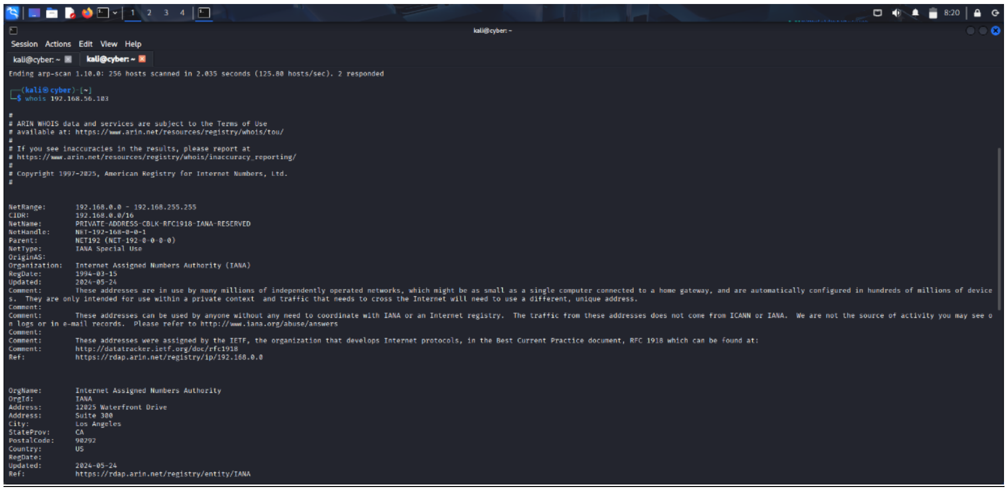
Task 2 — Network Security & Scanning

Intern Name: **Nitesh Sharma** Date: **30/10/2025**

1. Reconnaissance :-

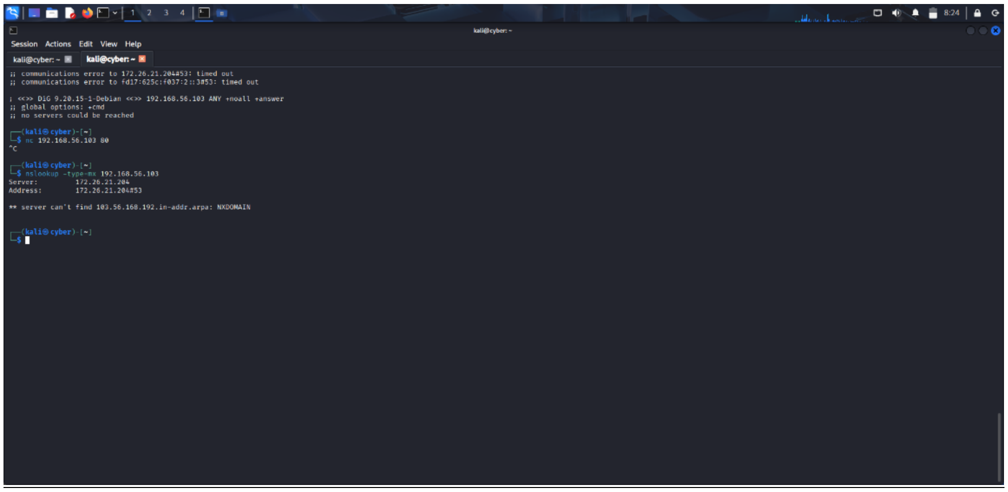
A) Passive Recon :

- Whois



```
Ending arp-scan 1.10.0: 256 hosts scanned in 2.035 seconds (125.80 hosts/sec). 2 responded

┌──(kali㉿cyber)-[~]
└─$ whois 192.168.56.103

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2024-05-24
Comment:        These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of device
s.  They are only intended for use within a private context  and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry.  The traffic from these addresses does not come from ICANN or IANA.  We are not the source of activity you may see o
n logs or in e-mail records.  Please refer to http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2024-05-24
Ref:            https://rdap.arin.net/registry/entity/IANA
```

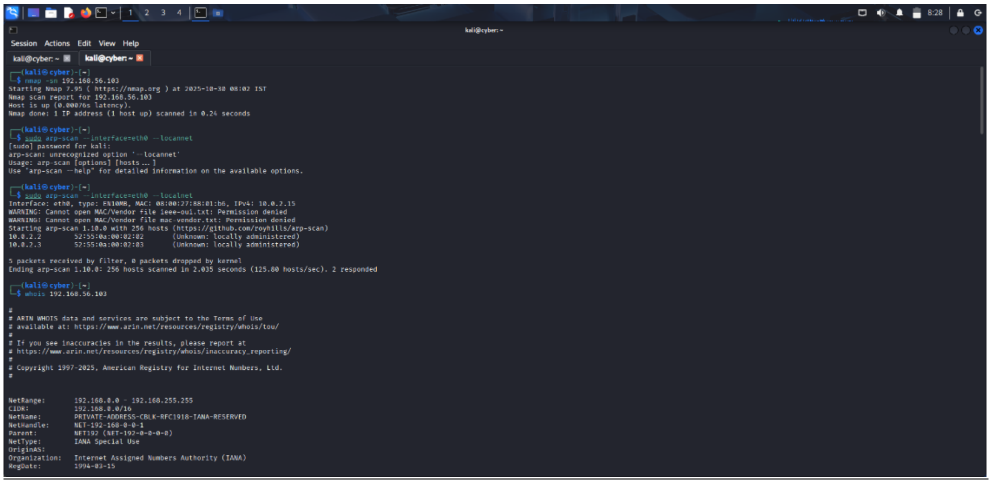
- Nslookup :-



```
;; communications error to 172.26.21.204#53: timed out
;; communications error to fd17:625c:f037:2::3#53: timed out

; <<>> DiG 9.20.15-1-Debian <<>> 192.168.56.103 ANY +noall +answer
;; global options: +cmd
;; no servers could be reached

┌──(kali㉿cyber)-[~]
└─$ nc 192.168.56.103 80
^C

┌──(kali㉿cyber)-[~]
└─$ nslookup -type=mx 192.168.56.103
Server:         172.26.21.204
Address:        172.26.21.204#53

** server can't find 103.56.168.192.in-addr.arpa: NXDOMAIN


┌──(kali㉿cyber)-[~]
└─$ 
```

B) Active recon :-

- Ping Sweep
- Banner Grabbing



```
┌──(kali㉿cyber)-[~]
└─$ nmap -sn 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 08:02 IST
Nmap scan report for 192.168.56.103
Host is up (0.00076s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(kali㉿cyber)-[~]
└─$ sudo arp-scan --interface=eth0 --locannet
[sudo] password for kali:
arp-scan: unrecognized option '--locannet'
Usage: arp-scan [options] [hosts ... ]
Use "arp-scan --help" for detailed information on the available options.

┌──(kali㉿cyber)-[~]
└─$ sudo arp-scan --interface=eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:88:01:b6, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2        52:55:0a:00:02:02       (Unknown: locally administered)
10.0.2.3        52:55:0a:00:02:03       (Unknown: locally administered)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.035 seconds (125.80 hosts/sec). 2 responded

┌──(kali㉿cyber)-[~]
└─$ whois 192.168.56.103

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
```

2. Port & Service Scanning :-

```
┌──(root㉿kali)-[/home/kali]
└─# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=255 time=3.20 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=255 time=4.05 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=255 time=1.68 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=255 time=4.25 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=255 time=3.04 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=255 time=3.81 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=255 time=3.09 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=255 time=5.38 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=255 time=2.52 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=255 time=3.45 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=255 time=3.15 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=255 time=2.57 ms
^C
--- 192.168.56.101 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11072ms
rtt min/avg/max/mdev = 1.677/3.347/5.377/0.910 ms
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 22:34 IST
Nmap scan report for 192.168.56.101
Host is up (0.019s latency).
Not shown: 977 filtered tcp ports (no-response)
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  □etasploi-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

Nmap done: 1 IP address (1 host up) scanned in 4.50 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 22:36 IST
Nmap scan report for 192.168.56.101
```

```
Host is up (0.0044s latency).
Not shown: 996 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 4.62 seconds


┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -v -O 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 22:37 IST
NSE: Loaded 47 scripts for scanning.
Initiating Ping Scan at 22:37
Scanning 192.168.56.101 [4 ports]
Completed Ping Scan at 22:37, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. At 22:37
Completed Parallel DNS resolution of 1 host. At 22:37, 0.02s elapsed
Initiating SYN Stealth Scan at 22:37
Scanning 192.168.56.101 [1000 ports]
Discovered open port 22/tcp on 192.168.56.101
Discovered open port 53/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 5900/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 3306/tcp on 192.168.56.101
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 111/tcp on 192.168.56.101
Discovered open port 6667/tcp on 192.168.56.101
Discovered open port 2121/tcp on 192.168.56.101
Discovered open port 2049/tcp on 192.168.56.101
Discovered open port 512/tcp on 192.168.56.101
Discovered open port 513/tcp on 192.168.56.101
Discovered open port 1524/tcp on 192.168.56.101
Discovered open port 8009/tcp on 192.168.56.101
Discovered open port 5432/tcp on 192.168.56.101
Discovered open port 514/tcp on 192.168.56.101
Discovered open port 1099/tcp on 192.168.56.101
Discovered open port 8180/tcp on 192.168.56.101
Discovered open port 6000/tcp on 192.168.56.101
Completed SYN Stealth Scan at 22:37, 4.45s elapsed (1000 total ports)
Initiating Service scan at 22:37
Scanning 23 services on 192.168.56.101
Completed Service scan at 22:37, 11.46s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.101
Retrying OS detection (try #2) against 192.168.56.101
NSE: Script scanning 192.168.56.101.
Initiating NSE at 22:37
Completed NSE at 22:37, 0.29s elapsed
Initiating NSE at 22:37
Completed NSE at 22:37, 0.12s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.0022s latency).
Not shown: 977 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded
(94%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp
cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210
voice gateway (94%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=19 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; Oss:
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.88 seconds
        Raw packets sent: 2032 (93.232KB) | Rcvd: 706 (29.752KB)

┌──(root㉿kali)-[/home/kali]
└─# nmap –script vuln 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 22:42 IST


┌──(root㉿kali)-[/home/kali]
└─# nmap –script vuln 192.168.56.101 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 22:44 IST
NSE: Loaded 105 scripts for scanning.
```

```
NSE: Script Pre-scanning.
Initiating NSE at 22:44
Completed NSE at 22:44, 10.02s elapsed
Initiating NSE at 22:44
Completed NSE at 22:44, 0.00s elapsed
Initiating Ping Scan at 22:44
Scanning 192.168.56.101 [4 ports]
Completed Ping Scan at 22:44, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. At 22:44
Completed Parallel DNS resolution of 1 host. At 22:44, 0.01s elapsed
Initiating SYN Stealth Scan at 22:44
Scanning 192.168.56.101 [1000 ports]
Discovered open port 111/tcp on 192.168.56.101
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Discovered open port 3306/tcp on 192.168.56.101
Discovered open port 53/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 5900/tcp on 192.168.56.101
Discovered open port 8009/tcp on 192.168.56.101
Discovered open port 514/tcp on 192.168.56.101
Discovered open port 2121/tcp on 192.168.56.101
Discovered open port 1099/tcp on 192.168.56.101
Discovered open port 2049/tcp on 192.168.56.101
Discovered open port 513/tcp on 192.168.56.101
Discovered open port 8180/tcp on 192.168.56.101
Discovered open port 1524/tcp on 192.168.56.101
Discovered open port 6667/tcp on 192.168.56.101
Discovered open port 6000/tcp on 192.168.56.101
Discovered open port 5432/tcp on 192.168.56.101
Discovered open port 512/tcp on 192.168.56.101
Completed SYN Stealth Scan at 22:44, 4.65s elapsed (1000 total ports)
NSE: Script scanning 192.168.56.101.
Initiating NSE at 22:44
```

```
NSE: [ssl-ccs-injection] No response from server: Unknown TLS protocol version or
content type
Completed NSE at 22:49, 316.87s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 1.52s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.018s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
| ssl-poodle:
|  VULNERABLE:
|  SSL POODLE information leak
|   State: VULNERABLE
|   IDs:  BID:70574  CVE:CVE-2014-3566
|       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.openssl.org/~bodo/ssl-poodle.pdf
|     https://www.securityfocus.com/bid/70574
|_    https://www.imperialviolet.org/2014/10/14/poodle.html
| 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_WITH_3DES_EDE_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: postfix builtin
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
|   References:
|     https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|   State: VULNERABLE
|   IDs:  BID:74733  CVE:CVE-2015-4000
|     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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|     https://www.securityfocus.com/bid/74733
|     https://weakdh.org
|
| 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
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
| 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-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.101
|   Found the following possible CSRF vulnerabilities:
|
|    Path: http://192.168.56.101:80/dvwa/
|    Form id:
|    Form action: login.php
|
|    Path: http://192.168.56.101:80/dvwa/login.php
|    Form id:
|    Form action: login.php
|
|    Path: http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php
|    Form id: id-bad-cred-tr
|    Form action: index.php?page=text-file-viewer.php
|
|    Path: http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php
|    Form id: id-bad-cred-tr
|_   Form action: index.php?page=text-file-viewer.php
| http-enum:
|  /tikiwiki/: Tikiwiki
|  /test/: Test page
|  /phpinfo.php: Possible information file
|  /phpMyAdmin/: phpMyAdmin
|  /doc/: Potentially interesting directory w/ listing on ‘apache/2.2.8 (ubuntu) dav/2’
|  /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-sql-injection:
|  Possible sqli for queries:
|    http://192.168.56.101:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
| http://192.168.56.101:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
| http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|    http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|   http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|   http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=rene-magritte.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|    http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|    http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|   http://192.168.56.101:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|   http://192.168.56.101:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|    http://192.168.56.101:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|_   http://192.168.56.101:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|_http-dombased-xss: Couldn’t find any DOM based XSS.
| http-fileupload-exploiter:
|
|_   Couldn’t find a file-type field.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn’t find any stored XSS vulnerabilities.
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  ⍰etasploi-ds
512/tcp  open  exec
513/tcp  open  login
```

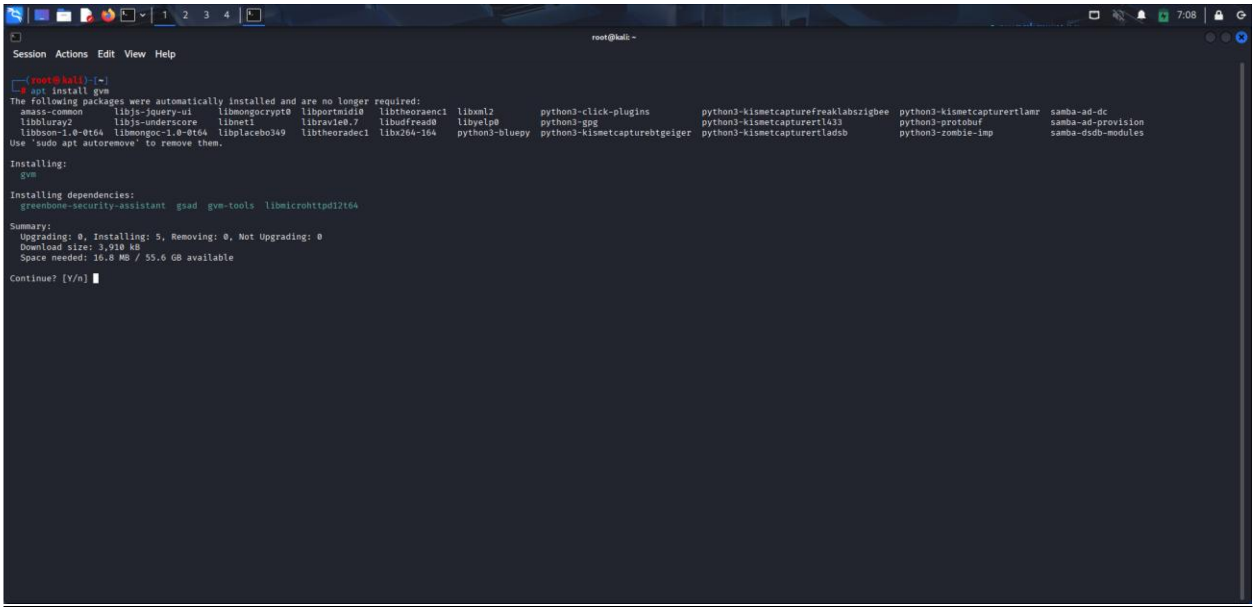
```
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs
which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/⍰etasploit-
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-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
| ssl-poodle:
|  VULNERABLE:
|  SSL POODLE information leak
|    State: VULNERABLE
|    IDs:  BID:70574  CVE:CVE-2014-3566
|        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.openssl.org/~bodo/ssl-poodle.pdf
|     https://www.securityfocus.com/bid/70574
|_     https://www.imperialviolet.org/2014/10/14/poodle.html
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
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:
|   JSESSIONID:
|     httponly flag not set
| /admin/admin-login.html:
|   JSESSIONID:
|     httponly flag not set
| /admin/adminLogin.html:
|   JSESSIONID:
|     httponly flag not set
| /admin/controlpanel.html:
|   JSESSIONID:
|     httponly flag not set
| /admin/cp.html:
|   JSESSIONID:
|     httponly flag not set
| /admin/index.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/login.jsp:
|   JSESSIONID:
|     httponly flag not set
| /admin/admin.jsp:
```

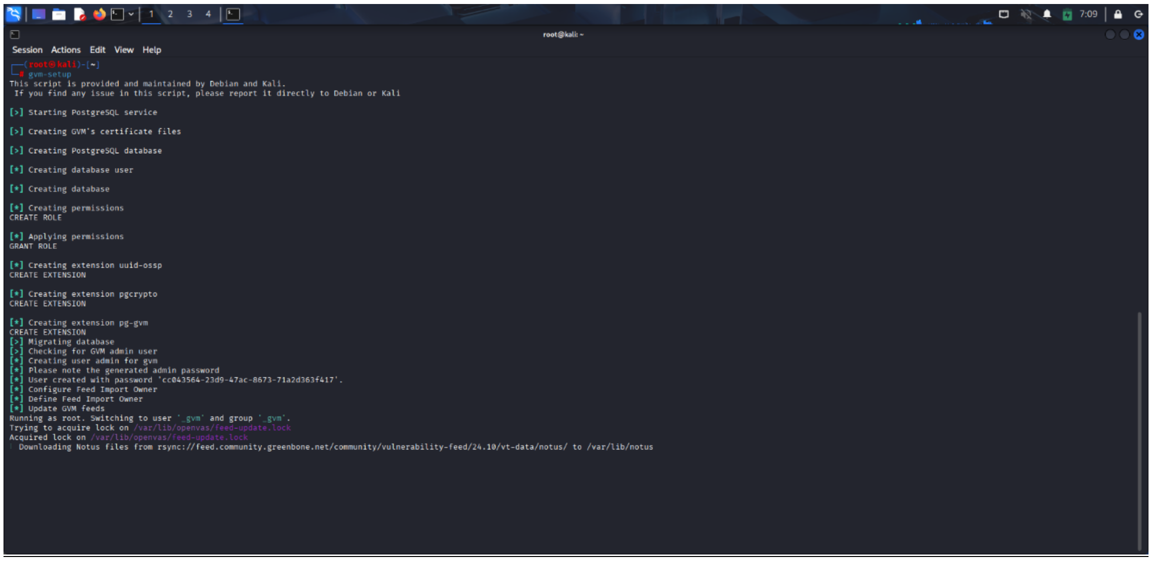
```
|    JSESSIONID:
|      httponly flag not set
|  /admin/home.jsp:
|    JSESSIONID:
|      httponly flag not set
|  /admin/controlpanel.jsp:
|    JSESSIONID:
|      httponly flag not set
|  /admin/admin-login.jsp:
|    JSESSIONID:
|      httponly flag not set
|  /admin/cp.jsp:
|    JSESSIONID:
|      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

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

NSE: Script Post-scanning.
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Initiating NSE at 22:49
Completed NSE at 22:49, 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 333.43 seconds
        Raw packets sent: 1982 (87.180KB) | Rcvd: 737 (29.572KB)
```

3) **Vulnerability Scanning :-**

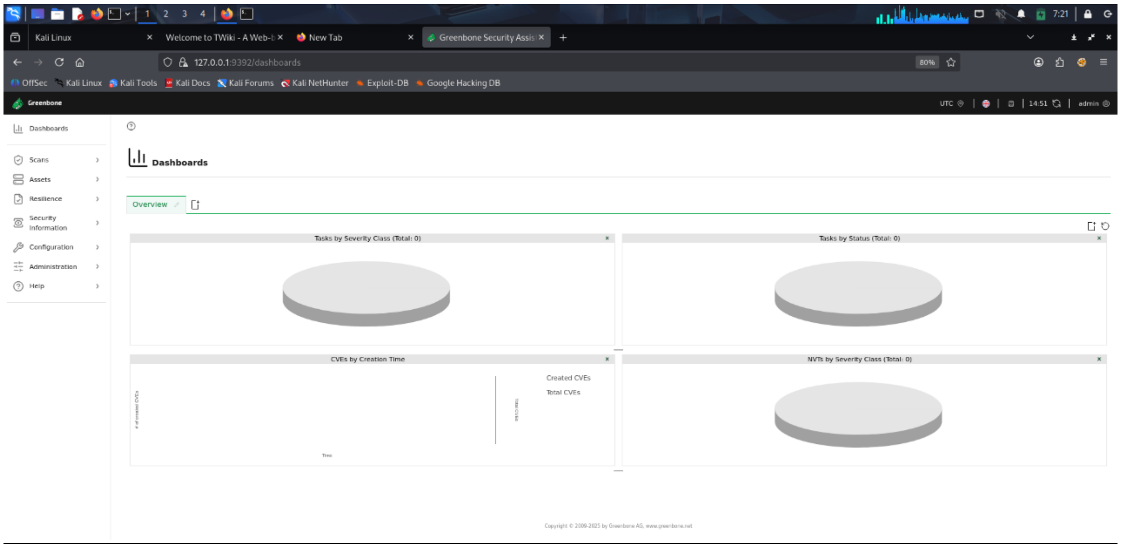
- Setup OpenVAS



```
┌──(root㉿kali)-[~]
└─# apt install gvm
The following packages were automatically installed and are no longer required:
  amass-common      libjs-jquery-ui     libmongocrypt0  libportmidi0   libtheoraenc1  libxml2        python3-click-plugins          python3-kismetcapturefreaklabszigbee  python3-kismetcapturertlamr  samba-ad-dc
  libbluray2        libjs-underscore    libnet1         librav1e0.7    libudfread0    libyelp0       python3-gpg                    python3-kismetcapturertl433           python3-protobuf             samba-ad-provision
  libbson-1.0-0t64  libmongoc-1.0-0t64  libplacebo349   libtheoradec1  libx264-164    python3-bluepy python3-kismetcapturebtgeiger  python3-kismetcapturertladsb          python3-zombie-imp           samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.

Installing:
  gvm

Installing dependencies:
  greenbone-security-assistant  gsad  gvm-tools  libmicrohttpd12t64

Summary:
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 0
  Download size: 3,910 kB
  Space needed: 16.8 MB / 55.6 GB available

Continue? [Y/n] █
```



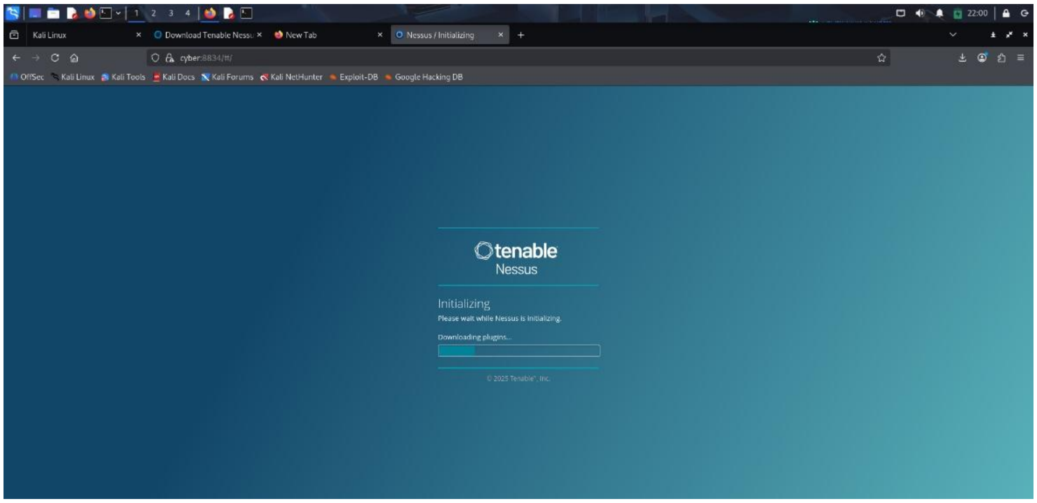
```
┌──(root㉿kali)-[~]
└─# gvm-setup
This script is provided and maintained by Debian and Kali.
 If you find any issue in this script, please report it directly to Debian or Kali

[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database

[*] Creating database user

[*] Creating database

[*] Creating permissions
CREATE ROLE

[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-ossp
CREATE EXTENSION

[*] Creating extension pgcrypto
CREATE EXTENSION

[*] Creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password 'cc043564-23d9-47ac-8673-71a2d363f417'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
  Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/24.10/vt-data/notus/ to /var/lib/notus
```



Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

OR

Nessus Essential:-

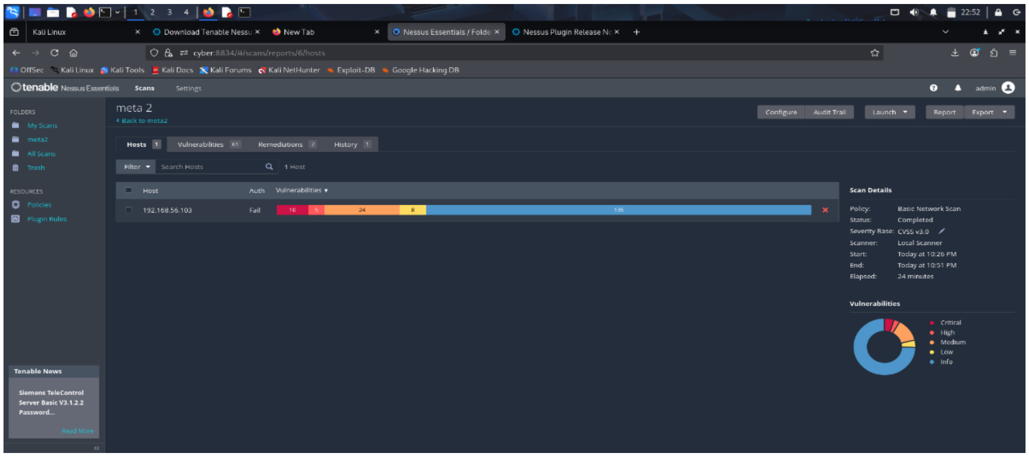


Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2025 Tenable®, Inc.



meta 2

< Back to meta2

1 Host

Host	Auth	Vulnerabilities
192.168.56.103	Fail	10 5 24 8 135

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

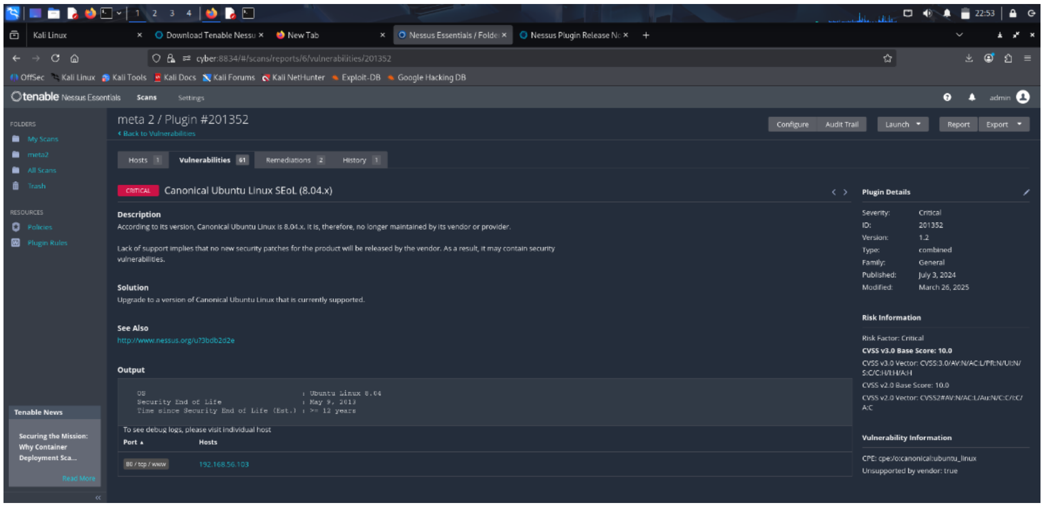
Scanner: Local Scanner

Start: Today at 10:26 PM

End: Today at 10:51 PM

Elapsed: 24 minutes

Vulnerabilities



meta 2 / Plugin #201352

CRITICAL Canonical Ubuntu Linux SEoL (8.04.x)

Description

According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

See Also

http://www.nessus.org/u?3bdb2d2e

Output

```
  OS                                   : Ubuntu Linux 8.04
  Security End of Life                 : May 9, 2013
  Time since Security End of Life (Est.) : >= 12 years
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	192.168.56.103

Plugin Details

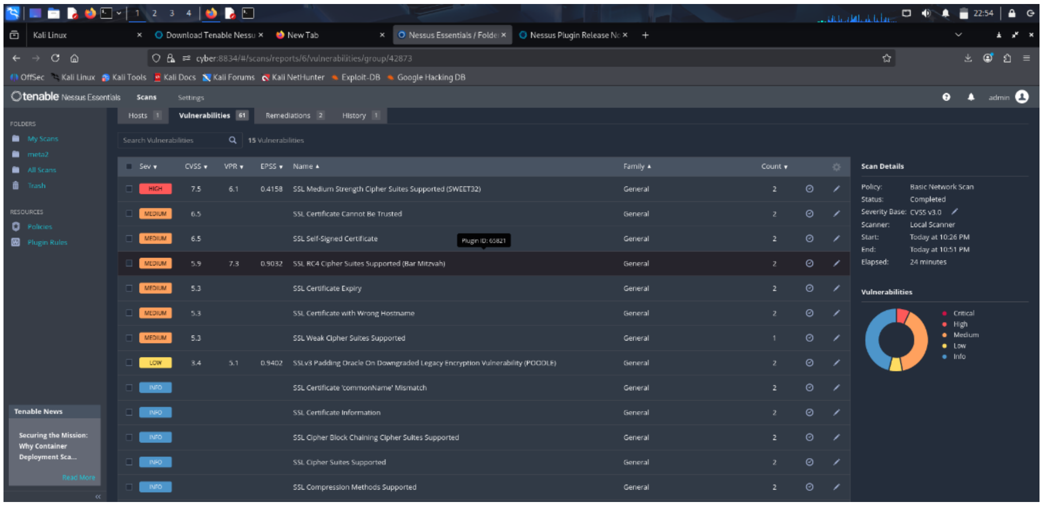
Severity: Critical
ID: 201352
Version: 1.2
Type: combined
Family: General
Published: July 3, 2024
Modified: March 26, 2025

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/o:canonical:ubuntu_linux
Unsupported by vendor: true



15 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▲	Family ▲	Count ▾
HIGH	7.5	6.1	0.4158	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	2
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	2
MEDIUM	6.5			SSL Self-Signed Certificate	General	2
MEDIUM	5.9	7.3	0.9032	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	2
MEDIUM	5.3			SSL Certificate Expiry	General	2
MEDIUM	5.3			SSL Certificate with Wrong Hostname	General	2
MEDIUM	5.3			SSL Weak Cipher Suites Supported	General	1
LOW	3.4	5.1	0.9402	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	2
INFO				SSL Certificate 'commonName' Mismatch	General	2
INFO				SSL Certificate Information	General	2
INFO				SSL Cipher Block Chaining Cipher Suites Supported	General	2
INFO				SSL Cipher Suites Supported	General	2
INFO				SSL Compression Methods Supported	General	2

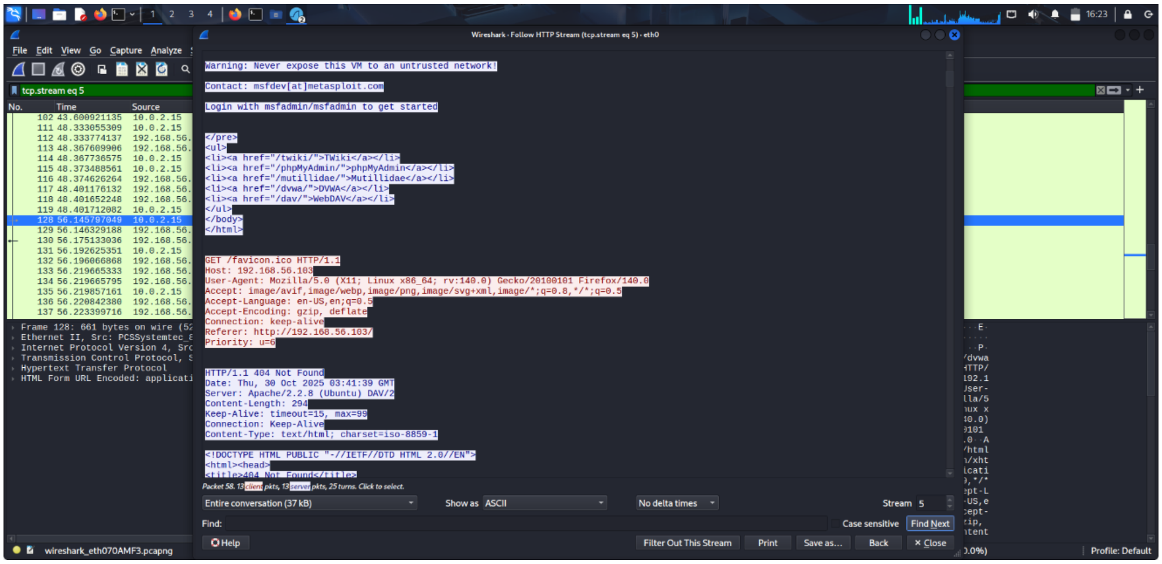
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:26 PM
End: Today at 10:51 PM
Elapsed: 24 minutes

Vulnerabilities

4) Packet Analysis with Wireshark:-

- Capture HTTP , FTP, DNS traffic / Filter credential



Wireshark · Follow HTTP Stream (tcp.stream eq 5) · eth0
File Edit View Go Capture Analyze
tcp.stream eq 5
16:23

```
No.  Time          Source
 102 43.600921135  10.0.2.15
 111 48.333055309  10.0.2.15
 112 48.333774137  192.168.56.
 113 48.367609906  192.168.56.
 114 48.367736575  10.0.2.15
 115 48.373488561  10.0.2.15
 116 48.374626264  192.168.56.
 117 48.401176132  192.168.56.
 118 48.401652248  192.168.56.
 119 48.401712082  10.0.2.15
 128 56.145797049  10.0.2.15
 129 56.146329188  192.168.56.
 130 56.175133036  192.168.56.
 131 56.192625351  10.0.2.15
 132 56.196066868  192.168.56.
 133 56.219665333  192.168.56.
 134 56.219665795  192.168.56.
 135 56.219857161  10.0.2.15
 136 56.220842380  192.168.56.
 137 56.223399716  192.168.56.

› Frame 128: 661 bytes on wire (52
› Ethernet II, Src: PCSSystemtec_8
› Internet Protocol Version 4, Src
› Transmission Control Protocol, S
› Hypertext Transfer Protocol
› HTML Form URL Encoded: applicati
```

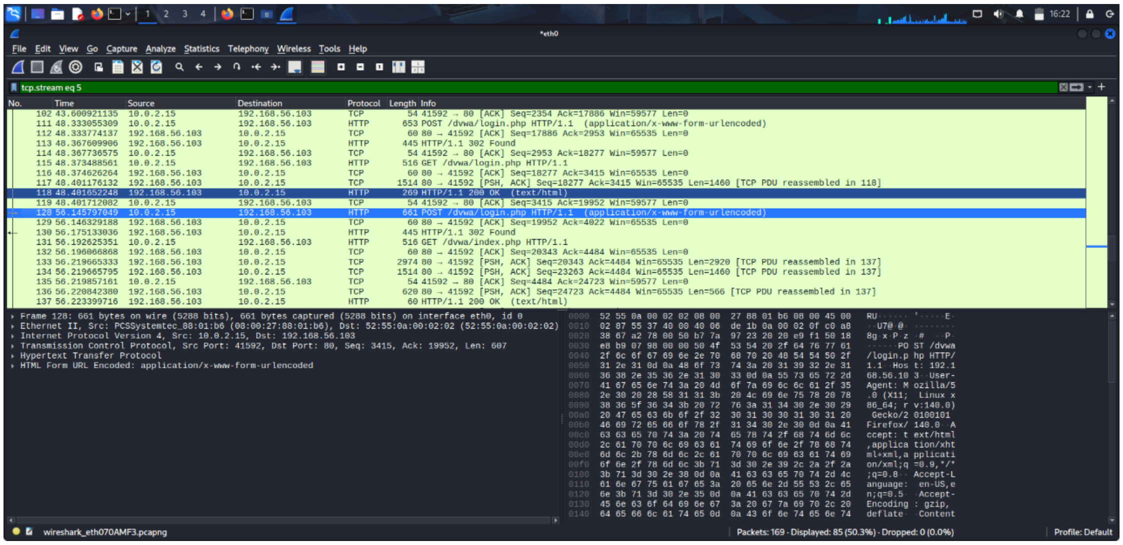
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>


GET /favicon.ico HTTP/1.1
Host: 192.168.56.103
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.56.103/
Priority: u=6


HTTP/1.1 404 Not Found
Date: Thu, 30 Oct 2025 03:41:39 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Length: 294
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
```

Packet 58. 13 client pkts, 13 server pkts, 25 turns. Click to select.

Entire conversation (37 kB) | Show as ASCII | No delta times | Stream 5

Find: | ☐ Case sensitive | Find Next

Help
Filter Out This Stream
Print
Save as…
Back
✕ Close
wireshark_eth070AMF3.pcapng
Profile: Default



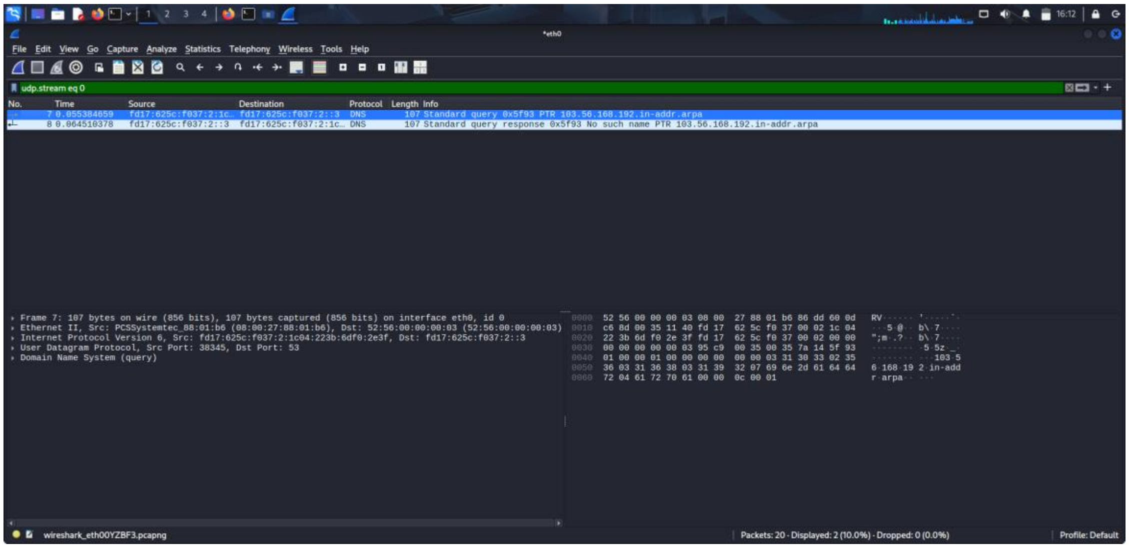
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 5
16:22

```
No.  Time          Source          Destination     Protocol Length Info
 102 43.600921135  10.0.2.15       192.168.56.103  TCP        54 41592 → 80 [ACK] Seq=2354 Ack=17886 Win=59577 Len=0
 111 48.333055309  10.0.2.15       192.168.56.103  HTTP      653 POST /dvwa/login.php HTTP/1.1  (application/x-www-form-urlencoded)
 112 48.333774137  192.168.56.103  10.0.2.15       TCP        60 80 → 41592 [ACK] Seq=17886 Ack=2953 Win=65535 Len=0
 113 48.367609906  192.168.56.103  10.0.2.15       HTTP      445 HTTP/1.1 302 Found
 114 48.367736575  10.0.2.15       192.168.56.103  TCP        54 41592 → 80 [ACK] Seq=2953 Ack=18277 Win=59577 Len=0
 115 48.373488561  10.0.2.15       192.168.56.103  HTTP      516 GET /dvwa/login.php HTTP/1.1
 116 48.374626264  192.168.56.103  10.0.2.15       TCP        60 80 → 41592 [ACK] Seq=18277 Ack=3415 Win=65535 Len=0
 117 48.401176132  192.168.56.103  10.0.2.15       TCP      1514 80 → 41592 [PSH, ACK] Seq=18277 Ack=3415 Win=65535 Len=1460 [TCP PDU reassembled in 118]
 118 48.401652248  192.168.56.103  10.0.2.15       HTTP      269 HTTP/1.1 200 OK  (text/html)
 119 48.401712082  10.0.2.15       192.168.56.103  TCP        54 41592 → 80 [ACK] Seq=3415 Ack=19952 Win=59577 Len=0
 128 56.145797049  10.0.2.15       192.168.56.103  HTTP      661 POST /dvwa/login.php HTTP/1.1  (application/x-www-form-urlencoded)
 129 56.146329188  192.168.56.103  10.0.2.15       TCP        60 80 → 41592 [ACK] Seq=19952 Ack=4022 Win=65535 Len=0
 130 56.175133036  192.168.56.103  10.0.2.15       HTTP      445 HTTP/1.1 302 Found
 131 56.192625351  10.0.2.15       192.168.56.103  HTTP      516 GET /dvwa/index.php HTTP/1.1
 132 56.196066868  192.168.56.103  10.0.2.15       TCP        60 80 → 41592 [ACK] Seq=20343 Ack=4484 Win=65535 Len=0
 133 56.219665333  192.168.56.103  10.0.2.15       TCP      2974 80 → 41592 [PSH, ACK] Seq=20343 Ack=4484 Win=65535 Len=2920 [TCP PDU reassembled in 137]
 134 56.219665795  192.168.56.103  10.0.2.15       TCP      1514 80 → 41592 [PSH, ACK] Seq=23263 Ack=4484 Win=65535 Len=1460 [TCP PDU reassembled in 137]
 135 56.219857161  10.0.2.15       192.168.56.103  TCP        54 41592 → 80 [ACK] Seq=4484 Ack=24723 Win=59577 Len=0
 136 56.220842380  192.168.56.103  10.0.2.15       TCP       620 80 → 41592 [PSH, ACK] Seq=24723 Ack=4484 Win=65535 Len=566 [TCP PDU reassembled in 137]
 137 56.223399716  192.168.56.103  10.0.2.15       HTTP       60 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 128: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_88:01:b6 (08:00:27:88:01:b6), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.168.56.103
› Transmission Control Protocol, Src Port: 41592, Dst Port: 80, Seq: 3415, Ack: 19952, Len: 607
› Hypertext Transfer Protocol
› HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  52 55 0a 00 02 02 08 00  27 88 01 b6 08 00 45 00   RU······ '·····E·
0010  02 87 55 37 40 00 40 06  de 1b 0a 00 02 0f c0 a8   ··U7@·@· ········
0020  38 67 a2 78 00 50 b7 7a  97 23 20 20 e9 f1 50 18   8g·x·P·z ·#   ··P·
0030  e8 b9 07 98 00 00 50 4f  53 54 20 2f 64 76 77 61   ······PO ST /dvwa
0040  2f 6c 6f 67 69 6e 2e 70  68 70 20 48 54 54 50 2f   /login.p hp HTTP/
0050  31 2e 31 0d 0a 48 6f 73  74 3a 20 31 39 32 2e 31   1.1··Hos t: 192.1
0060  36 38 2e 35 36 2e 31 30  33 0d 0a 55 73 65 72 2d   68.56.10 3··User-
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
0080  2e 30 20 28 58 31 31 3b  20 4c 69 6e 75 78 20 78   .0 (X11;  Linux x
0090  38 36 5f 36 34 3b 20 72  76 3a 31 34 30 2e 30 29   86_64; r v:140.0)
00a0  20 47 65 63 6b 6f 2f 32  30 31 30 30 31 30 31 20    Gecko/2 0100101 
00b0  46 69 72 65 66 6f 78 2f  31 34 30 2e 30 0d 0a 41   Firefox/ 140.0··A
00c0  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
00d0  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
00e0  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
00f0  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 2a 2f 2a   on/xml;q =0.9,*/*
0100  3b 71 3d 30 2e 38 0d 0a  41 63 63 65 70 74 2d 4c   ;q=0.8·· Accept-L
0110  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
0120  6e 3b 71 3d 30 2e 35 0d  0a 41 63 63 65 70 74 2d   n;q=0.5· ·Accept-
0130  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip, 
0140  64 65 66 6c 61 74 65 0d  0a 43 6f 6e 74 65 6e 74   deflate· ·Content
```

wireshark_eth070AMF3.pcapng | Packets: 169 · Displayed: 85 (50.3%) · Dropped: 0 (0.0%) | Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
16:12

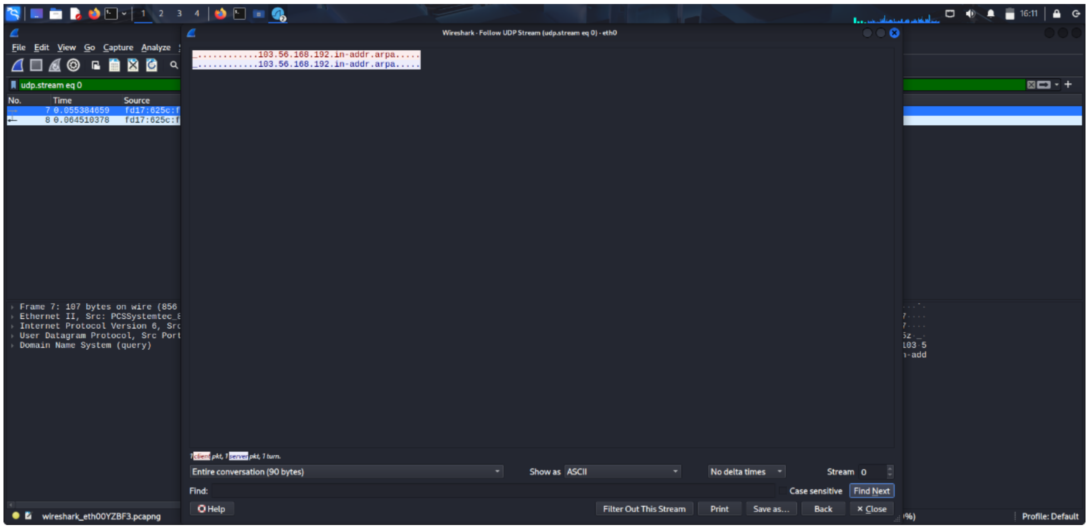
udp.stream eq 0

```
No.   Time          Source               Destination          Protocol Length Info
    7 0.055384659   fd17:625c:f037:2:1c… fd17:625c:f037:2::3  DNS      107 Standard query 0x5f93 PTR 103.56.168.192.in-addr.arpa
    8 0.064510378   fd17:625c:f037:2::3  fd17:625c:f037:2:1c… DNS      107 Standard query response 0x5f93 No such name PTR 103.56.168.192.in-addr.arpa
```

```
› Frame 7: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_88:01:b6 (08:00:27:88:01:b6), Dst: 52:56:00:00:00:03 (52:56:00:00:00:03)
› Internet Protocol Version 6, Src: fd17:625c:f037:2:1c04:223b:6df0:2e3f, Dst: fd17:625c:f037:2::3
› User Datagram Protocol, Src Port: 38345, Dst Port: 53
› Domain Name System (query)
```

```
0000  52 56 00 00 00 03 08 00  27 88 01 b6 86 dd 60 0d   RV······'·····`·
0010  c6 8d 00 35 11 40 fd 17  62 5c f0 37 00 02 1c 04   ···5·@··b\·7····
0020  22 3b 6d f0 2e 3f fd 17  62 5c f0 37 00 02 00 00   ";m·.?··b\·7····
0030  00 00 00 00 00 03 95 c9  00 35 00 35 7a 14 5f 93   ·········5·5z·_·
0040  01 00 00 01 00 00 00 00  00 00 03 31 30 33 02 35   ···········103·5
0050  36 03 31 36 38 03 31 39  32 07 69 6e 2d 61 64 64   6·168·19 2·in-add
0060  72 04 61 72 70 61 00 00  0c 00 01                 r·arpa·· ···
```

wireshark_eth00YZBF3.pcapng | Packets: 20 · Displayed: 2 (10.0%) · Dropped: 0 (0.0%) | Profile: Default



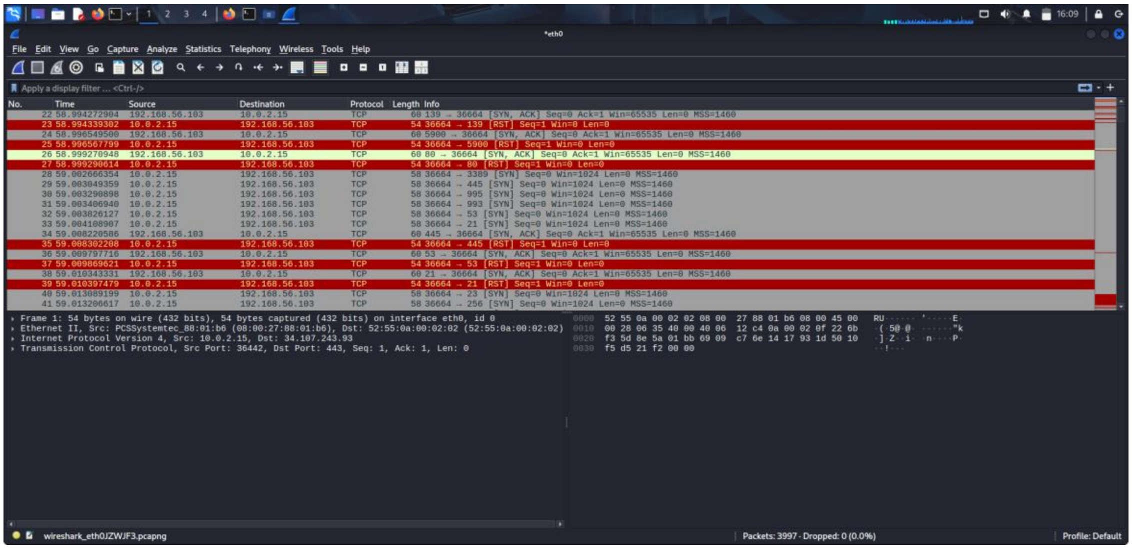
Wireshark · Follow UDP Stream (udp.stream eq 0) · eth0

```
_............103.56.168.192.in-addr.arpa.....
_............103.56.168.192.in-addr.arpa.....
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (90 bytes) Show as ASCII No delta times Stream 0

Find: □ Case sensitive


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
16:09

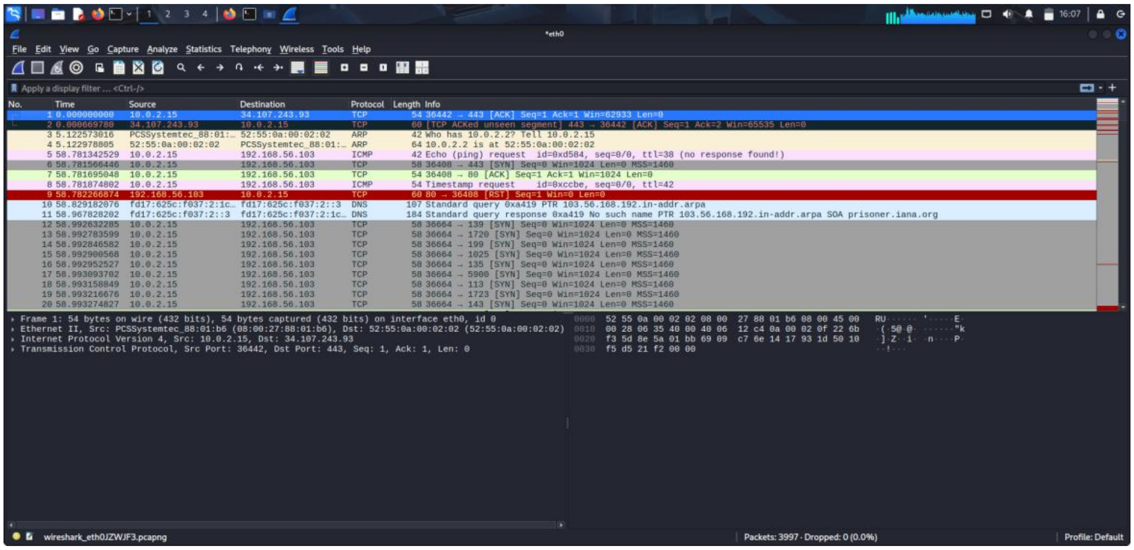
Apply a display filter … <Ctrl-/>

```
No.   Time          Source           Destination      Protocol Length Info
   22 58.994272904  192.168.56.103   10.0.2.15        TCP      60 139 → 36664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   23 58.994339302  10.0.2.15        192.168.56.103   TCP      54 36664 → 139 [RST] Seq=1 Win=0 Len=0
   24 58.996549500  192.168.56.103   10.0.2.15        TCP      60 5900 → 36664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   25 58.996567799  10.0.2.15        192.168.56.103   TCP      54 36664 → 5900 [RST] Seq=1 Win=0 Len=0
   26 58.999270948  192.168.56.103   10.0.2.15        TCP      60 80 → 36664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   27 58.999290614  10.0.2.15        192.168.56.103   TCP      54 36664 → 80 [RST] Seq=1 Win=0 Len=0
   28 59.002666354  10.0.2.15        192.168.56.103   TCP      58 36664 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   29 59.003049359  10.0.2.15        192.168.56.103   TCP      58 36664 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   30 59.003290898  10.0.2.15        192.168.56.103   TCP      58 36664 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   31 59.003406940  10.0.2.15        192.168.56.103   TCP      58 36664 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   32 59.003826127  10.0.2.15        192.168.56.103   TCP      58 36664 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   33 59.004108907  10.0.2.15        192.168.56.103   TCP      58 36664 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   34 59.008220586  192.168.56.103   10.0.2.15        TCP      60 445 → 36664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   35 59.008302208  10.0.2.15        192.168.56.103   TCP      54 36664 → 445 [RST] Seq=1 Win=0 Len=0
   36 59.009797716  192.168.56.103   10.0.2.15        TCP      60 53 → 36664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   37 59.009869621  10.0.2.15        192.168.56.103   TCP      54 36664 → 53 [RST] Seq=1 Win=0 Len=0
   38 59.010343331  192.168.56.103   10.0.2.15        TCP      60 21 → 36664 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
   39 59.010397479  10.0.2.15        192.168.56.103   TCP      54 36664 → 21 [RST] Seq=1 Win=0 Len=0
   40 59.013089199  10.0.2.15        192.168.56.103   TCP      58 36664 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   41 59.013206617  10.0.2.15        192.168.56.103   TCP      58 36664 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
› Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_88:01:b6 (08:00:27:88:01:b6), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.243.93
› Transmission Control Protocol, Src Port: 36442, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  52 55 0a 00 02 02 08 00  27 88 01 b6 08 00 45 00   RU······'·····E·
0010  00 28 06 35 40 00 40 06  12 c4 0a 00 02 0f 22 6b   ·(·5@·@·······"k
0020  f3 5d 8e 5a 01 bb 69 09  c7 6e 14 17 93 1d 50 10   ·]·Z··i··n····P·
0030  f5 d5 21 f2 00 00                                  ··!···
```

wireshark_eth0JZWJF3.pcapng | Packets: 3997 · Dropped: 0 (0.0%) | Profile: Default



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
16:07

```
No.  Time         Source                   Destination              Protocol Length Info
   1 0.000000000  10.0.2.15                34.107.243.93            TCP        54 36442 → 443 [ACK] Seq=1 Ack=1 Win=62933 Len=0
   2 0.000669780  34.107.243.93            10.0.2.15                TCP        60 [TCP ACKed unseen segment] 443 → 36442 [ACK] Seq=1 Ack=2 Win=65535 Len=0
   3 5.122573016  PCSSystemtec_88:01:…     52:55:0a:00:02:02        ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
   4 5.122978805  52:55:0a:00:02:02        PCSSystemtec_88:01:…     ARP        64 10.0.2.2 is at 52:55:0a:00:02:02
   5 58.781342529 10.0.2.15                192.168.56.103           ICMP       42 Echo (ping) request  id=0xd584, seq=0/0, ttl=38 (no response found!)
   6 58.781566446 10.0.2.15                192.168.56.103           TCP        58 36408 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   7 58.781695048 10.0.2.15                192.168.56.103           TCP        54 36408 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
   8 58.781874802 10.0.2.15                192.168.56.103           ICMP       54 Timestamp request    id=0xccbe, seq=0/0, ttl=42
   9 58.782266874 192.168.56.103           10.0.2.15                TCP        60 80 → 36408 [RST] Seq=1 Win=0 Len=0
  10 58.829182076 fd17:625c:f037:2:1c…     fd17:625c:f037:2::3      DNS       107 Standard query 0xa419 PTR 103.56.168.192.in-addr.arpa
  11 58.967828202 fd17:625c:f037:2::3      fd17:625c:f037:2:1c…     DNS       184 Standard query response 0xa419 No such name PTR 103.56.168.192.in-addr.arpa SOA prisoner.iana.org
  12 58.992632285 10.0.2.15                192.168.56.103           TCP        58 36664 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  13 58.992783599 10.0.2.15                192.168.56.103           TCP        58 36664 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  14 58.992846582 10.0.2.15                192.168.56.103           TCP        58 36664 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  15 58.992900568 10.0.2.15                192.168.56.103           TCP        58 36664 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  16 58.992952527 10.0.2.15                192.168.56.103           TCP        58 36664 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  17 58.993093702 10.0.2.15                192.168.56.103           TCP        58 36664 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  18 58.993158849 10.0.2.15                192.168.56.103           TCP        58 36664 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  19 58.993216676 10.0.2.15                192.168.56.103           TCP        58 36664 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
  20 58.993274827 10.0.2.15                192.168.56.103           TCP        58 36664 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

```
› Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_88:01:b6 (08:00:27:88:01:b6), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 34.107.243.93
› Transmission Control Protocol, Src Port: 36442, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  52 55 0a 00 02 02 08 00  27 88 01 b6 08 00 45 00   RU······'·····E·
0010  00 28 06 35 40 00 40 06  12 c4 0a 00 02 0f 22 6b   ·(·5@·@·······"k
0020  f3 5d 8e 5a 01 bb 69 09  c7 6e 14 17 93 1d 50 10   ·]·Z··i··n····P·
0030  f5 d5 21 f2 00 00                                  ··!···
```

```
wireshark_eth0JZWJF3.pcapng          Packets: 3997 · Dropped: 0 (0.0%)          Profile: Default
```

5) Firewall Basics :-

1. Prepare (reset rules)

Commands:

```
sudo iptables -F
sudo iptables -X
sudo iptables -Z
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

2. Essential safe rules

Allow loopback and established connections:

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Allow specific services (example):

```
sudo iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT   # SSH
sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT   # HTTP
sudo iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW -j ACCEPT  # HTTPS
```

3. Simple port-scan detection & block (recent-based)

This detects many NEW connection attempts from the same IP in short time and drops them:

```
sudo iptables -N PS_DETECT
sudo iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j PS_DETECT
sudo iptables -A PS_DETECT -m recent --name portscan --set
sudo iptables -A PS_DETECT -m recent --name portscan --update --seconds 60 --hitcount 15 -j LOG --log-prefix "PORTSCAN: "
sudo iptables -A PS_DETECT -m recent --name portscan --update --seconds 60 --hitcount 15 -j DROP
```

4. Throttle SYNs (alternative)

Limit new TCP SYNs per source:

```
sudo iptables -A INPUT -p tcp --syn -m hashlimit --hashlimit-name conn_limit --hashlimit-above 5/sec --hashlimit-burst 10 --hashlimit-mode srcip -j DROP
```

5. Logging & checking

Log file to watch: /var/log/syslog or use journalctl. List rules:

```
sudo iptables -L -n -v --line-numbers
```

View logs: sudo tail -f /var/log/syslog

6. Undo (restore access)

```
sudo iptables -F
sudo iptables -X
sudo iptables -Z
sudo iptables -P INPUT ACCEPT
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT
```