine whether an attack was possible. Also, Kali Linux was one powerful Free and Open Source Software tool employed to carry out multiple attacks from one attacking machine. The simulation was carried out in a Virtual Environment using the Zentyal unified network, which has in it, pre-installed systems that needed to be configured. Such tools are the DHCP module, Gateway module, Intrusion detection module, and many more other modules, which are not necessarily related to this study.

4.1 Results from Fping

In figure 8 the Fping result reveals that three nodes were alive on the Local Area Network as shown in table 3 whereas the rest of the IP addresses are unreachable since they are not up and running.

Table 3: Fping result

IP Addresses	Status
10.10.2.1	Alive
10.10.2.2	Alive
10.10.2.3	Unreachable
10.10.2.4	Alive

4.2 Implication of Fping result

Fping like the normal ping test is the quickest way to scout on the network for nodes that are up and running so as to allow for concentration on a selected block of IP addresses that may have the Alive signature. This action also forestalls the event of a wild goose chase in bid to identifying a node to attack on a network.

4.3 Results from Nmap Scan

In figure 9, the Nmap result of 10.10.2.1 reports about 15 opened ports on the Zentyal server were running, however, three of them have been tabulated in the table 3. All of these ports are expensive information that can lead to further exploitations. Hence, it's advisable to keep certain ports closed if not in use. Intelligence gathering provided the foundation for the next scanning and vulnerability assessment phase.

Table 4: Nmap result on 10.10.2.1

IP Address	Port	State	Service
10.10.2.1	22/tcp 53/tcp 80/tcp	Open Open Open	ssh domain http

4.4 Implication of Nmap result

In table 4, the ports that were opened in the Nmap result suggests that, certain special services that were running on the computer, had helped in giving off vital information for further attacks to be carried out on the node under surveillance by the attacker.

4.5 Results from Intrusion Detection

In Figure 10 the result from the IDS is represented in a tabular form as shown in table 5 which means an NMAP protocol event occurred on 2016-09-03 from a source 10.10.0.1 through port 8 to a Destination 10.10.2.1 through port 0. The priority value shows how critical that event is to the system. Obviously priority 1 would have posed a critical security concern. Nevertheless, priority 2 should create some security alertness should an adverse attack happen.

Table 5: IDS result during Nmap scan

Date	Priority	Description	Source	Destination
2016-09-03 02:14:46	2	ICMP PING NMAP	10.10.0.1:8	10.10.2.1:0

4.6 Implication of IDS result

This is a useful tool to the network administrator since network attacks are logged, stored and quickly brought into sharp focus the moment an attack occurs. This can really help in giving a security policy direction that will improve network security.

4.7 Exploitation Phase

At this stage, vulnerabilities identified using OpenVAS were verified to find out whether the vulnerabilities and loopholes identified during scanning and vulnerability assessment phase posed any critical security threat. This phase acted as verification of potential vulnerabilities enumerated in the OWASP Top 10 -2013 vulnerabilities. Table 6 highlights on the full features entailed within the search results. During this exploitation phase, vulnerabilities were exploited by using publicly available exploits. Metasploit was one of such open source exploitation frameworks that were extensively used during this exploitation phase of the penetration test. Based on the information discovered from the vulnerability scanning stage target hosts (all from the internal network segment) with identified vulnerabilities, which were selected for further research and possible exploitation.

Table 6: Web application vulnerability

Name of Vulnerability	Disclosure date	rank	Description
exploit/multi/http/drupal_drupageddon	2014-10-15	Excellent	Drupal Http Parameter key/value sql injection

4.8 Implication of metasploit search result

Further to the vulnerability analysis, in table 6, the metasploit search result reveals the kind of exploitation to carry out having in mind its relevance and ranking.

4.9 Implications of Exploiting web application

Metasploit, reported host 10.10.2.1 to be running a web application that had a drupal sql vulnerability in figure 13. This vulnerability was exploited. This vulnerability can allow the attacker to vertically elevate his privilege as the web server admin on the host. When this was exploited the host 10.10.2.1, system gave the attacker the admin user privilege over the network to compromise the system. Following the vulnerability analysis is the exploitation mode where metasploit presented the remote platform to unleash the attack meltdown that finally puts the system in a compromised position, a state every attacker is happy about.

5. CONCLUSION AND RECOMMENDATION

The dependence on Internet is increasing day by day. Attacks and malicious activities are very common in this cyber world. An intrusion detection system is an essential mechanism to help create awareness that could protect computers applications and networks from attacks. The underlying security issues however leave much to be concerned about as networks particularly those of educational institutions are mostly more vulnerable to security breaches due to the limitations of their security mechanisms as a result of budgetary constraints. Hence the need for this research, which brought to the fore, a cost effective way of simulating intrusion detection on campus networks using FOSS tools. Detailed experimental tests have shown that the simulation worked as per the defined functions of detecting intrusions from attack methods like Xmas scans and SQL injection.

It is therefore recommended, that in view of the benefits of this simulation framework, management of the institution should consider this report in so as to augment the already existing security policies for the institution’s network.

6. REFERENCES

[1] Bragg, R., Phodes-Ousley, M., & Strassberg, K. (2004). Network Security: The complete Reference. McGraw-Hill/ Osborne (Vol. 53). http://doi.org/10.1017/CBO9781107415324.004

[2] White, J. S., Fitzsimmons, T., & Matthews, J. N. (2013). Quantitative analysis of intrusion detection systems: Snort and Suricata. Proceedings of SPIE, 8757, 875704. http://doi.org/10.1117/12.2015616

[3] Pathan, A. (2014). The State of the Art in Intrusion Prevention and Detection, 472. Retrieved from http://books.google.com/books?hl=en&lr=&id=o39cAgAAQBAJ&oi=fnd&pg=PP1&dq=The+State+of+the+Art+in+Intrusion+Prevention+and+Detection&ots=yD8AGesoz9&sig=rdvWXKWoK5f0UHio9n4QSJe0NB8

[4] Zentyal Documentation. 3rd June 2016. https://wiki.zentyal.org/wiki/Zentyal_Wiki

[5] Liebowitz, M., Kusek, C., & Spies, R. (2014). VMware vSphere Performance.

[6] Kennedy, D., O’Gorman, J., Kearns, D., & Aharoni, M. (2013). Metasploit the Penetration Tester’s Guide. Computers & Security (Vol. 32). http://doi.org/10.1016/j.cose.2012.09.009

[7] Beggs, R. W., Cutler, T. P., Heriyadi, D., Singh, T., Amit, K., Karpe, P., … Jones, J. (2014). Mastering Kali Linux for Advanced Penetration Testing Mastering Kali Linux for Advanced Penetration Testing Cover image. Retrieved from www.packtpub.com

[8] OWASP top 10-2013. 16 September 2016. https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf