Proyecto de Reconocimiento en Pentesting de Vulnerabilidades

28 de Abril del 2025

VISIÓN GENERAL

En este proyecto haremos una serie de pruebas para encontrar posibles vulnerabilidades así como acciones recomendadas para reforzar la seguridad informática de la empresa.

ESPECIFICACIONES

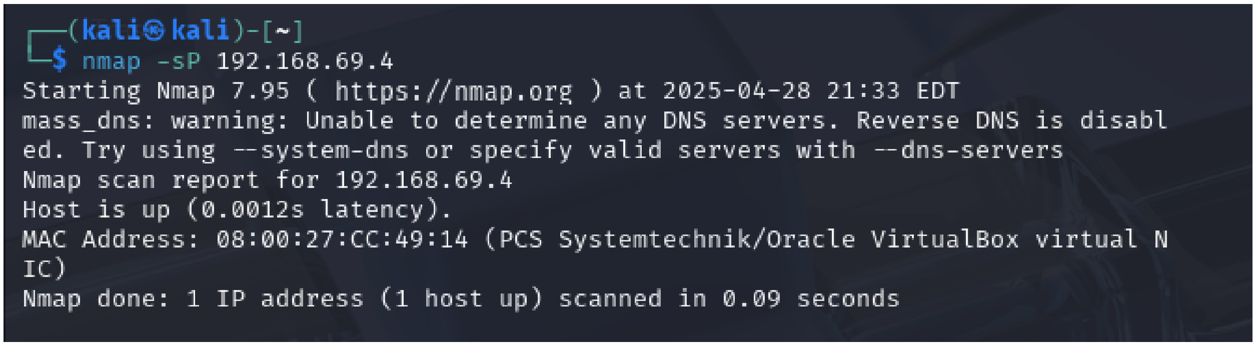
Haremos pruebas a través de Kali linux, para encontrar vulnerabilidades utilizando la herramienta NMAPS.

Escaneo y sus resultados.

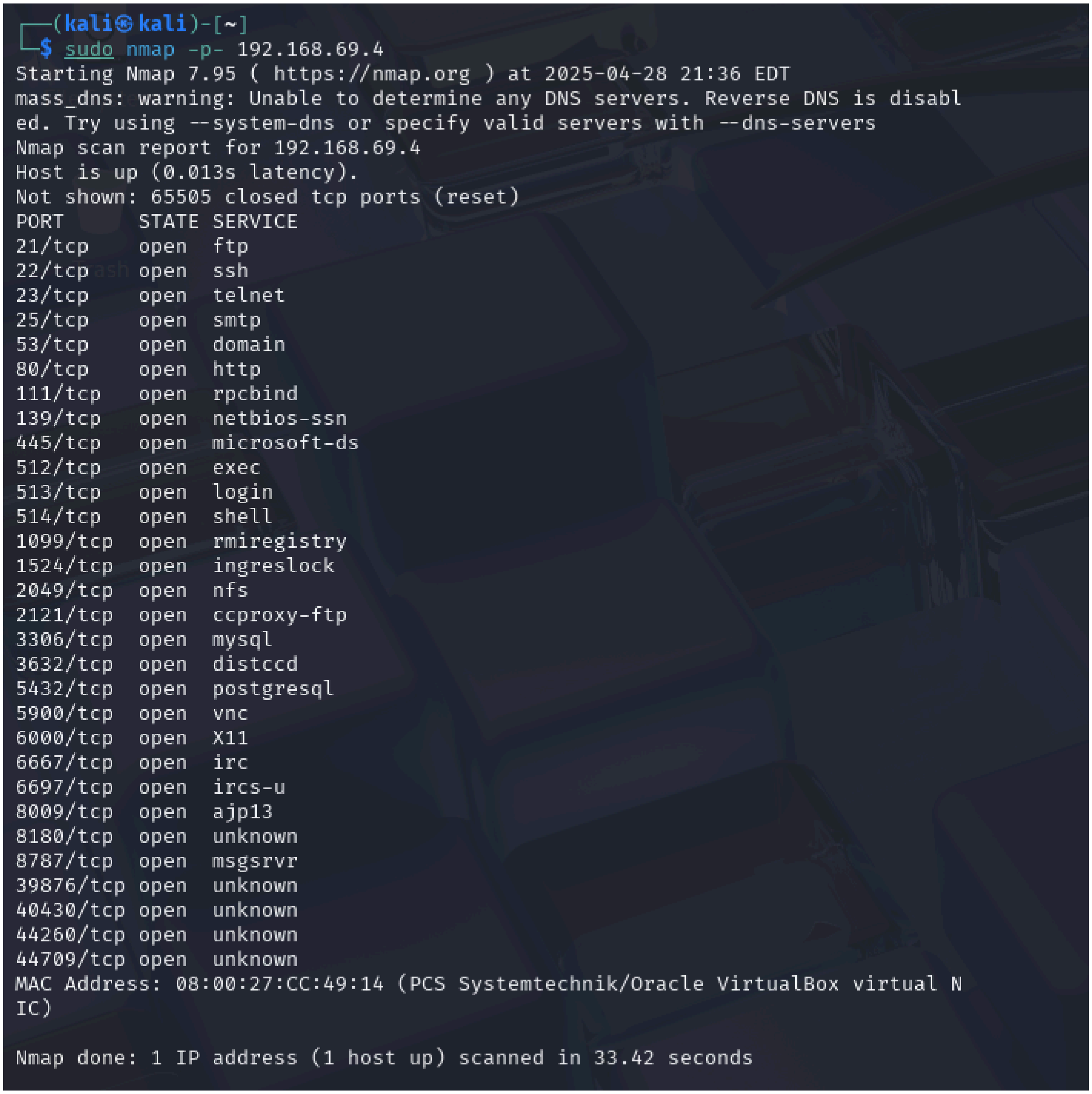
utilizando las lineas de comando:

1. Ping y descubrimiento de puertos: nmap -sP <direccion ip>
2. Escaneo de servicios y versiones: nmap -sV <direccion ip>
3. Deteccion del sistema operativo: nmap -O <direccion ip>
4. Informe de las anteriores, escaneo de script y traceroute: sudo nmap -A <direccion ip>
5. Para enumerar los puertos vulnerables y servicios: sudo nmap -p- <direccion ip>
6. Para detección de vulnerabilidades: sudo nmap –script vuln <direccion ip>

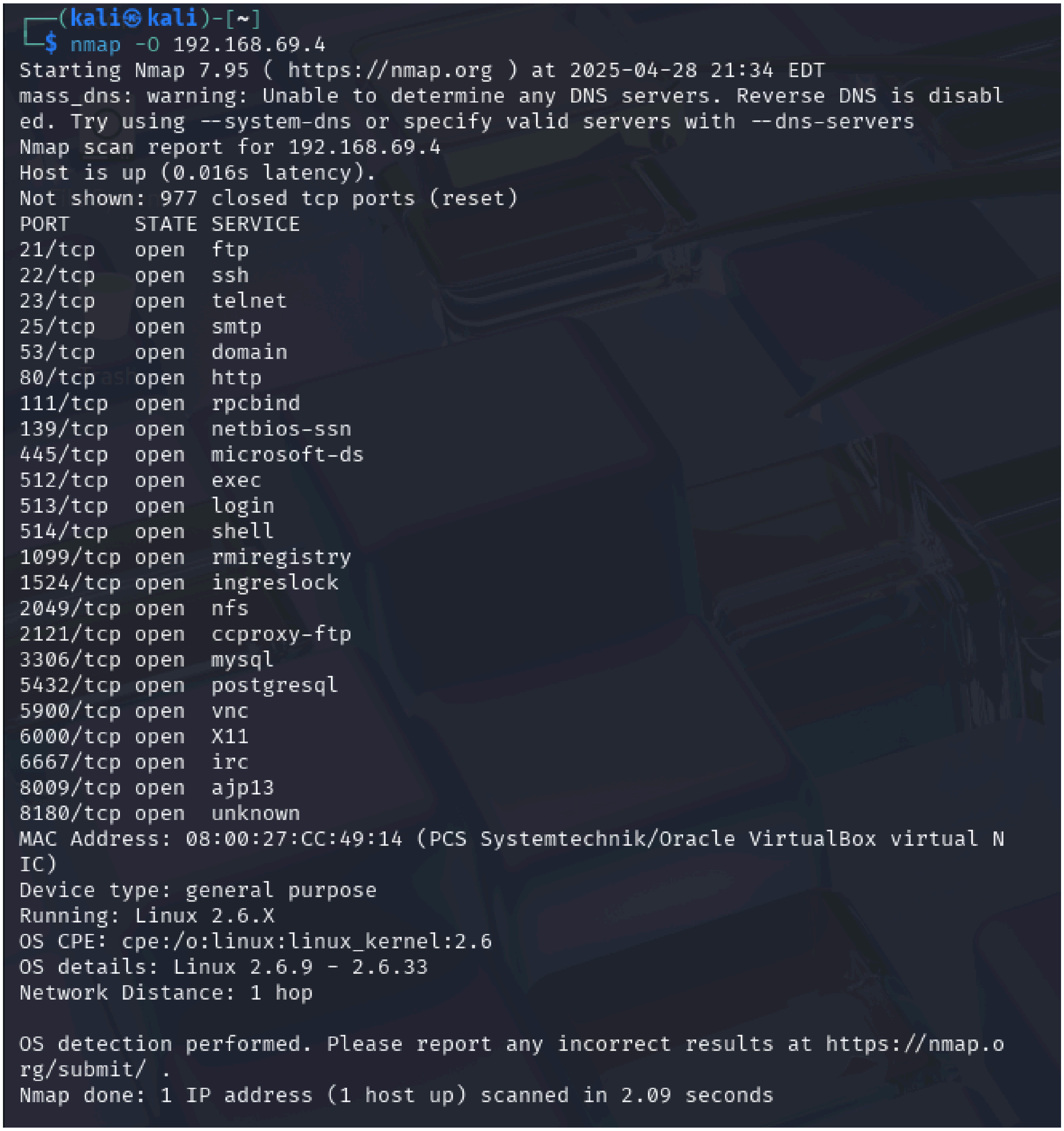
Imagenes de los resultados:



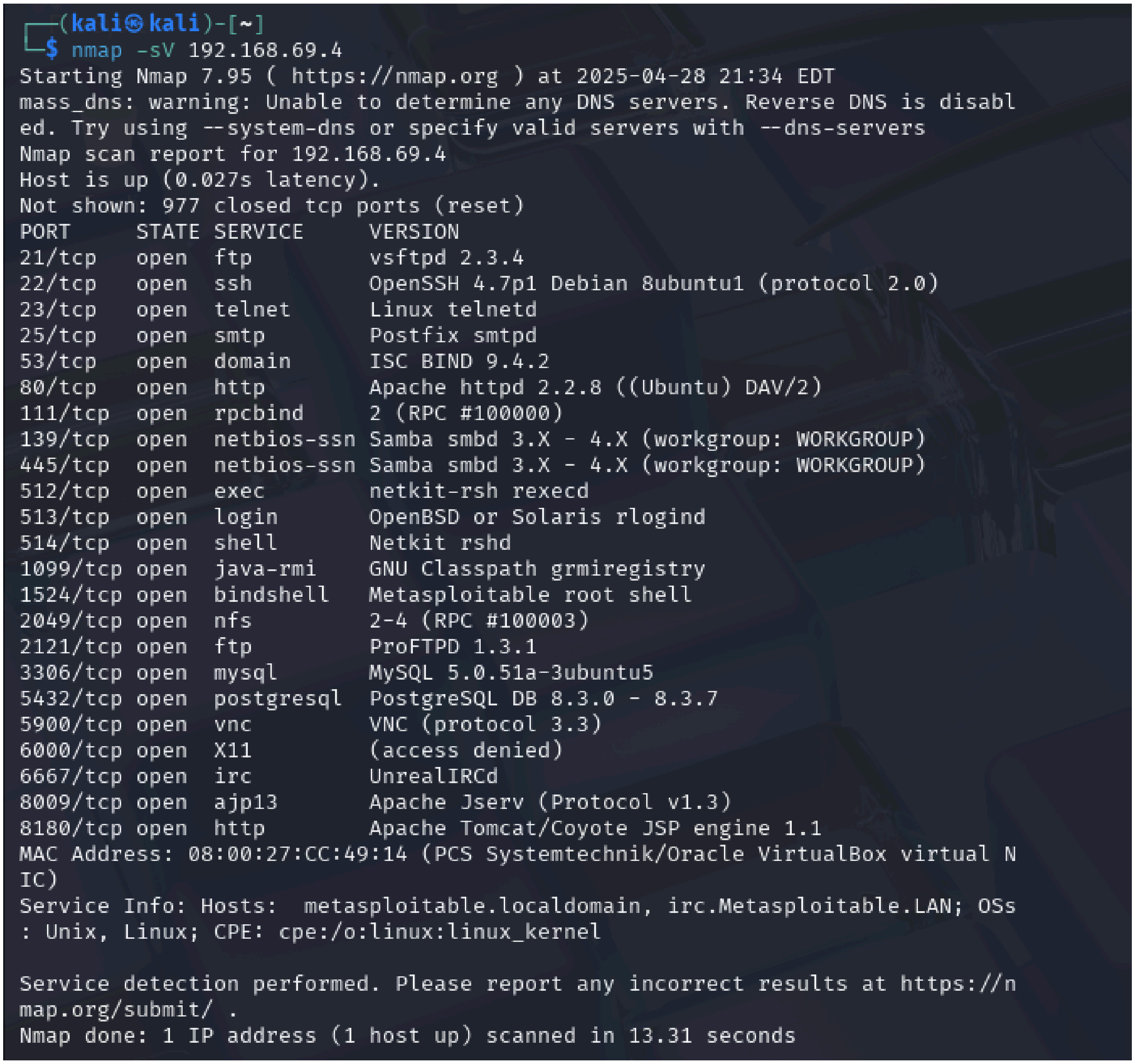
```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.69.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 21:33 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.69.4
Host is up (0.0012s latency).
MAC Address: 08:00:27:CC:49:14 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```



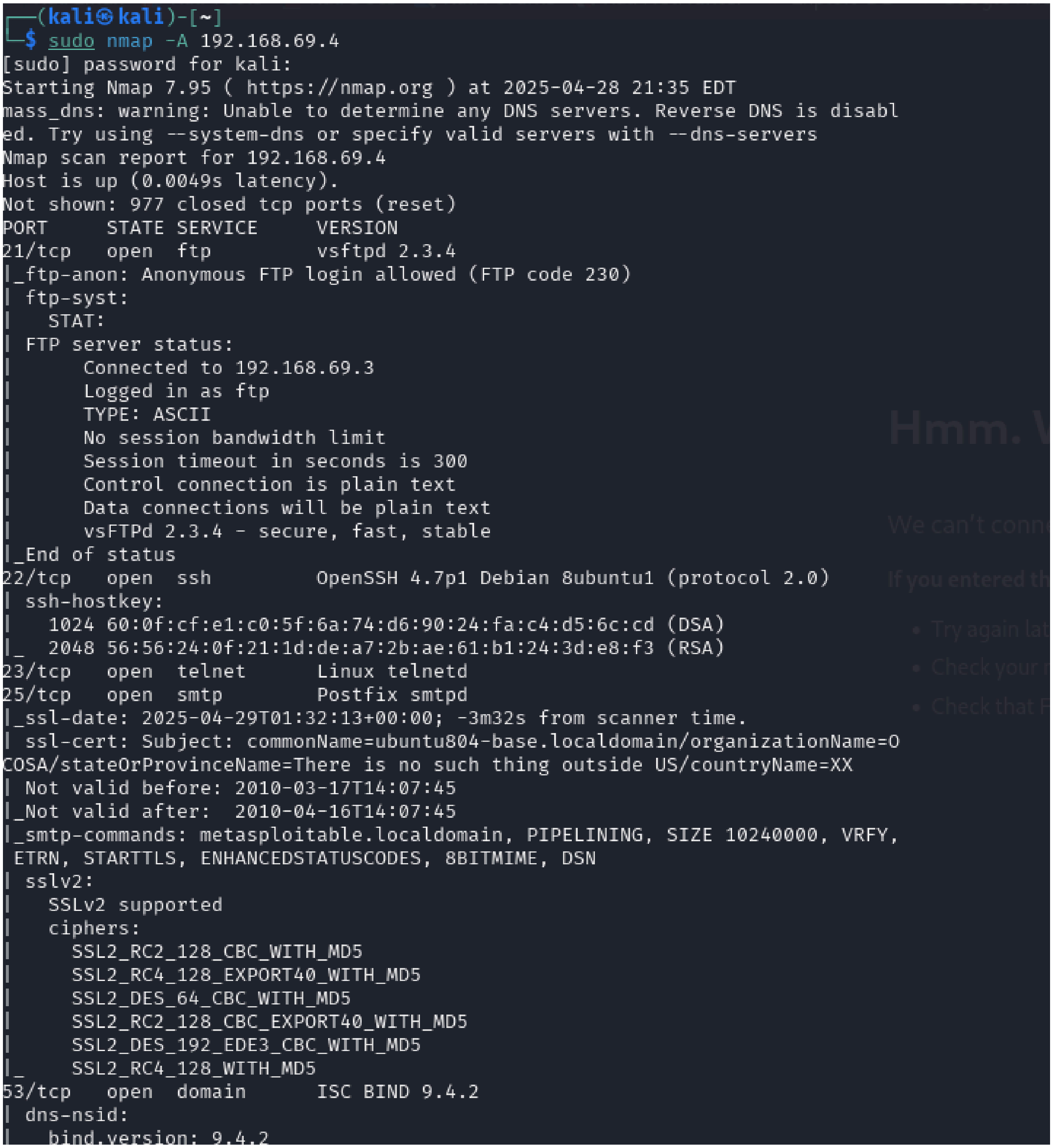
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.69.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 21:36 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.69.4
Host is up (0.013s latency).
Not shown: 65505 closed tcp ports (reset)
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
39876/tcp open  unknown
40430/tcp open  unknown
44260/tcp open  unknown
44709/tcp open  unknown
MAC Address: 08:00:27:CC:49:14 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 33.42 seconds
```



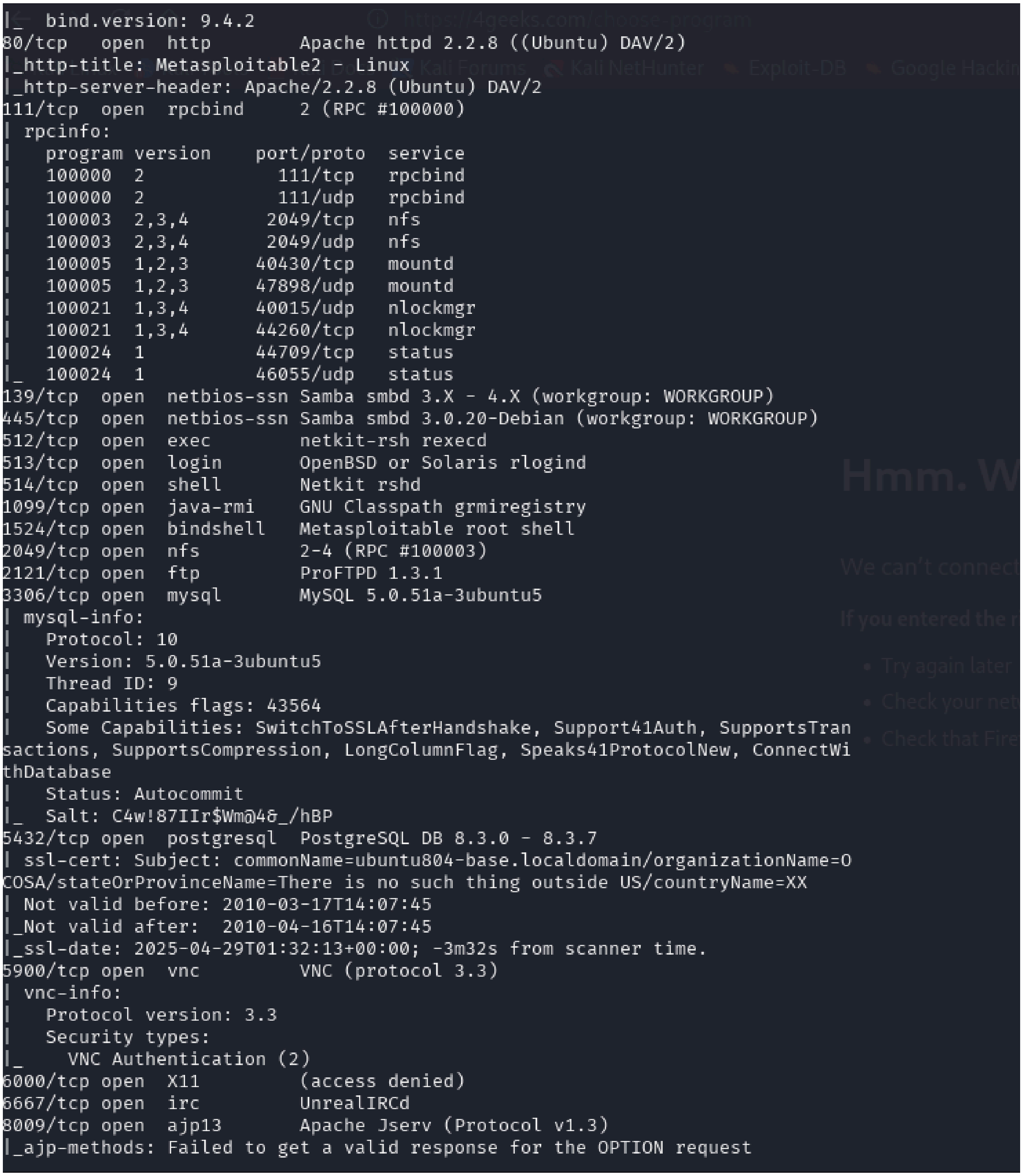
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.69.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 21:34 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.69.4
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
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: 08:00:27:CC:49:14 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```



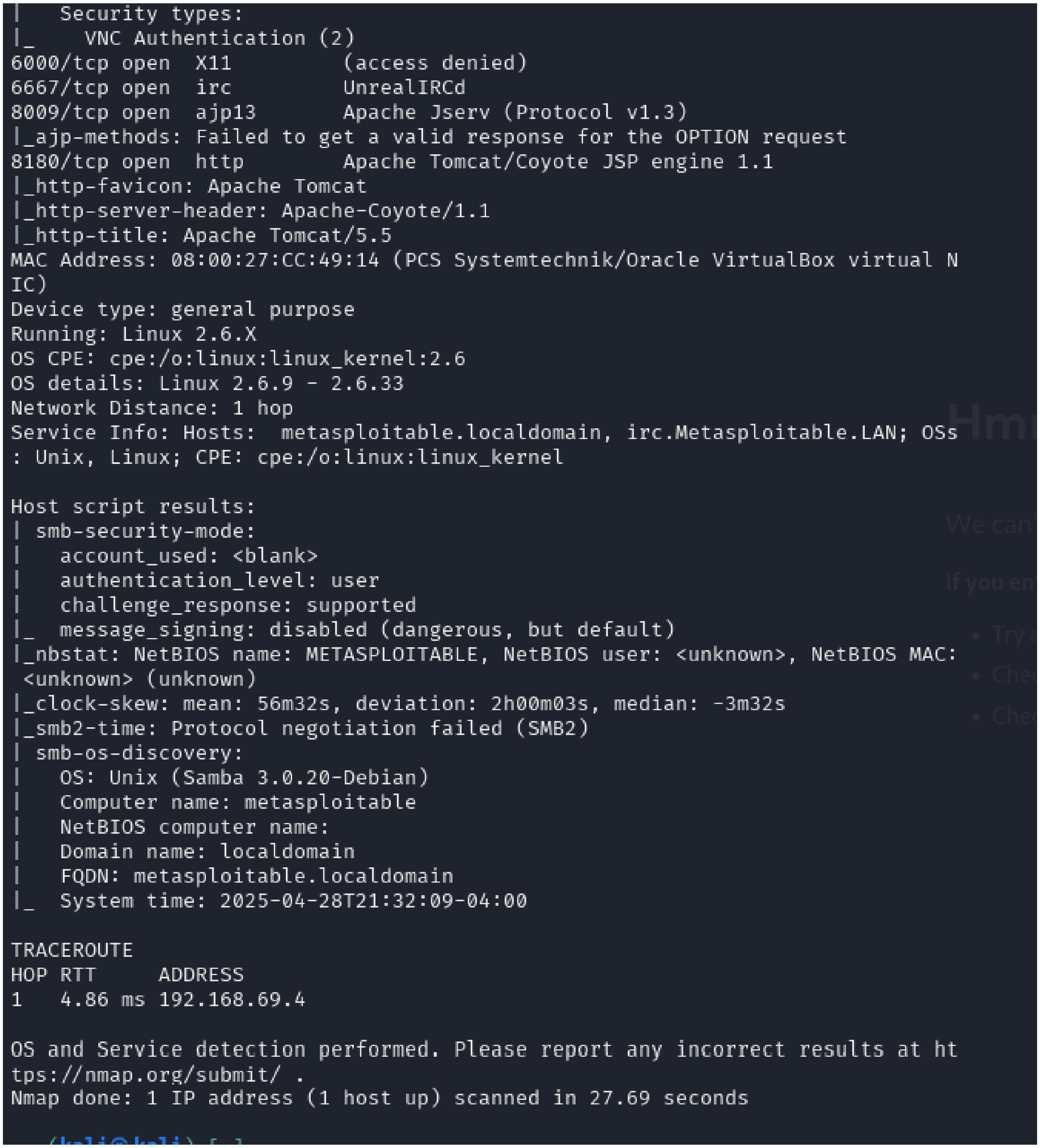
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.69.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 21:34 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.69.4
Host is up (0.027s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CC:49:14 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```



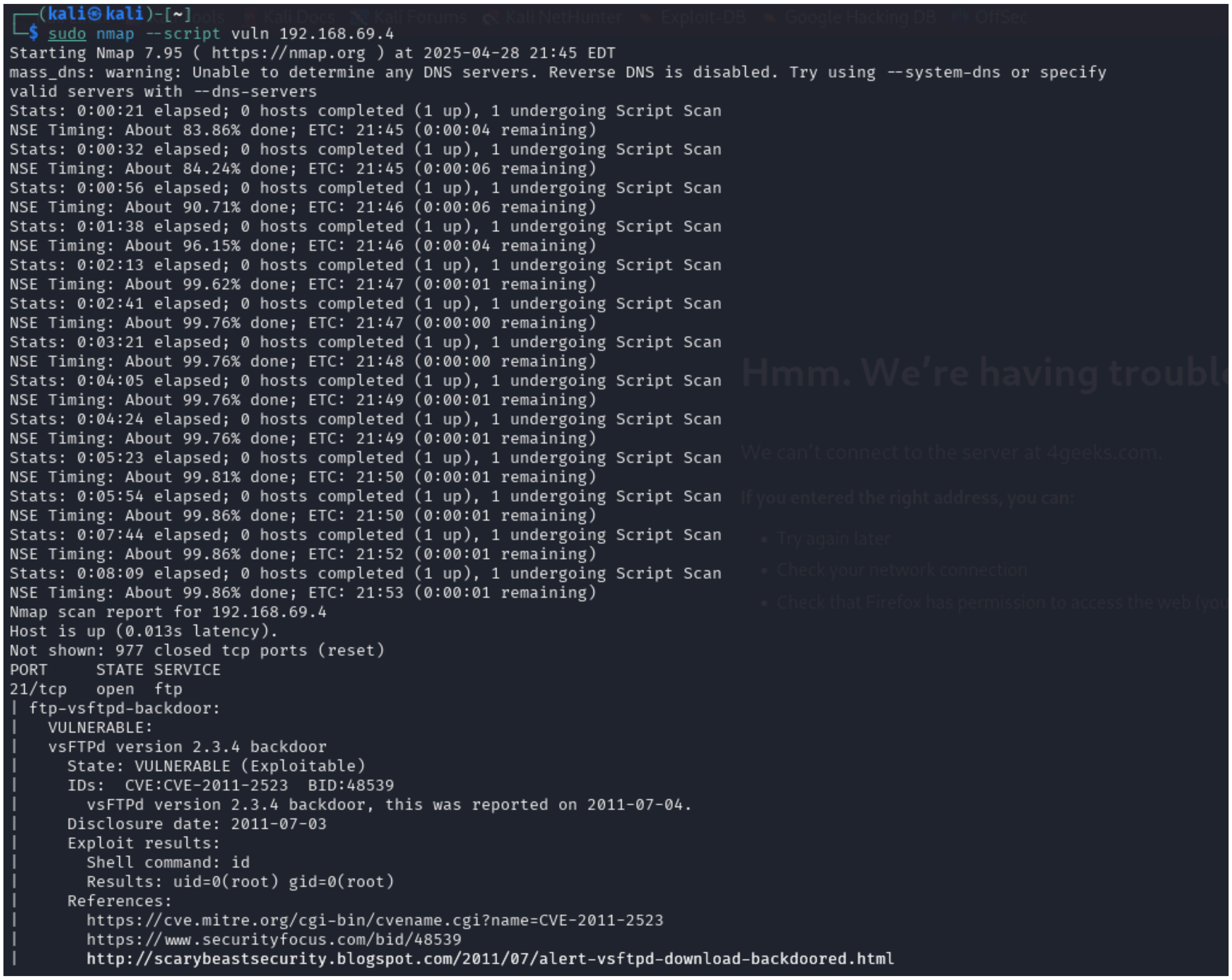
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.69.4
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 21:35 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.69.4
Host is up (0.0049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.69.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-04-29T01:32:13+00:00; -3m32s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
```



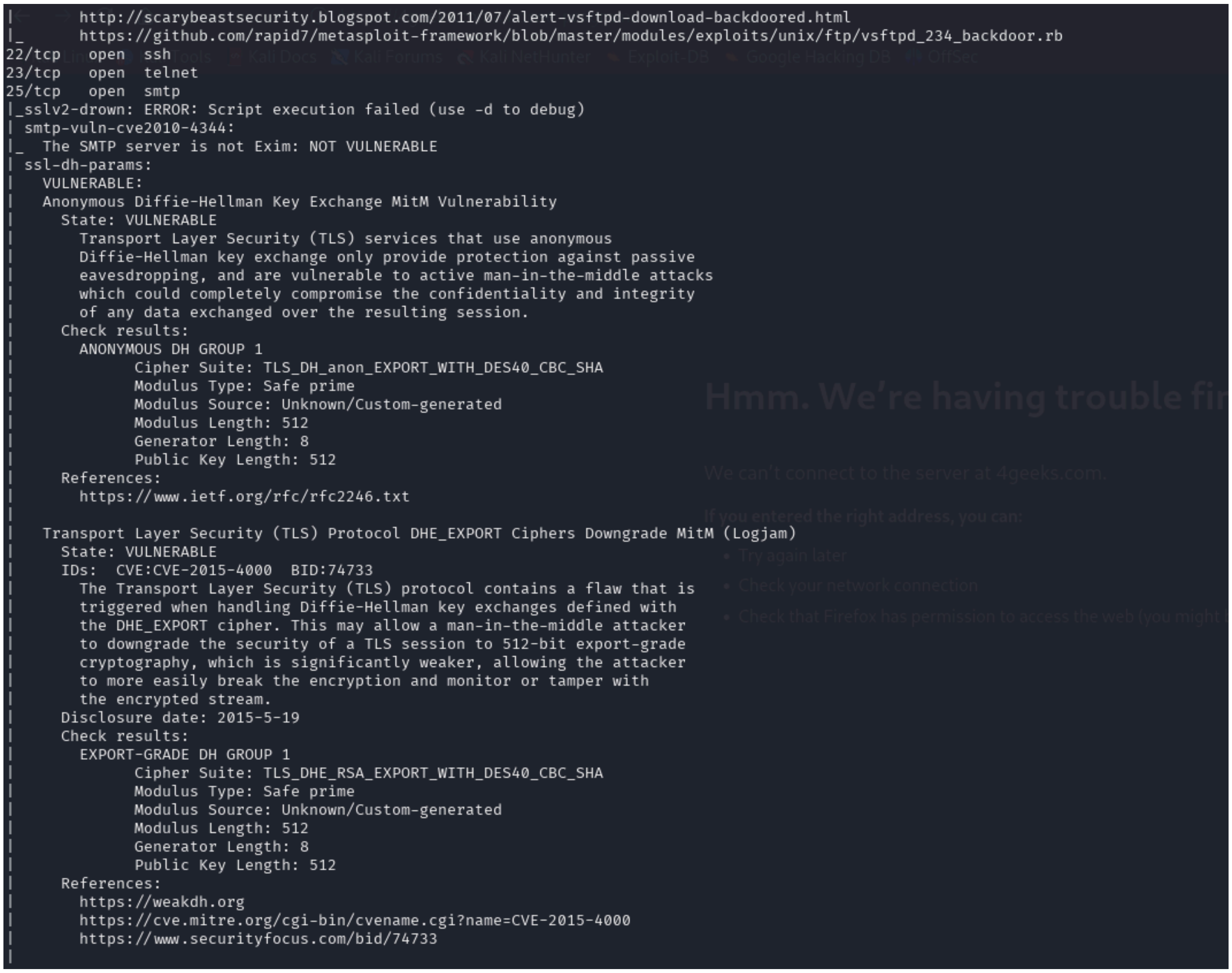
```
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            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      40430/tcp   mountd
|   100005  1,2,3      47898/udp   mountd
|   100021  1,3,4      40015/udp   nlockmgr
|   100021  1,3,4      44260/tcp   nlockmgr
|   100024  1          44709/tcp   status
|_  100024  1          46055/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, SupportsTran
sactions, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, ConnectWi
thDatabase
|   Status: Autocommit
|_  Salt: C4w!87IIr$Wm@4&_/hBP
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-04-29T01:32:13+00:00; -3m32s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
```



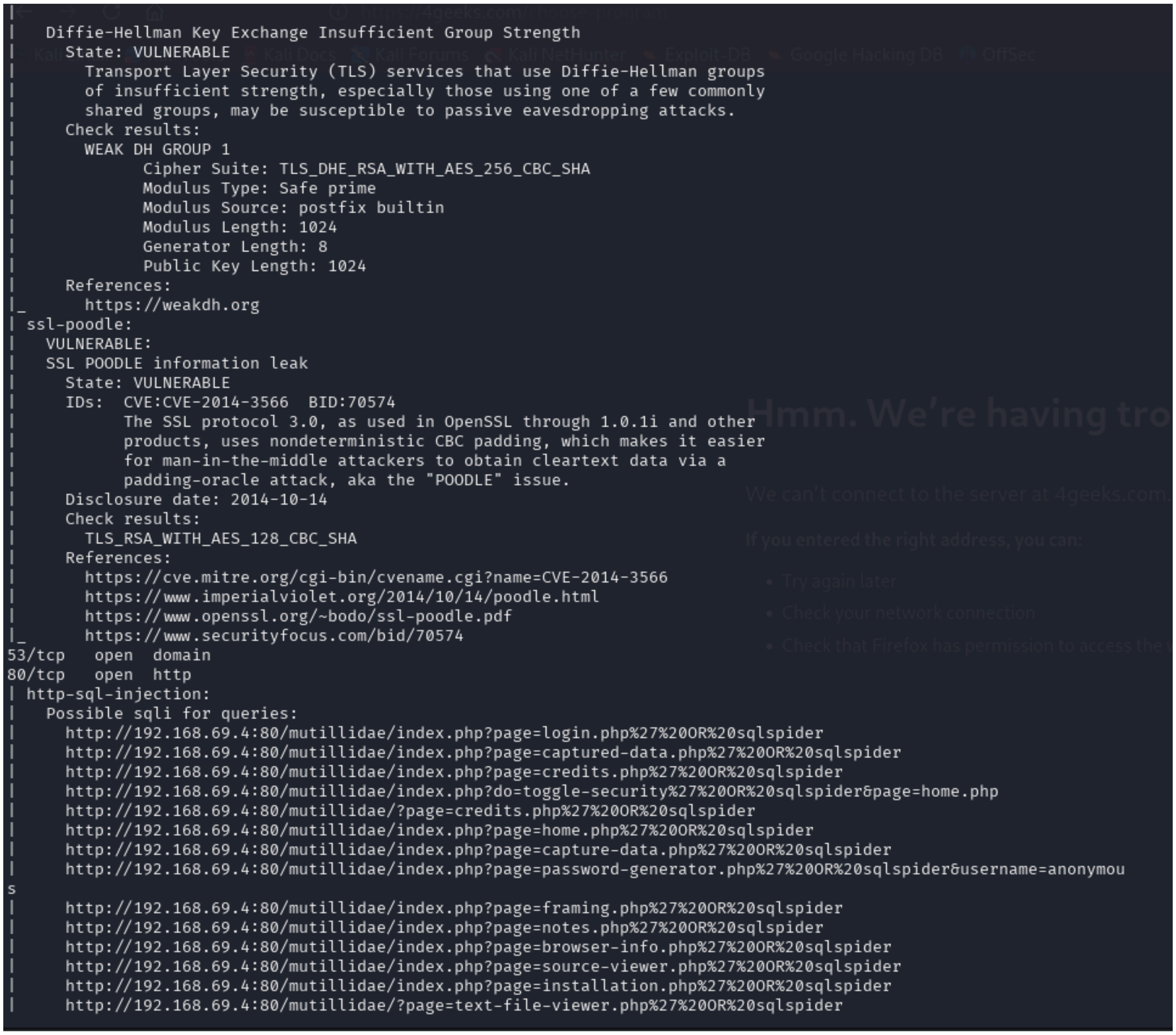
```
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:CC:49:14 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
 <unknown> (unknown)
|_clock-skew: mean: 56m32s, deviation: 2h00m03s, median: -3m32s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-04-28T21:32:09-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   4.86 ms 192.168.69.4

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.69 seconds
```



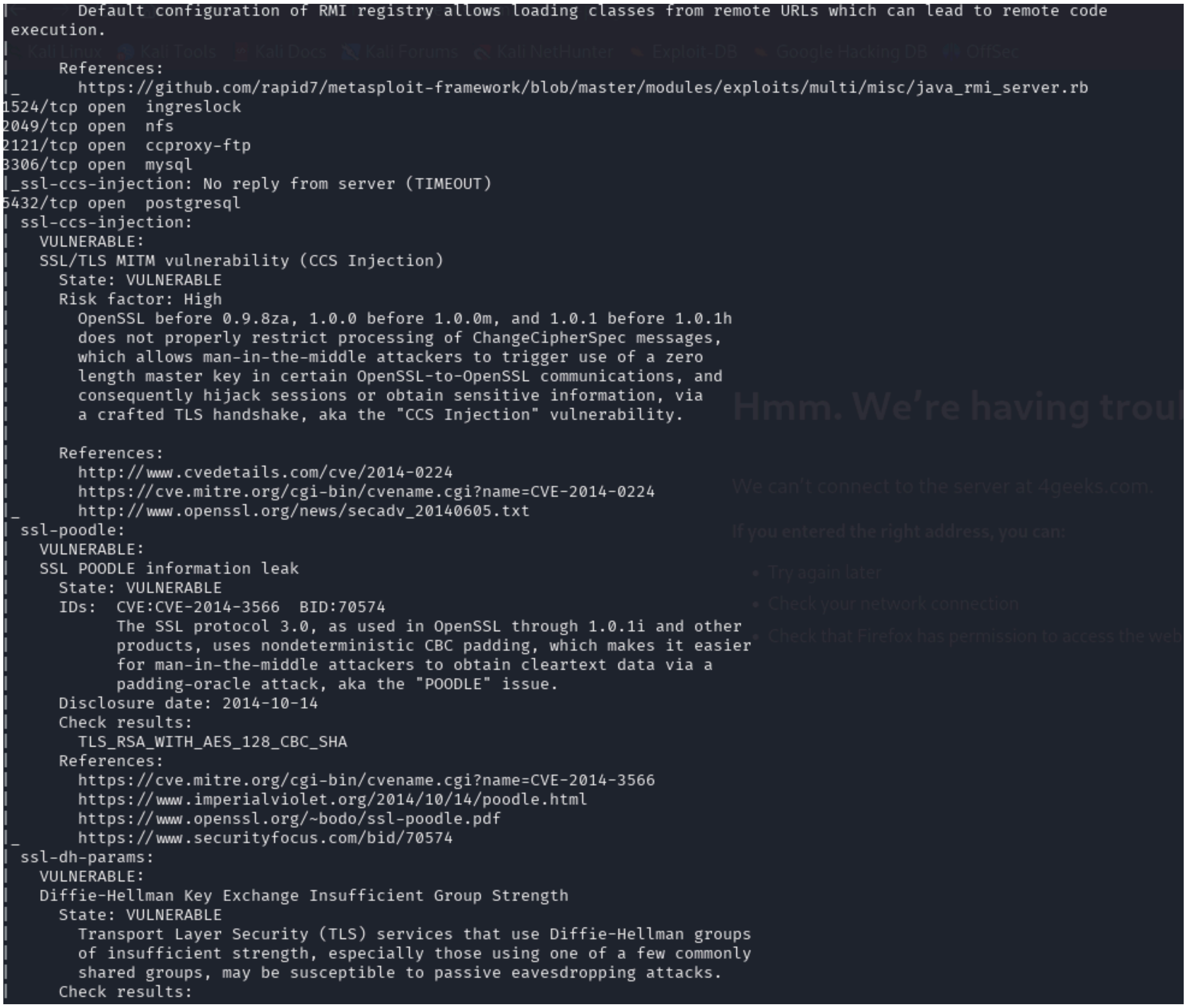
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln 192.168.69.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-28 21:45 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
valid servers with --dns-servers
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 83.86% done; ETC: 21:45 (0:00:04 remaining)
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.24% done; ETC: 21:45 (0:00:06 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.71% done; ETC: 21:46 (0:00:06 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.15% done; ETC: 21:46 (0:00:04 remaining)
Stats: 0:02:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.62% done; ETC: 21:47 (0:00:01 remaining)
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 21:47 (0:00:00 remaining)
Stats: 0:03:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 21:48 (0:00:00 remaining)
Stats: 0:04:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 21:49 (0:00:01 remaining)
Stats: 0:04:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 21:49 (0:00:01 remaining)
Stats: 0:05:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 21:50 (0:00:01 remaining)
Stats: 0:05:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 21:50 (0:00:01 remaining)
Stats: 0:07:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 21:52 (0:00:01 remaining)
Stats: 0:08:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.86% done; ETC: 21:53 (0:00:01 remaining)
Nmap scan report for 192.168.69.4
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```



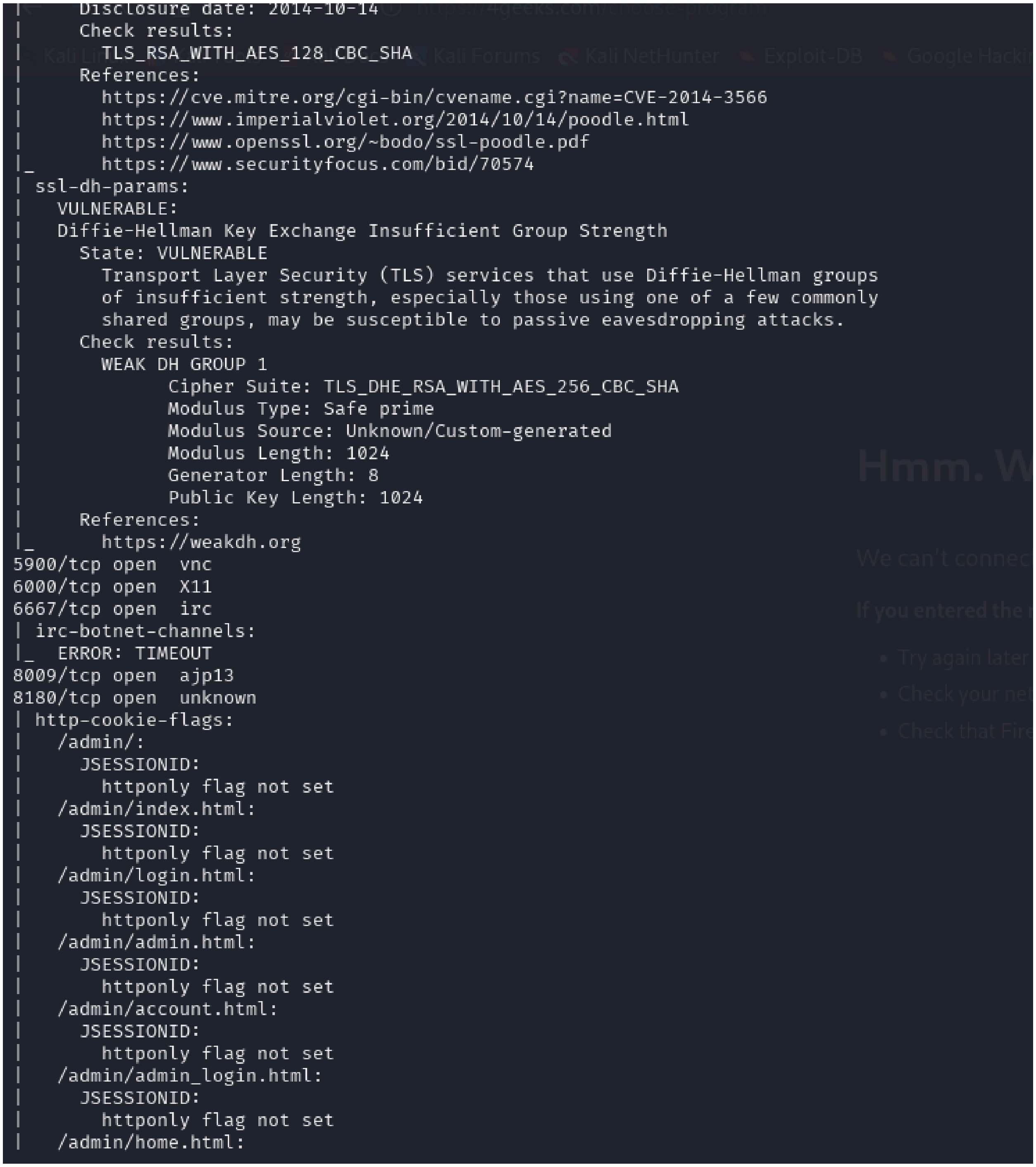
```
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://weakdh.org
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|       https://www.securityfocus.com/bid/74733
|
```



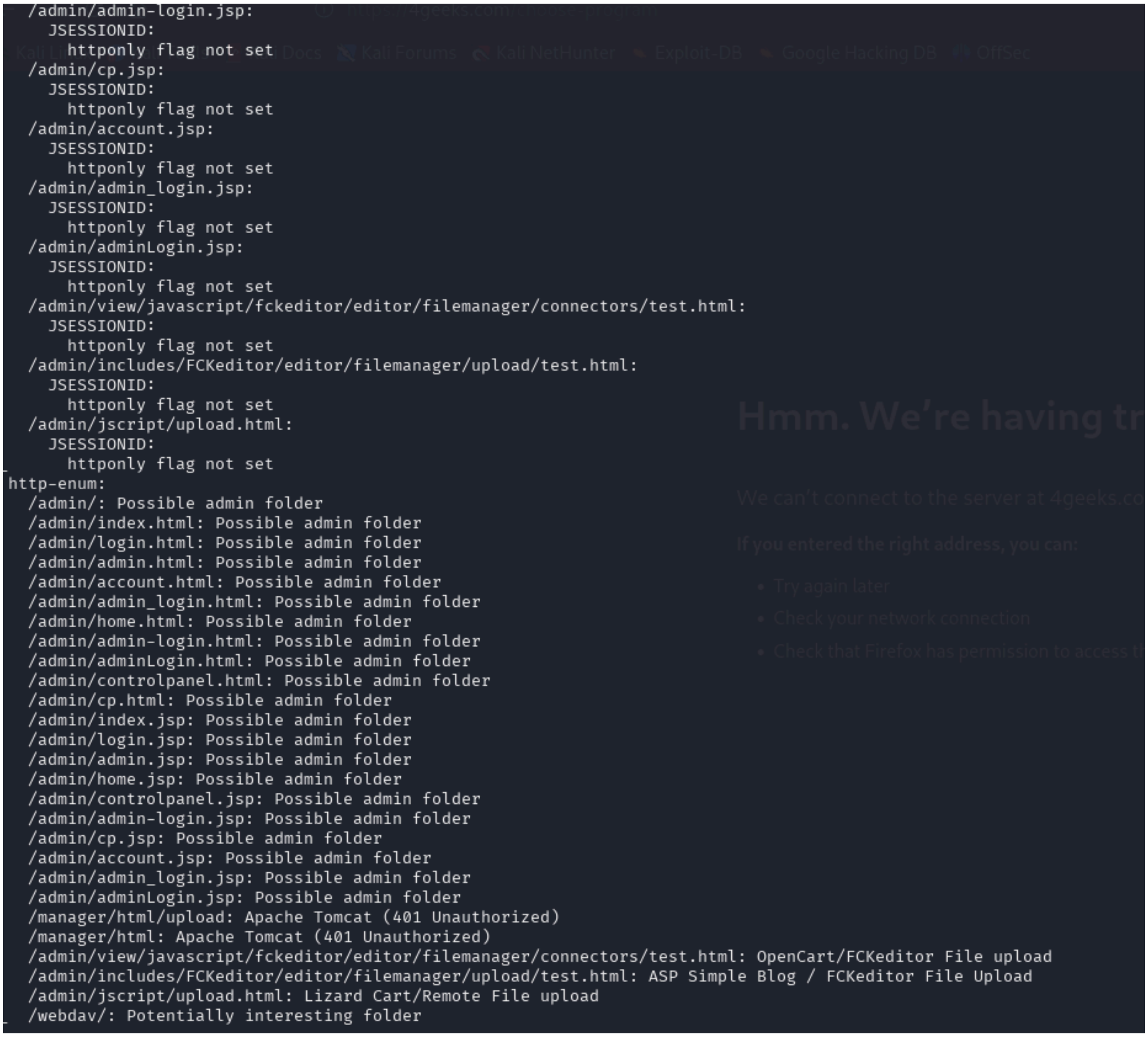
```
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
53/tcp   open  domain
80/tcp   open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.69.4:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|     http://192.168.69.4:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymou
s
|     http://192.168.69.4:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.69.4:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
```



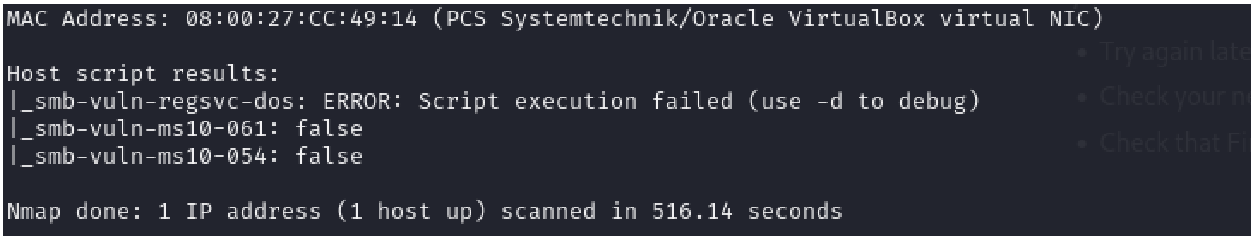
```
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code
 execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.cvedetails.com/cve/2014-0224
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
```



```
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
| irc-botnet-channels:
|_  ERROR: TIMEOUT
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
```



```
  /admin/admin-login.jsp:
    JSESSIONID:
      httponly flag not set
  /admin/cp.jsp:
    JSESSIONID:
      httponly flag not set
  /admin/account.jsp:
    JSESSIONID:
      httponly flag not set
  /admin/admin_login.jsp:
    JSESSIONID:
      httponly flag not set
  /admin/adminLogin.jsp:
    JSESSIONID:
      httponly flag not set
  /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
    JSESSIONID:
      httponly flag not set
  /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
    JSESSIONID:
      httponly flag not set
  /admin/jscript/upload.html:
    JSESSIONID:
      httponly flag not set
http-enum:
  /admin/: Possible admin folder
  /admin/index.html: Possible admin folder
  /admin/login.html: Possible admin folder
  /admin/admin.html: Possible admin folder
  /admin/account.html: Possible admin folder
  /admin/admin_login.html: Possible admin folder
  /admin/home.html: Possible admin folder
  /admin/admin-login.html: Possible admin folder
  /admin/adminLogin.html: Possible admin folder
  /admin/controlpanel.html: Possible admin folder
  /admin/cp.html: Possible admin folder
  /admin/index.jsp: Possible admin folder
  /admin/login.jsp: Possible admin folder
  /admin/admin.jsp: Possible admin folder
  /admin/home.jsp: Possible admin folder
  /admin/controlpanel.jsp: Possible admin folder
  /admin/admin-login.jsp: Possible admin folder
  /admin/cp.jsp: Possible admin folder
  /admin/account.jsp: Possible admin folder
  /admin/admin_login.jsp: Possible admin folder
  /admin/adminLogin.jsp: Possible admin folder
  /manager/html/upload: Apache Tomcat (401 Unauthorized)
  /manager/html: Apache Tomcat (401 Unauthorized)
  /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
  /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
  /admin/jscript/upload.html: Lizard Cart/Remote File upload
  /webdav/: Potentially interesting folder
```



```
MAC Address: 08:00:27:CC:49:14 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 516.14 seconds
```

Vulnerabilidades y puertos escaneados.

Puerto	Servicio	Versión	Vulnerabilidades	Referencias
22	SSH	OpenSSH 9.2p1 Debian 2+deb12u5	Múltiples CVEs críticos como CVE-2023-38408, CVE-2023-28531	https://vulners.com/cve/CVE-2023-38408 https://vulners.com/cve/CVE-2023-28531
80	HTTP	Apache 2.4.62 (Debian)		
443	HTTPS	Apache 2.4.62 con SSL		