

OSSIM

**Pauline Finlay**

**B00107945**

***Department of Informatics***

***School of Informatics & Engineering***

***Technological University Dublin, Blanchardstown***

***Dublin 15.***

**Word Limit for Assignment: 3500 Actual Word Count: 2656**

**BSc (Hons) in Computing in Digital Forensics & Cyber Security**

**DFCS H4015 Network Security Analytics**

**11 January 2021**

**Plagiarism Declaration**

I hereby certify that this material, which I am submitting for assessment for the course title of BSc. (Hons) In Computing in Digital Forensics and Cyber Security is my own work and that I have:

* Clearly referenced/listed all sources as appropriate
* Given the sources of all pictures, data etc. that are not my own
* Any work of any other student(s) either past or present is clearly referenced
* Not submitted for assessment work previously submitted for any other course, degree or qualification
* Not incorporated any text acquired from external agencies other than extracts from attributed sources (including online facilities)
* Acknowledged in appropriate places any help that I have received from others (e.g. fellow students, technicians, statisticians, external sources)
* My work may be electronically checked for plagiarism, including, but not exclusively, by the use of plagiarism detection software and stored for future comparison
* Any false claim for this work will be penalised in accordance with the College’s regulations

**Signature:** Pauline Finlay **Date:** 11/01/2021

**Abstract**

This report is an analysis of Pen Testing techniques and a small sample of attacks carried out against a test environment to Scan, Gain and Maintain access. AlienVault OSSIM has been hosted on a Virtual Box VM to monitor this system and analyze how these attacks are identified if at all.

Table of Contents

[1 Introduction 7](#_Toc61106795)

[2 Pen Testing Research 8](#_Toc61106796)

[3 Lab Setup 10](#_Toc61106797)

[4 Attacks 11](#_Toc61106798)

[4.1 Scanning 11](#_Toc61106799)

[4.1.1 Attack 1: Nmap Scan 11](#_Toc61106800)

[4.1.2 Attack 2: Nikto Scan 14](#_Toc61106801)

[4.2 Gaining Access 16](#_Toc61106802)

[4.2.1 Attack 3: Brute Force Apache Tomcat 16](#_Toc61106803)

[4.2.2 Attack 4: FTP backdoor 19](#_Toc61106804)

[4.3 Maintaining Access 21](#_Toc61106805)

[4.3.1 Attack 5: 21](#_Toc61106806)

[4.3.2 Supplementary Attack: 26](#_Toc61106807)

[5 Mitigation 27](#_Toc61106808)

[6 Conclusion 29](#_Toc61106809)

[7 References 30](#_Toc61106810)

[8 Appendix 31](#_Toc61106811)

[8.1 Presentation Link 31](#_Toc61106812)

[8.2 Nmap Scan 32](#_Toc61106813)

[8.3 Nmap Scan of 192.168.56.103 36](#_Toc61106814)

[8.4 Nikto Scan 37](#_Toc61106815)

**Table of Tables**

[Table 1: Test Machines 10](#_Toc61106816)

**Table of Figures**

[Figure 1: Pen Testing Stages www.slideteam.net [1] 9](#_Toc61106817)

[Figure 2: Discover IP addresses on network - **sudo netdiscover** 11](#_Toc61106818)

[Figure 3: Nmap scan of 192.168.56.103 12](#_Toc61106819)

[Figure 4: Event alerts generated by Nmap scan 12](#_Toc61106820)

[Figure 5: IRC chat 'Low' risk alarm 13](#_Toc61106821)

[Figure 6: Medium risk IRC alert 13](#_Toc61106822)

[Figure 7: Metasploitable Wb Application 14](#_Toc61106823)

[Figure 8: Nikto scan 14](#_Toc61106824)

[Figure 9: OSSIM showing alerts generated 15](#_Toc61106825)

[Figure 10: Drilling into Nikto generated alert 15](#_Toc61106826)

[Figure 11: Run Brute Force Login exploit 16](#_Toc61106827)

[Figure 12: Set RHOST, RPORT and STOP\_ON \_SUCCESS 16](#_Toc61106828)

[Figure 13: Output of all username:password combinations tested 17](#_Toc61106829)

[Figure 14: Username **tomcat** and password **tomcat** identified 17](#_Toc61106830)

[Figure 15: Apache Tomcat password unencrypted on Port 8180 18](#_Toc61106831)

[Figure 16: Select the attack – **use** **unix/ftp/vsftpd\_234\_backdoor** 19](#_Toc61106832)

[Figure 17: Check attack requirements - **show options** 19](#_Toc61106833)

[Figure 18: Set RHOSTS requirement - **set RHOST 192.168.56.103** 20](#_Toc61106834)

[Figure 19: Execute the attack - **exploit** 20](#_Toc61106835)

[Figure 20: FTP vsftpd exploited detected 20](#_Toc61106836)

[Figure 21: Apache Tomcat on port 8180 accessed through browser 21](#_Toc61106837)

[Figure 22: Apache Tomcat Manager Login Screen 21](#_Toc61106838)

[Figure 23: Application Manager Screen listing applications and deployment methods 22](#_Toc61106839)

[Figure 24: Create WAR file in msfvenom 22](#_Toc61106840)

[Figure 25: File pwn.war saved on the Kali machine for upload 23](#_Toc61106841)

[Figure 26: Deploy WAR file to server 23](#_Toc61106842)

[Figure 27: WAR file pwn.war visible in Applications List 24](#_Toc61106843)

[Figure 28: Start Listener in Kali using Netcat 24](#_Toc61106844)

[Figure 29: Connection on Netcat Listener 24](#_Toc61106845)

[Figure 30: Access as user tomcat55 24](#_Toc61106846)

[Figure 31: Apache Tomcat Exploit detected 25](#_Toc61106847)

[Figure 32: Disable the root folder 26](#_Toc61106848)

[Figure 33: 503 error page when 'Welcome to Tomcat' page stopped 26](#_Toc61106849)

[Figure 34: OSSIM Vulnerability Scan Results by Severity 27](#_Toc61106850)

[Figure 35: OSSIM Vulnerability Scan Results by Service 27](#_Toc61106851)

# Introduction

The objective of this assignment was to implement Alien Vault OSSIM (Open Source Security Information Management) as a SIEM (Security Information and Event Management) on a VM (virtual machine) and carry out a series of attacks against the system using a second VM. Pen testing techniques were researched to carry out the attacks. The attacks are subsequently examined in OSSIM to gain an understanding of how alerts are generated, attacks identified and mitigated against. In total 5 attacks of increasing complexity are to be executed.

# Pen Testing Research

There are 5 main steps in the Pen Testing Process:

**Planning & Reconnaissance**

During this phase, the aim is to gain as much information as possibleabout the target such as IP addresses, domain details, mail servers, network topology, etc. This is key to the pen testing process as the information gathered during this stage will prove invaluable during the remaining phases. Examples include Open Source Intelligence (OSINT) which provide a variety of tools to gain information about the target.

**Scanning**

At this point we begin interacting with the target sending probes and scanning the system to see what response, if any is received. Examples of scanning techniques include Nmap, Nessus and Niko scans.

**Gaining access**

Once weaknesses have been identified in the system the next phase is to try to exploit these weaknesses and obtain access to the system. There are numerous ways of gaining access to a system but depend on the vulnerabilities found.

**Maintaining Access**

Once access is obtained the next step is to maintain it even is the system is rebooted, reset or modified. This is known as persistence and allows attackers to gain knowledge of the over a period and exploit it at the most opportune time. Examples may include escalating privilege, compromising other system tools, inserting files or scripts.

**Analysis & Firewall Configuration**

It is at this stage that pen testing differs from an actual attack. An attacker would now exploit the system for their personal or financial gain but in the pen testing scenario this is controlled, and the vulnerabilities reported back to the client. It is then up to the client or management in an internal testing environment to address and mitigate the vulnerabilities or accept them.

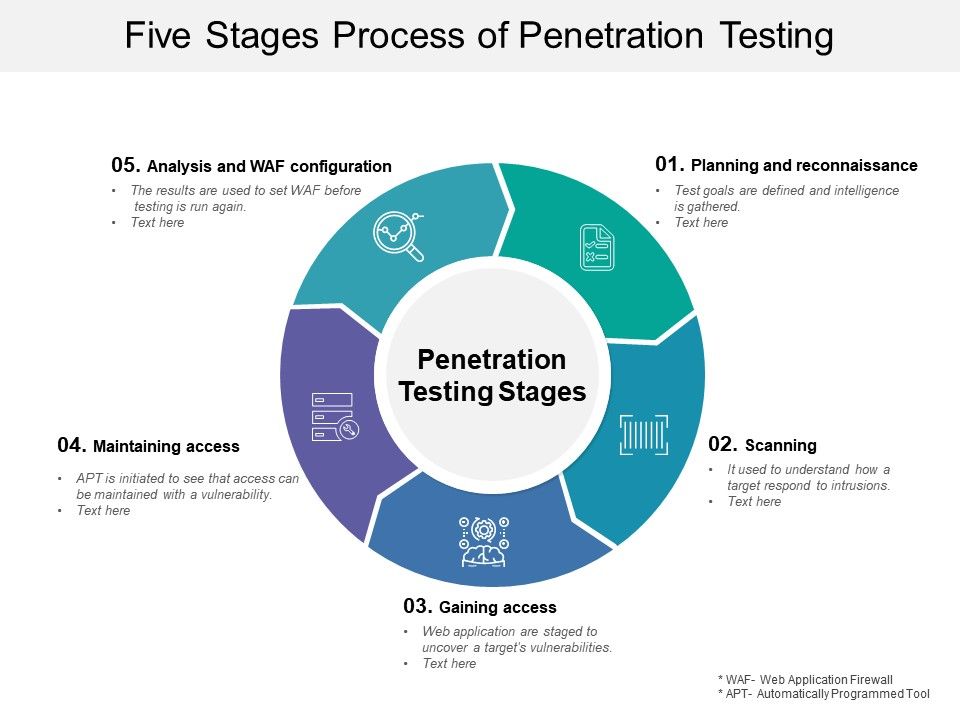


Figure 1: Pen Testing Stages [www.slideteam.net](http://www.slideteam.net) [1]

# Lab Setup

Virtual Box 6.1.16 was used to host the virtual machines used in this investigation. Due to the hardware limitations of the host machine a simple topography for testing was implemented. Metasploitable is our victim machine and is being monitored by OSSIM and attacked from a Kali Linux box.

Table 1: Test Machines

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **IP Address** | **Operating System** | **Function** |
| Metasploitable | 192.168.56.103 | Linux | The is a deliberately vulnerable machine designed for testing |
| OSSIM | 192.168.56.102 Network  192.168.56.106 Mgmt | Linux | SIEM for analysis |
| Kali-Linux | 192.168.56.104 | Linux | The attack machine |

# Attacks

Reconnaissance is the first step in a pen testing engagement but in this test scenario we are dealing with private IP addressing in an internal network so a search would not reveal any useful information. In this situation we can use the command ***‘sudo netdiscover’*** to see the IP addresses configured on the network.



Figure 2: Discover IP addresses on network - **sudo netdiscover**

We are also not dealing with an organisation so the OSINT tools would not be useful in gaining information about the organisation structure. In this scenario the most valuable source of information is in scanning and will provide a foothold from which to begin testing.

The attacks carried out in this assessment were carried out in keeping with stages 2, 3 and 4 in the Pen Testing lifecycle namely scanning, gaining access and maintaining access.

## Scanning

### Attack 1: Nmap Scan

#### Implementation

An Nmap scan was used to detect the services running and the ports assigned to those services. The command used was:

***nmap -sV -sC -A 192.168.56.100/24***

where **-sV** outputs the version of service on port, **-sC** issues command scripts automating common tasks and **-A** the OS service and version**.**

The results of this scan revealed several interesting items which may prove fruitful for an attacker. IP 192.168.56.103 which was the Metasploit machine shows port 21 was open for ftp and allowed anonymous login. On ports 139 and 445 Samba was running and there are known exploits available for certain versions, Apache was running on port 8180 which also contains vulnerabilities in certain versions. The full report is available in Appendix 8.2.

For a tidier version of the ports and services running on 192.168.56.103 the command ***‘nmap -sV -p- 192.168.56.103’*** was run, see Appendix 8.3.



Figure 3: Nmap scan of 192.168.56.103

#### Analysis

Analysis the security events in the Alien Vault SIEM the scan generated several alerts. Among the Event Name alerts generated were:

* **SSHd: Did not receive identification string**
* **AlienVault HIDS: SSH insecure connection attempt**
* **sudo: Session opened**
* **sudo: Session closed**
* **AlienVault HIDS: Login session opened**
* **AlienVault HIDS: Login session closed**
* **SSHd Session disconnected**
* **AlienVault NIDS: “ET SCAN possible Nmap User Agent Oberved”**
* **AlienVault NIDS: “AV-RULES FTP password detected in cleartext”**
* **AlienVault NIDS: “ET TROJAN IRC USER command”**
* **directive\_event: AV-FREE-FEED Policy violation, IRC chat usage on SRC\_IP**
* **AlienVault NIDS: “ET TROJAN IRC NICK command”**

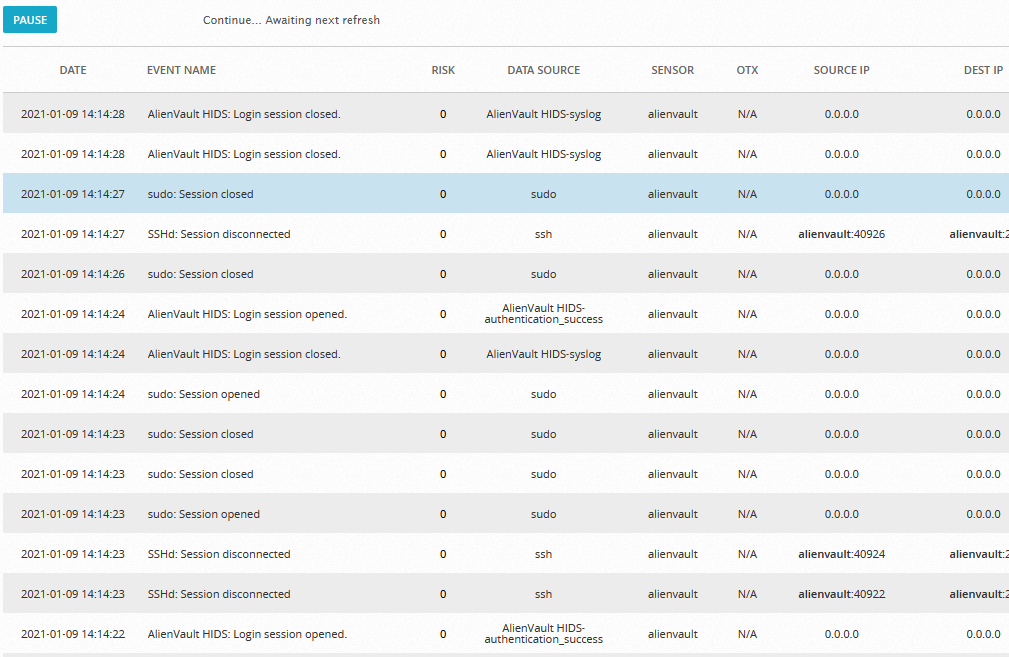


Figure 4: Event alerts generated by Nmap scan

The only event which generated an alarm was the IRC chat but was initially labelled ‘Low’ risk and categorised under Environmental Awareness.

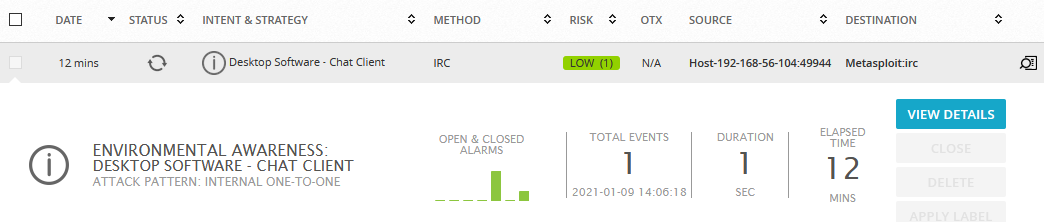


Figure 5: IRC chat 'Low' risk alarm

However this was escalated to ‘Medium’ risk under the event **name ‘directive\_event: AV-FREE-FEED Policy violation, IRC chat usage on 192.168.56.104’**. The Nmap command used uses common scripts and it is believed that one of them initiated an IRC chat triggering the alert.



Figure 6: Medium risk IRC alert

### Attack 2: Nikto Scan

#### Implementation

The Nmap scan identified port 80 as open on the Metasploitable 2 machine. Opening this page in the browser we see a simple web application.

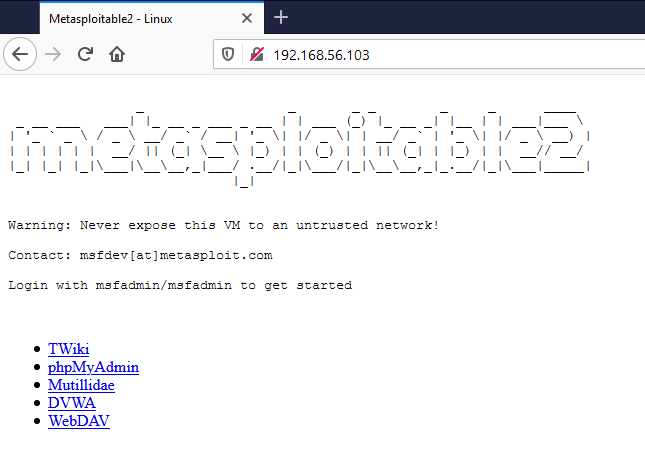


Figure 7: Metasploitable Wb Application

Using a Nikto scan on IP address 192.168.56.103 we can gain extra information about the service. The command used:

**sudo nikto -h 192.168.56.103**

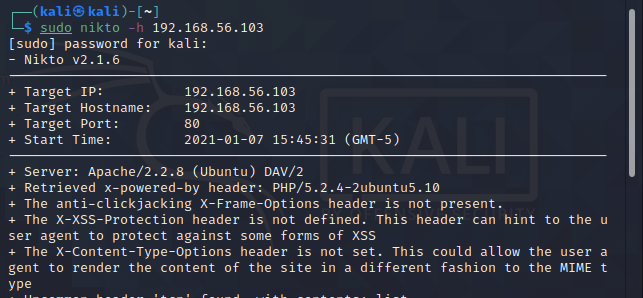


Figure 8: Nikto scan

The server hosting the application is Apache 2.2.8 which is and outdated version. There are also numerous issues in the configuration – the /doc/ directory is browsable, potentially sensitive information is revealed via certain HTTP requests, the phpMyAdmin directory was found and is responsible for managing MySQL databases and should be limited to authorised users. The full scan report can be found in Appendix 8.4.

#### Analysis

This scan triggers alerts in OSSIM under the event name ***‘AlienVault NIDS: ET WEB\_SERVER Possible CVE-2014-6271 Attempt’***.

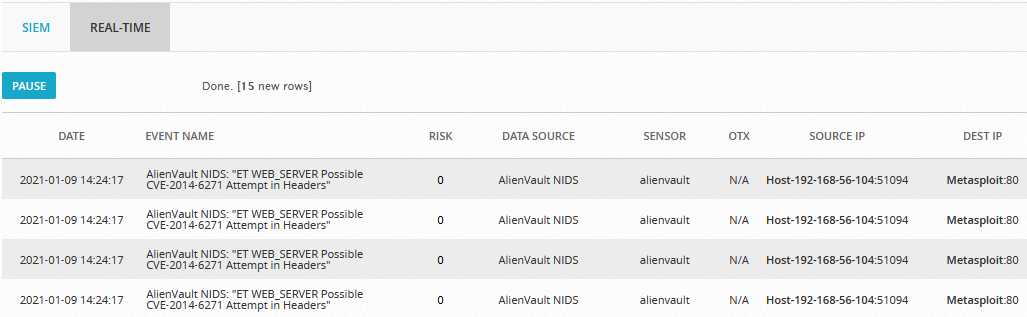


Figure 9: OSSIM showing alerts generated

Drilling into this alert we can see the attacker IP and MAC address together with Sub-Category for the alert which is and ‘**IDS Alert’**.

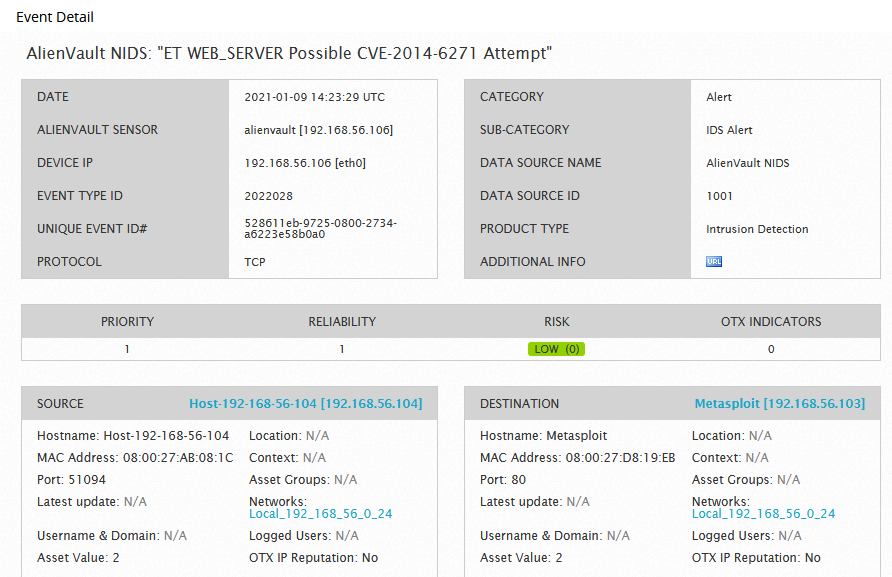


Figure 10: Drilling into Nikto generated alert

## Gaining Access

Metasploit Framework is a powerful tool used to probe and exploit vulnerabilities on a network or server. It is easily customisable making it relatively easy to use. We will take advantage of this to gain access to the system.

### Attack 3: Brute Force Apache Tomcat

Apache Tomcat was identified in the Nmap scans as running on port 8180. In this attack we will use Metasploit to Brute Force the Login Credentials. Searching for a suitable Metasploit module identifies **‘scanner/http/tomcat\_mgr\_login’** [2].

#### Implementation

Opening the Metasploit Framework we choose this exploit and enter the **‘show options’** command to check the prerequisites.



Figure 11: Run Brute Force Login exploit

We must the then set the RHOST, RPORT as port 8080 is selected by default not 8180 as in this scenario and set it to stop running when successful login credentials are obtained. We them run the exploit.

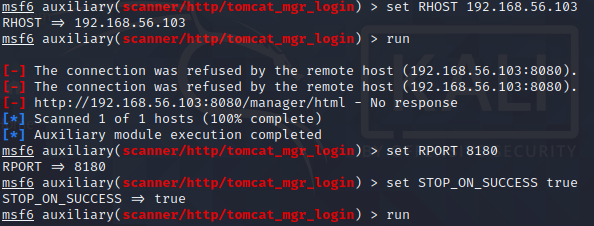


Figure 12: Set RHOST, RPORT and STOP\_ON \_SUCCESS

The exploit runs through many possible username and password combinations until a valid combination is found.



Figure 13: Output of all username:password combinations tested

The username:password combination of **tomcat:tomcat** is identified.



Figure 14: Username **tomcat** and password **tomcat** identified

#### Analysis

Checking the SIEM logs at this time the event Name **‘ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted’** is detected on Meatsploit:8180.



Figure 15: Apache Tomcat password unencrypted on Port 8180

### Attack 4: FTP backdoor

#### Implementation

Armed with information gathered in the Nmap scan we see that ftp allows anonymous login and that the version it uses is vstfpd 2.3.4. A google search to see if there are any exploits for this version reveals that there is a Metasploit module available for the specified version which runs a Backdoor Command Execution allowing the attacker to gain access called VSFTPD v2.3.4 Backdoor Command Execution [3]

To select this attack, we open the Metasploit Framework in Kali and enter ***‘use unix/ftp/vsftpd\_234\_backdoor’*** but before we can execute the attack, we need to configure the payload.



Figure 16: Select the attack – **use** **unix/ftp/vsftpd\_234\_backdoor**

In order to check the prerequisites for this payload we enter ***‘show options’*** which reveals that just the RHOSTS and RPORT are required and in this case the port number is already set to 21 which is what we require. The host needs to be set to the IP address of the metasploitable machine.

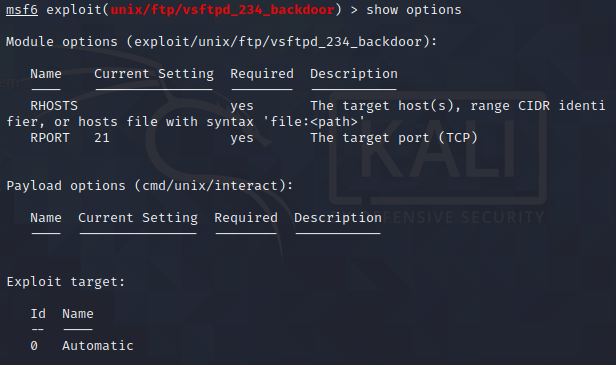


Figure 17: Check attack requirements - **show options**

To set the RHOSTS requirement we enter ***‘set RHOST 192.168.56.103’*** which is the IP address of the metasploitable machine.



Figure 18: Set RHOSTS requirement - **set RHOST 192.168.56.103**

The exploit is executed by entering ‘exploit’ or ‘run’.

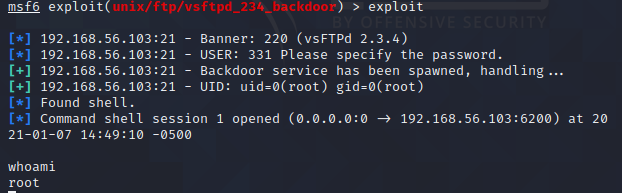


Figure 19: Execute the attack - **exploit**

In this instance the attack was successful, and a shell was spawned, entering the command **‘*whoami’*** we can see that we have successfully gained access as the root user.

#### Analysis

Analysing the security events, we can see that the SIEM identified the attack under 2 distinct Event Names, ***‘ET POLICY Possible Kali Linux hostname in DHCP Request Packet’*** and ***‘AV-RULES FTP password detected in cleartext’.***

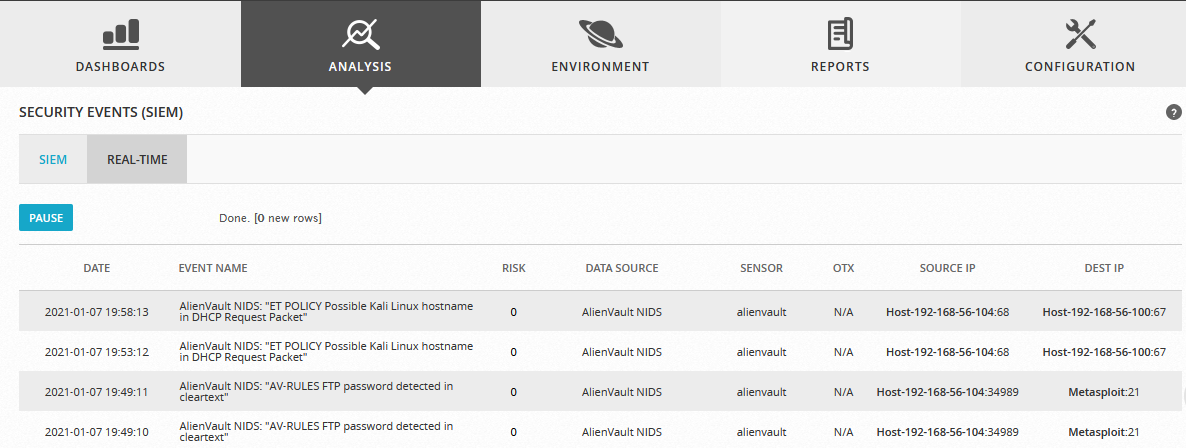


Figure 20: FTP vsftpd exploited detected

## Maintaining Access

The final attack carried out was concerned with persistent access. Using the Apache Tomcat credentials obtained from the Brute Force attack.

### Attack 5:

#### Implementation

Open the service in browser on 192.168.56.103:8180 and login into the Administration section under Tomcat Manager and login with username **tomcat** and password **tomcat**.

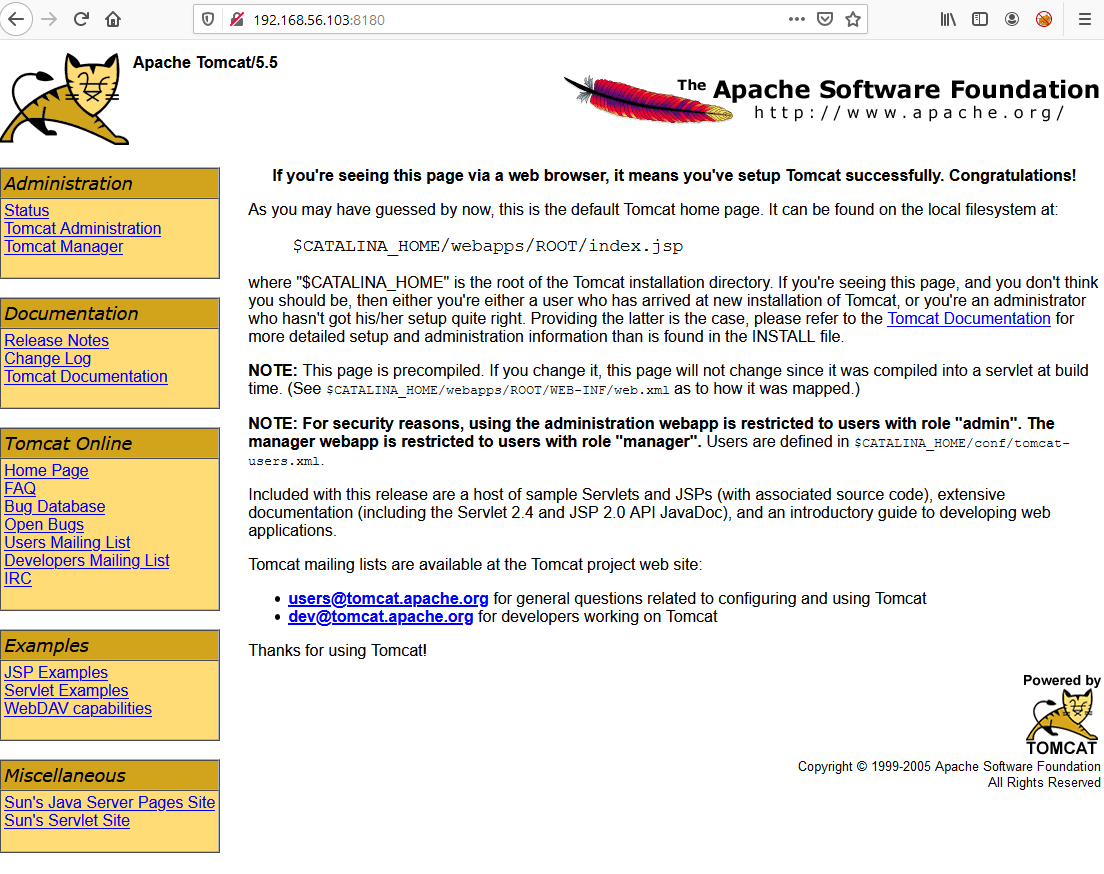


Figure 21: Apache Tomcat on port 8180 accessed through browser

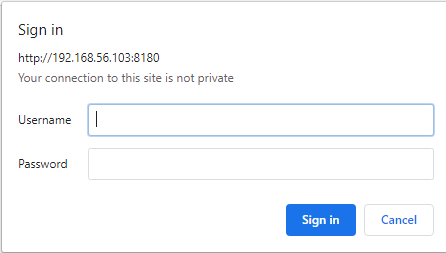


Figure 22: Apache Tomcat Manager Login Screen

Under the application manager section, we can see a list of applications running and deployment methods available to us. For this attack we will deploy a WAR file to the application [4].

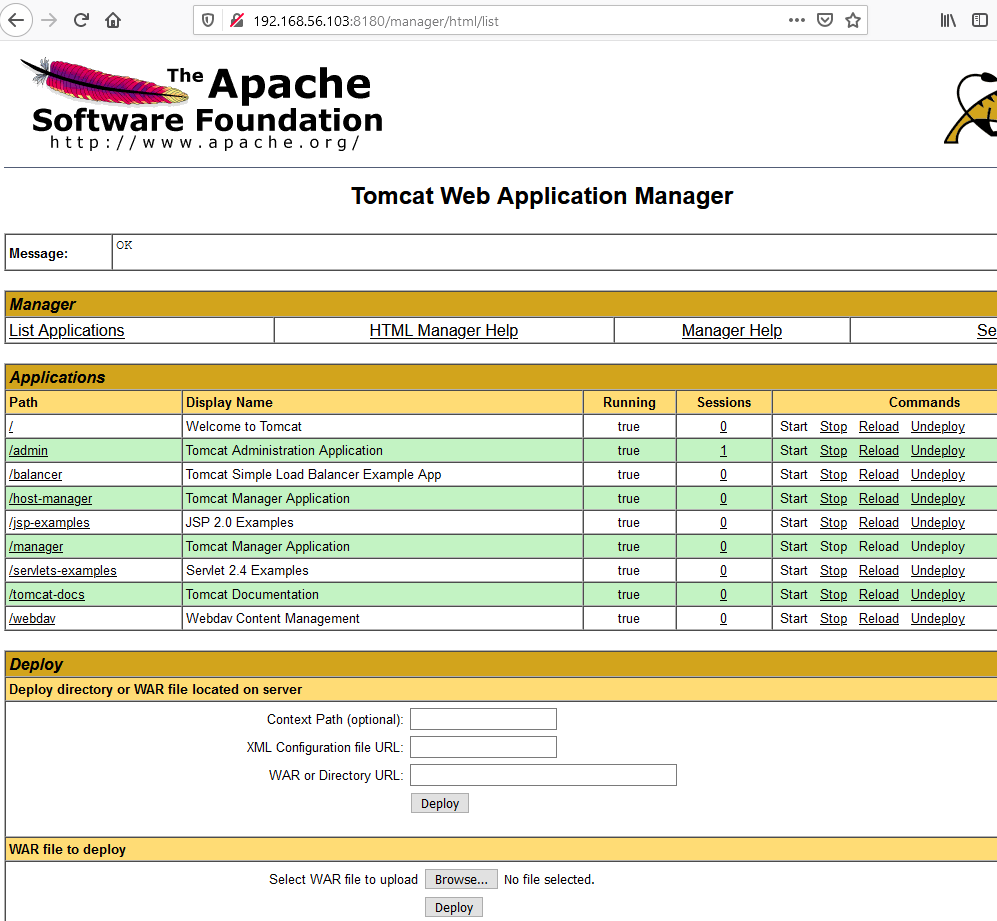


Figure 23: Application Manager Screen listing applications and deployment methods

Before we can deploy the WAR file we must first create one and this is done through msfvenom, which will generate a reverse shell on our kali machine on port 4321 when the page is opened.

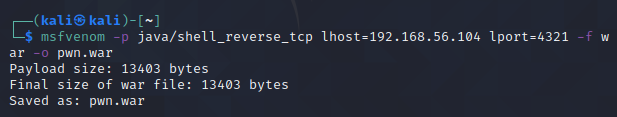


Figure 24: Create WAR file in msfvenom

The WAR file is called pwn.war and is saved on the Kali machine from where it will be uploaded to the Apache server.

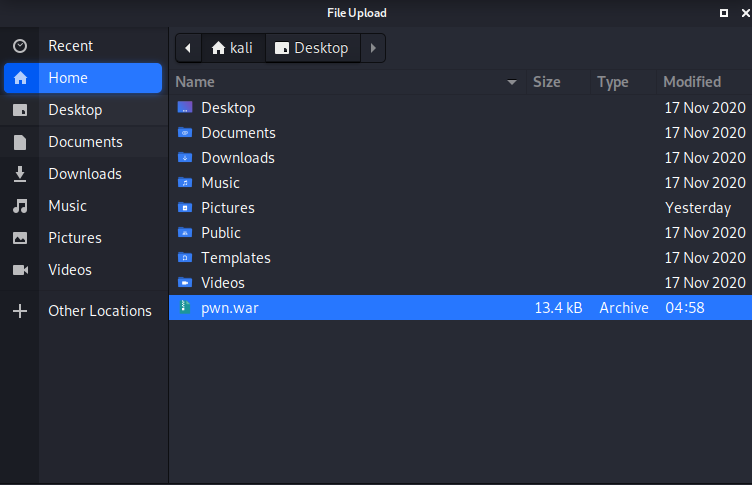


Figure 25: File pwn.war saved on the Kali machine for upload

Moving back to the Apache server in the browser we move down to deploy the WAR file browse to the save location and select the file and deploy.

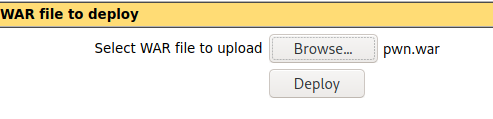


Figure 26: Deploy WAR file to server

Once the file has been deployed it is visible in the applications list ready for us to open but before we do this, we need to start a listener on the Kali Machine on port 4321 using Netcat with the command:

**nc -lvnp 4321**

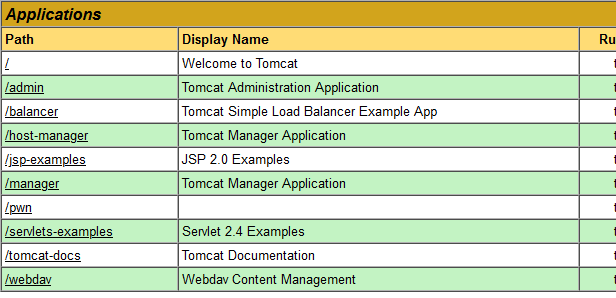


Figure 27: WAR file pwn.war visible in Applications List



Figure 28: Start Listener in Kali using Netcat

When we open the pwn file on the browser the get a connection in the listener.

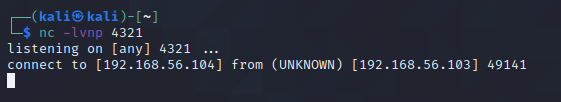


Figure 29: Connection on Netcat Listener

When we type in the **‘whoami’** command we see that we have access as user tomcat55.

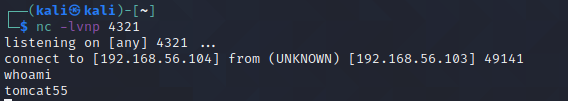


Figure 30: Access as user tomcat55

#### Analysis

Analysing the SIEM events in connection with this attack there is just one Event Name Triggered, **‘AlienVault NIDS:** “**ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted”’.**

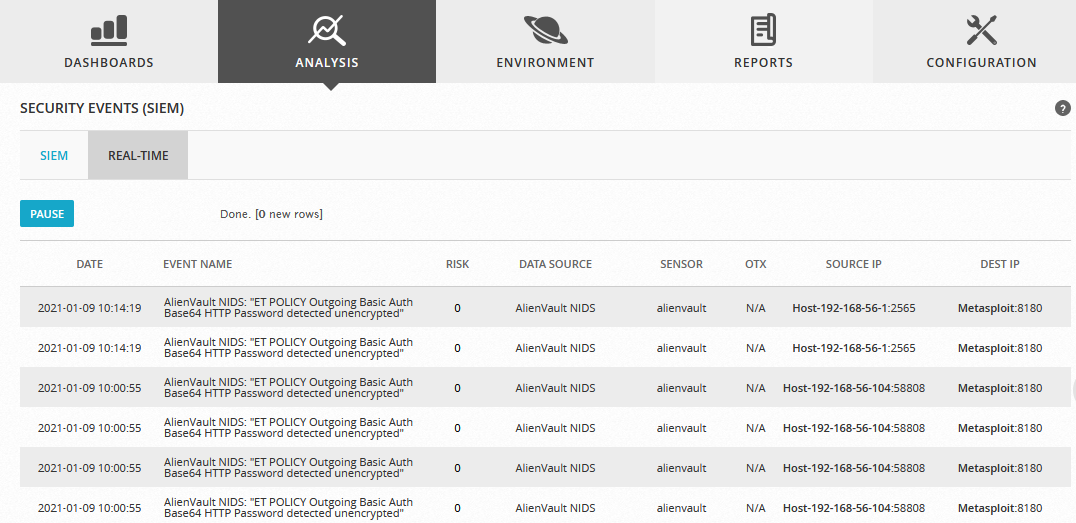
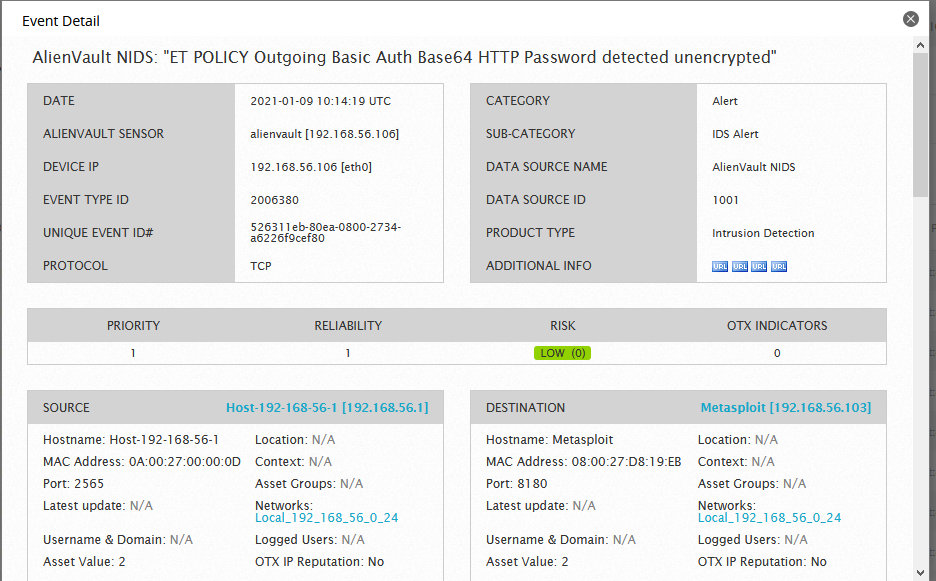


Figure 31: Apache Tomcat Exploit detected

Drilling into this alert



### Supplementary Attack:

#### Implementation

With access to the Apache Tomcat Application Manager page it is also possible to disrupt the service by simply stopping the service, redeploying or reloading application. As a proof of concept simply stop the ‘Welcome to Tomcat’ page by pressing Stop as highlighted in yellow.

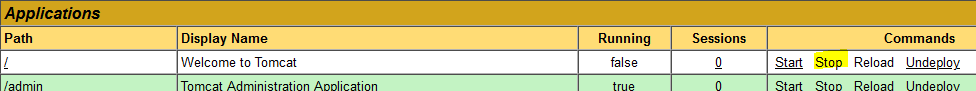


Figure 32: Disable the root folder

Once the page has been stopped when open the application in the browser on 192.168.56.103:8180 again and this time there is 503 error page.

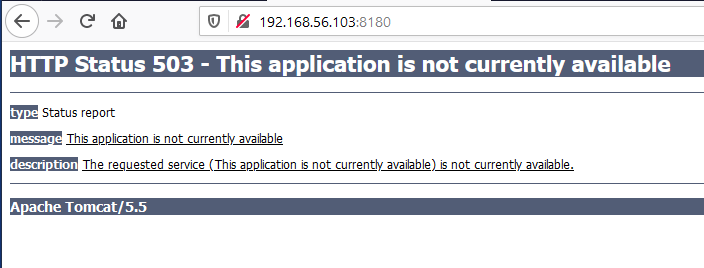


Figure 33: 503 error page when 'Welcome to Tomcat' page stopped

# Mitigation

OSSIM offers a vulnerability scan tool this was ran against the Metasploit Machine IP 192.168.56.103 and revealed the following results by severity.

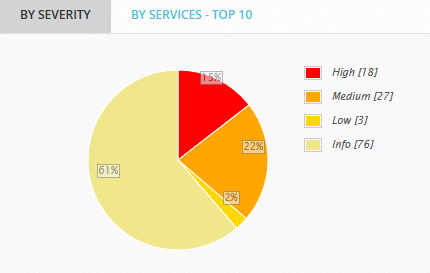


Figure 34: OSSIM Vulnerability Scan Results by Severity

The scan can also breakdown the results in terms of the Top 10 Services.

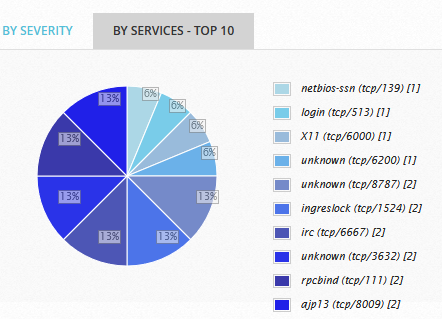


Figure 35: OSSIM Vulnerability Scan Results by Service

The full results of the scan are also available in HTML, PDF or Excel format and the scan results for 192.168.56.103 are available and should be investigated and remediated against.

Among the findings in this report 18 issues were identified with high severity namely:

* **OS End of Life Detection – Ubuntu 8.04**
* **FTP Brute Force Login Possible with Weak/Known Credentials**
* **SSH Brute Force Login with Default Credentials**
* **PHP-CGI-based setups vulnerability when parsing query string parameters from php files**
* **Test HTTP dangerous methods**
* **phpinfo() output Reporting**
* **TWiki XSS and Command Execution Vulnerabilities**
* **Check for rexecd Service**
* **Check for rsh Service**
* **Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability**
* **Possible Backdoor: Ingreslock**
* **FTP Brute Force Logins Reporting**
* **MySQL / MariaDB weak password**
* **DistCC Remote Code Execution Vulnerability**
* **PostgreSQL weak password**
* **VNC Brute Force Login**
* **Apache Tomcat AJP RCE Vulnerability**
* **Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities**

For each vulnerability there is a recommended solution and this report should be provided to management with the pen test report for them to make the decision regarding remediation or acceptable risk.

Generally default or weak passwords should never be used and would be the basic recommendation for remediation.

Within OSSIM alerts can be drilled into as shown in the context of this report and if necessary a ticket can be issued to escalate the alert for further investigation.

# Conclusion

The setup and installation of the Alien Vault OSSIM is not for the novice user and due to the large amount of RAM required is beyond the reach of most home users. The attacks carried out in this report were limited by the processing power available and only cover a minute selection of what is available to even a novice attacker. They were chosen to reflect the goals of a pen test covering scanning and enumeration, gaining access, and maintaining access. The report structure reflects in detail how the attacks were carried out and what the SIEM detected during these attacks. The analysis was carried out without finetuning alerts and as such reflects an out of the box install of OSSIM.

The mitigation techniques mentioned if implemented would create a more refined analysis tool. This lab setup does not reflect a small business network layout which would incorporate more users, servers, routers, printers, and services. A large amount of traffic was generated with just one simple machine so one can only imagine the volume of data that would be generated in even a very small network.

Within the scope of a pen test the final phase is analysis and reporting and in this way this report is indicative in part of what would be provided to the client albeit without the full description of the attack. For a pen test report, it merely a matter of identifying the vulnerability and where it exists and a suggested mitigation, the final say on whether to carry out the suggested mitigation lies with client management.

# References

[1]Slideteam.net. 2021. [online] Available at: <https://www.slideteam.net/media/catalog/product/cache/960x720/f/i/five\_stages\_process\_of\_penetration\_testing\_slide01.jpg> [Accessed 9 January 2021].

[2] Rapid7. 2021. *Tomcat Application Manager Login Utility*. [online] Available at: <https://www.rapid7.com/db/modules/auxiliary/scanner/http/tomcat\_mgr\_login/> [Accessed 9 January 2021].

[2] Rapid7. 2021. *VSFTPD V2.3.4 Backdoor Command Execution*. [online] Available at: <https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd\_234\_backdoor/> [Accessed 9 January 2021].

[4] Drd\_. 2021. *How To Hack Apache Tomcat Via Malicious WAR File Upload*. [online] WonderHowTo. Available at: <https://null-byte.wonderhowto.com/how-to/hack-apache-tomcat-via-malicious-war-file-upload-0202593/> [Accessed 9 January 2021].

[5] Response, T., OSSIM, A., Cybersecurity, A., Response, T. and OSSIM, A., 2021. *OSSIM: The Open Source SIEM | Alienvault*. [online] Cybersecurity.att.com. Available at: <https://cybersecurity.att.com/products/ossim?utm\_source=google&utm\_medium=cpc&utm\_term=kwd-343983558916&utm\_campaign=10688982870&source=EBPS0000000PSM00P&WT.srch=1&wtExtndSource=ACS&wtpdsrchprg=AT%2526T%2520ABS&wtpdsrchgp=ABS\_SEARCH&wtPaidSearchTerm=%2Bossim%20%2Balienvault&wtpdsrchpcmt=%2Bossim%20%2Balienvault&kid=kwd-343983558916&cid=10688982870&TFN=B2B&gclsrc=aw.ds&&gclid=EAIaIQobChMI7frTzrGP7gIVG-3tCh0AmgrpEAAYASAAEgLT4\_D\_BwE&gclsrc=aw.ds> [Accessed 9 January 2021].

# Appendix

## Presentation Link

<https://www.youtube.com/watch?v=VKMIB4iGIzk&feature=youtu.be>

## Nmap Scan

┌──(kali㉿kali)-[~]

└─$ nmap -sV -sC -A 192.168.56.100/24

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 14:11 EST

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.56.102

Host is up (0.0019s latency).

Not shown: 996 filtered ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)

| ssh-hostkey:

|\_ 2048 40:4f:7d:c2:2d:0a:a2:f7:c1:c8:89:b6:ff:94:71:a1 (RSA)

80/tcp open http Apache httpd

|\_http-server-header: Apache

|\_http-title: Did not follow redirect to https://192.168.56.102/

443/tcp open ssl/http Apache httpd

|\_http-server-header: Apache

| http-title: AlienVault OSSIM

|\_Requested resource was session/login.php

| ssl-cert: Subject: commonName=alienvault

| Subject Alternative Name: email:system@alienvault.com

| Not valid before: 2021-01-06T23:21:17

|\_Not valid after: 2031-01-04T23:21:17

|\_ssl-date: TLS randomness does not represent time

| tls-alpn:

|\_ http/1.1

514/tcp open shell?

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Nmap scan report for 192.168.56.103

Host is up (0.0023s latency).

Not shown: 977 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.56.104

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

|\_ssl-date: 2021-01-07T19:15:06+00:00; 0s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|\_ bind.version: 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

|\_http-title: Metasploitable2 - Linux

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 49843/tcp mountd

| 100005 1,2,3 57157/udp mountd

| 100021 1,3,4 44068/udp nlockmgr

| 100021 1,3,4 55932/tcp nlockmgr

| 100024 1 42770/udp status

|\_ 100024 1 59606/tcp status

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login OpenBSD or Solaris rlogind

514/tcp open shell Netkit rshd

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

| mysql-info:

| Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 20

| Capabilities flags: 43564

| Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew

| Status: Autocommit

|\_ Salt: 7vpQ!OLl^rE>F(1]d\!,

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

|\_ssl-date: 2021-01-07T19:15:06+00:00; +1s from scanner time.

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|\_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-favicon: Apache Tomcat

|\_http-server-header: Apache-Coyote/1.1

|\_http-title: Apache Tomcat/5.5

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 1h15m01s, deviation: 2h30m01s, median: 0s

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2021-01-07T14:14:53-05:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-time: Protocol negotiation failed (SMB2)

Nmap scan report for 192.168.56.104

Host is up (0.000062s latency).

All 1000 scanned ports on 192.168.56.104 are closed

Nmap scan report for 192.168.56.106

Host is up (0.0020s latency).

Not shown: 996 filtered ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)

| ssh-hostkey:

|\_ 2048 40:4f:7d:c2:2d:0a:a2:f7:c1:c8:89:b6:ff:94:71:a1 (RSA)

80/tcp open http Apache httpd

|\_http-server-header: Apache

|\_http-title: Did not follow redirect to https://192.168.56.106/

443/tcp open ssl/http Apache httpd

|\_http-server-header: Apache

| http-title: AlienVault OSSIM

|\_Requested resource was session/login.php

| ssl-cert: Subject: commonName=alienvault

| Subject Alternative Name: email:system@alienvault.com

| Not valid before: 2021-01-06T23:21:17

|\_Not valid after: 2031-01-04T23:21:17

|\_ssl-date: TLS randomness does not represent time

| tls-alpn:

|\_ http/1.1

514/tcp open shell?

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Post-scan script results:

| ssh-hostkey: Possible duplicate hosts

| Key 2048 40:4f:7d:c2:2d:0a:a2:f7:c1:c8:89:b6:ff:94:71:a1 (RSA) used by:

| 192.168.56.102

|\_ 192.168.56.106

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (4 hosts up) scanned in 217.35 seconds

## Nmap Scan of 192.168.56.103

┌──(kali㉿kali)-[~]

└─$ nmap -sV -p- 192.168.56.103

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-08 15:23 EST

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 96.67% done; ETC: 15:24 (0:00:02 remaining)

Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 96.67% done; ETC: 15:25 (0:00:02 remaining)

Nmap scan report for 192.168.56.103

Host is up (0.0012s latency).

Not shown: 65505 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

53/tcp open domain ISC BIND 9.4.2

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login

514/tcp open shell Netkit rshd

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

6697/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

41936/tcp open mountd 1-3 (RPC #100005)

48377/tcp open nlockmgr 1-4 (RPC #100021)

52104/tcp open status 1 (RPC #100024)

52505/tcp open java-rmi GNU Classpath grmiregistry

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 130.90 seconds

## Nikto Scan

┌──(kali㉿kali)-[~]

└─$ nikto -h 192.168.56.103

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.56.103

+ Target Hostname: 192.168.56.103

+ Target Port: 80

+ Start Time: 2021-01-08 11:42:02 (GMT-5)

---------------------------------------------------------------------------

+ Server: Apache/2.2.8 (Ubuntu) DAV/2

+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Uncommon header 'tcn' found, with contents: list

+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php

+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ /phpinfo.php: Output from the phpinfo() function was found.

+ OSVDB-3268: /doc/: Directory indexing found.

+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.

+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008

+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3268: /test/: Directory indexing found.

+ OSVDB-3092: /test/: This might be interesting...

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /phpMyAdmin/: phpMyAdmin directory found

+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host

+ End Time: 2021-01-08 11:42:17 (GMT-5) (15 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested