

Scanning Networks

Tools:

Nmap, Netdiscover, Masscan, and Apache2

Download:

This all tools are pre-installed in pentesting linux distro

NMAP: <https://nmap.org/download>

Masscan: <https://github.com/robertdavidgraham/masscan>

Netdiscover: <https://github.com/netdiscover-scanner/netdiscover>

Apache 2: <https://httpd.apache.org/download.cgi>

- **Performing network scanning and device discovery**

Nmap :Network mapper

Syntax: nmap [options] [target(url) or (ip)]

NOTICE:

Here we are using the metasploitable machine as a target because we don't have any right or permissions to pentesting on any website available on internet

Some are the organization is provide websites for penetration tester to penetrate on it like acunetix, portswigger etc..

But Metasploitable is vulnerable machine and the website is also configured in it so we get all on one platform

Metasploitable IP [10.0.2.4] :different for all device

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6c:25:8e
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6c:258e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3882 (3.7 KB)  TX bytes:6168 (6.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

Nmap results :

Results of nmap for metasploitable

Command : nmap -sV -sC -A -p- -v 10.0.2.4

[-sV service version detection

-sC default script scan

-A- aggressive scan

-p- scanning all ports

-v verbose]

Syntax:

```
[root@warmachine]-[/]  
#nmap -sC -sV -A -p- -v 10.0.2.4
```

Scanning:

```
[root@warmachine]-[/]  
#nmap -sC -sV -A -p- -v 10.0.2.4  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 20:34 IST  
NSE: Loaded 155 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 20:34  
Completed NSE at 20:34, 0.00s elapsed  
Initiating NSE at 20:34  
Completed NSE at 20:34, 0.00s elapsed  
Initiating NSE at 20:34  
Completed NSE at 20:34, 0.00s elapsed  
Initiating ARP Ping Scan at 20:34  
Scanning 10.0.2.4 [1 port]  
Completed ARP Ping Scan at 20:34, 0.19s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 20:34  
Completed Parallel DNS resolution of 1 host. at 20:34, 0.11s elapsed  
Initiating SYN Stealth Scan at 20:34  
Scanning 10.0.2.4 [65535 ports]
```

Open ports:

```
Initiating SYN Stealth Scan at 20:34
Scanning 10.0.2.4 [65535 ports]
Discovered open port 139/tcp on 10.0.2.4
Discovered open port 3306/tcp on 10.0.2.4
Discovered open port 53/tcp on 10.0.2.4
Discovered open port 80/tcp on 10.0.2.4
Discovered open port 22/tcp on 10.0.2.4
Discovered open port 5900/tcp on 10.0.2.4
Discovered open port 21/tcp on 10.0.2.4
Discovered open port 445/tcp on 10.0.2.4
Discovered open port 25/tcp on 10.0.2.4
Discovered open port 23/tcp on 10.0.2.4
Discovered open port 111/tcp on 10.0.2.4
Discovered open port 6667/tcp on 10.0.2.4
Discovered open port 1524/tcp on 10.0.2.4
Discovered open port 6000/tcp on 10.0.2.4
Discovered open port 512/tcp on 10.0.2.4
Discovered open port 3632/tcp on 10.0.2.4
Discovered open port 6697/tcp on 10.0.2.4
Discovered open port 57519/tcp on 10.0.2.4
Discovered open port 59315/tcp on 10.0.2.4
Discovered open port 34014/tcp on 10.0.2.4
Discovered open port 513/tcp on 10.0.2.4
Discovered open port 5432/tcp on 10.0.2.4
Discovered open port 8009/tcp on 10.0.2.4
Discovered open port 8180/tcp on 10.0.2.4
Discovered open port 2121/tcp on 10.0.2.4
Discovered open port 1099/tcp on 10.0.2.4
Discovered open port 60859/tcp on 10.0.2.4
Discovered open port 2049/tcp on 10.0.2.4
Discovered open port 8787/tcp on 10.0.2.4
Discovered open port 514/tcp on 10.0.2.4
Completed SYN Stealth Scan at 20:35, 65.28s elapsed (65535 total ports)
```

We scan all 65535 ports and get the all open ports from 0 to 65535

Service and Service version:

```
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 10.0.2.15
|_     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:bl:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_ smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
|_ ssl-date: 2023-01-05T15:02:53+00:00; -5m11s from scanner time.
```

```
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
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           38683/udp   mountd
|_   100005  1,2,3           59315/tcp   mountd
|_   100021  1,3,4           34014/tcp   nlockmgr
|_   100021  1,3,4           39176/udp   nlockmgr
|_   100024  1                59164/udp   status
|_   100024  1                60859/tcp   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  tcpwrapped
1099/tcp   open  java-rmi     GNU Classpath grmiregistry
1524/tcp   open  bindshell    Metasploitable root shell
2049/tcp   open  nfs          2-4 (RPC #100003)
2121/tcp   open  ftp          ProFTPD 1.3.1
3306/tcp   open  mysql        MySQL 5.0.51a-3ubuntu5
|_ mysql-info:
|_   Protocol: 10
|_   Version: 5.0.51a-3ubuntu5
```

```

3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
mysql-info:
  Protocol: 10
  Version: 5.0.51a-3ubuntu5
  Thread ID: 8
  Capabilities flags: 43564
  Some Capabilities: SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression, Speaks41ProtocolNew, Support41Auth, LongColumnFlag, SupportsTransactions
  Status: Autocommit
  Salt: QAlgg2buHE 2z0-NGZo>
3632/tcp open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
  ssl-date: 2023-01-05T15:02:53+00:00; -5m11s 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
6697/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-methods:
  Supported Methods: GET HEAD POST OPTIONS
  http-title: Apache Tomcat/5.5
  http-server-header: Apache-Coyote/1.1
  http-favicon: Apache Tomcat
8787/tcp open  drb        Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
34014/tcp open  nlockmgr   1-4 (RPC #100021)
57519/tcp open  java-rmi   GNU Classpath grmiregistry
59315/tcp open  mountd     1-3 (RPC #100005)
60859/tcp open  status     1 (RPC #100024)

```

We got the services and the versions of service are running on different ports

Port /Services

21:ftp

22:ssh

23:telnet

25:smtp

53:domain

80:http

111:rpcbind

130:netbios-ssn

445:netbios-ssn

512:exec

513:login

514:tcpwrapped

1099:java-rmi

1524:bindshell

2049:nfs

2121:ftp

3306:mysql

Os Detection:

```
MAC Address: 08:00:27:6C:25:8E (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/5%OT=21%CT=1%CU=41404%PV=Y%DS=1%DC=D%G=Y%M=080027%TM
OS:=63B6E7D9%P=x86_64-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=C9%TI=Z%CI=Z%II=I%TS
OS:=5)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5=M
OS:5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16
OS:A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=
OS:S+F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+F=AS%O=M5B4ST11N
OS:W5%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%
OS:W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=
OS: )T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%
OS:UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.000 days (since Thu Jan 5 20:37:52 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We got the os of target

Os:Linux

Host and Traceroute:

```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1e>       Flags: <group><active>
|_clock-skew: mean: 1h09m51s, deviation: 2h30m02s, median: -5m11s
|_smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_   System time: 2023-01-05T10:02:50-05:00

TRACEROUTE
HOP RTT      ADDRESS
1   12.94 ms  10.0.2.4
```

We got the host and traceroute

We got the nsb,os name ,domain and domain name and ip address

Masscan:Faster network scanning

Syntax: masscan [target] [option]

Command :masscan <ip> -p 0-65535 -v --rate 10000 -oG masscan_result.txt

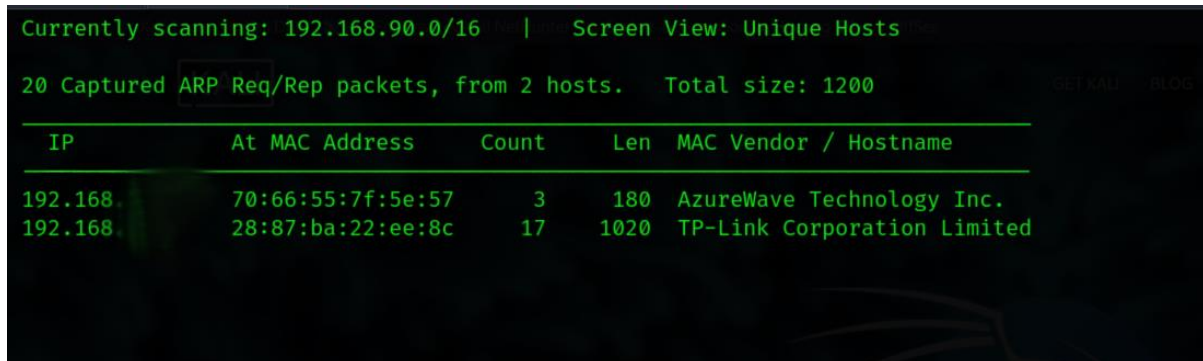
-p<port> , -v<verbose> , --rate<speed> -oG <output format >


```
(root@kali)-[/]
# masscan 192.168.1.0/24 -p 0-65535 -v --rate 10000 -oG masscan_result.txt
[-] pcap: failed to load: libpcap.so
[-] pcap: failed to load: libpcap.A.dylib
[-] pcap: failed to load: libpcap.dylib
[-] pcap: failed to load: libpcap.so.0.9.5
[-] pcap: failed to load: libpcap.so.0.9.4
[+] pcap: found library: libpcap.so.0.8
[+] interface = eth0
[+] if(eth0): pcap: libpcap version 1.10.1 (with TPACKET_V3)
[+] if(eth0): successfully opened
[+] interface-type = 1
if:eth0: type=ethernet(1)
[+] source-mac = 08-00-27-af-24-27
[+] source-ip = 192.168.1.1
[+] router-ip = 192.168.1.1
[+] arp: 192.168.1.1 = 28-87-ba-22-ee-8c
[+] router-mac-ipv4 = 28-87-ba-22-ee-8c
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-01-06 03:24:56 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
[+] starting transmit thread #0
[+] starting throttler: rate = 10000.00-pps
[+] starting receive thread #0
[+] waiting for threads to finish
[+] transmit thread #0 complete 0:00:00 remaining, found=11
[+] exiting transmit thread #0 und=11
[+] exiting receive thread #0 found=11
[+] all threads have exited
```

```
(root@kali)-[/]
# cat masscan_result.txt
# Masscan 1.3.2 scan initiated Fri Jan 6 03:24:56 2023
# Ports scanned: TCP(65536;0-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1672975497 Host: 192.168.1.1 () Ports: 1043/open/tcp//unknown//
Timestamp: 1672975497 Host: 192.168.1.1 () Ports: 445/open/tcp//microsoft-ds//
Timestamp: 1672975505 Host: 192.168.1.1 () Ports: 60859/open/tcp//unknown//
Timestamp: 1672975512 Host: 192.168.1.1 () Ports: 60860/open/tcp//unknown//
Timestamp: 1672975517 Host: 192.168.1.1 () Ports: 49668/open/tcp//unknown//
Timestamp: 1672975521 Host: 192.168.1.1 () Ports: 7680/open/tcp//unknown//
Timestamp: 1672975523 Host: 192.168.1.1 () Ports: 9013/open/tcp//unknown//
Timestamp: 1672975523 Host: 192.168.1.1 () Ports: 1042/open/tcp//unknown//
Timestamp: 1672975524 Host: 192.168.1.1 () Ports: 9012/open/tcp//unknown//
Timestamp: 1672975526 Host: 192.168.1.1 () Ports: 139/open/tcp//netbios-ssn//
Timestamp: 1672975533 Host: 192.168.1.1 () Ports: 135/open/tcp//epmap//
# Masscan done at Fri Jan 6 03:25:50 2023
```

Netdiscover : Scan the whole network

Command :netdiscover



The screenshot shows the Netdiscover interface with a dark background and green text. At the top, it says 'Currently scanning: 192.168.90.0/16 | Screen View: Unique Hosts'. Below that, it reports '20 Captured ARP Req/Rep packets, from 2 hosts. Total size: 1200'. A table follows with columns: IP, At MAC Address, Count, Len, and MAC Vendor / Hostname. Two entries are listed: one for IP 192.168.1.100 (partially visible) with MAC 70:66:55:7f:5e:57, and another for IP 192.168.1.1 (partially visible) with MAC 28:87:ba:22:ee:8c.

| IP | At MAC Address | Count | Len | MAC Vendor / Hostname |
|---------------|-------------------|-------|------|-----------------------------|
| 192.168.1.100 | 70:66:55:7f:5e:57 | 3 | 180 | AzureWave Technology Inc. |
| 192.168.1.1 | 28:87:ba:22:ee:8c | 17 | 1020 | TP-Link Corporation Limited |

- **launch a website on the personal system using the Apache2 server**

In this we are going with the default apache server which is pre-installed in kali linux

Apache server

Starting apache server

Command :service apache2 start

```
(root@kali)-[/]  
# service apache2 start
```

Checking Status:

Command: service apache2 status

```
(root@kali)-[/]  
# service apache2 status  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)  
   Active: active (running) since Thu 2023-01-05 21:17:47 IST; 43s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Process: 2888 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
   Main PID: 2911 (apache2)  
     Tasks: 7 (limit: 4611)  
   Memory: 20.4M  
      CPU: 3.040s  
   CGroup: /system.slice/apache2.service  
           └─2911 /usr/sbin/apache2 -k start  
             └─2916 /usr/sbin/apache2 -k start  
               └─2917 /usr/sbin/apache2 -k start  
                 └─2918 /usr/sbin/apache2 -k start  
                   └─2919 /usr/sbin/apache2 -k start  
                     └─2920 /usr/sbin/apache2 -k start  
                       └─2921 /usr/sbin/apache2 -k start  
  
Jan 05 21:17:39 kali systemd[1]: Starting The Apache HTTP Server...  
Jan 05 21:17:47 kali apachectl[2898]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Serv>  
Jan 05 21:17:47 kali systemd[1]: Started The Apache HTTP Server.  
lines 1-21/21 (END)
```

We also have to start mysql server

Command :service mysql start

```
(root@kali)-[/]  
# service mysql start
```

Checking status

Command :service mysql status

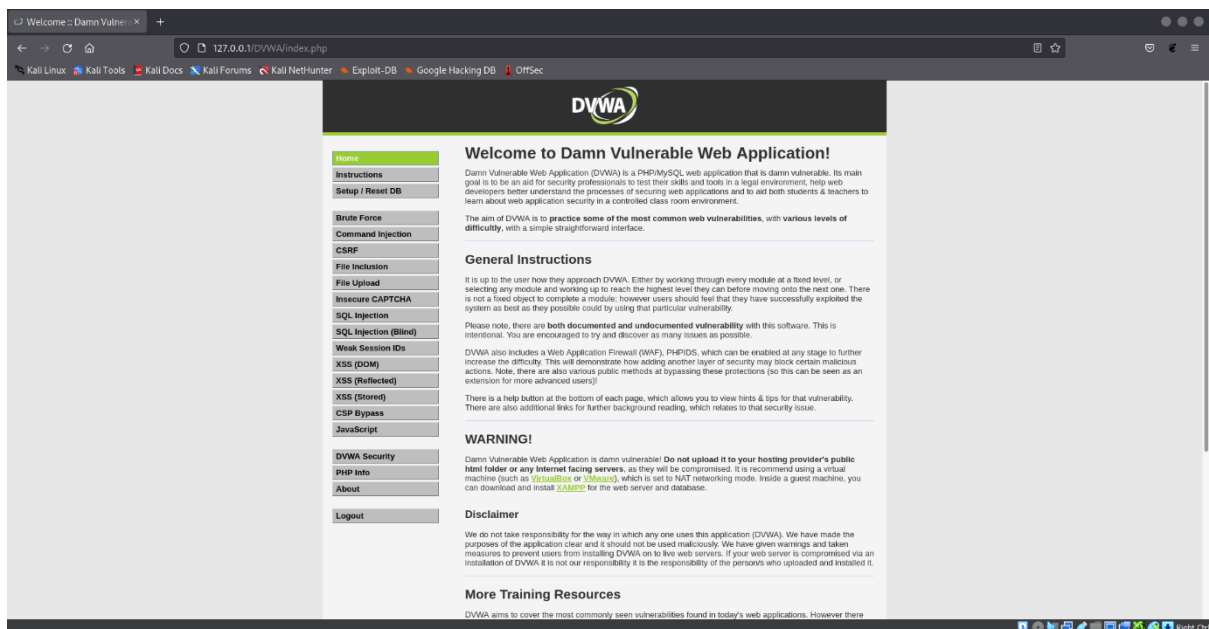
```

(root@kali)-[/]
# service mysql status
● mariadb.service - MariaDB 10.6.7 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2023-01-05 21:22:24 IST; 2min 35s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
 Process: 3033 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql (code=exited, status=0/SUCCESS)
 Process: 3034 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
 Process: 3036 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR="/usr/bin/galera_recovery"; [ $? -eq 0 ] && sy>
 Process: 3078 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
 Process: 3080 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 3066 (mariabdb)
   Status: "Taking your SQL requests now..."
    Tasks: 11 (limit: 4611)
  Memory: 92.8M
     CPU: 12.566s
    CGroup: /system.slice/mariadb.service
            └─3066 /usr/sbin/mariabdb

Jan 05 21:22:24 kali mariabdb[3066]: Version: '10.6.7-MariaDB-3' socket: '/run/mysqld/mysqld.sock' port: 3306 Debian build-
Jan 05 21:22:24 kali systemd[1]: Started MariaDB 10.6.7 database server.
Jan 05 21:22:24 kali /etc/mysql/debian-start[3082]: Upgrading MySQL tables if necessary.
Jan 05 21:22:26 kali /etc/mysql/debian-start[3086]: Looking for 'mysql' as: /usr/bin/mysql
Jan 05 21:22:26 kali /etc/mysql/debian-start[3086]: Looking for 'mysqlcheck' as: /usr/bin/mysqlcheck
Jan 05 21:22:26 kali /etc/mysql/debian-start[3086]: This installation of MariaDB is already upgraded to 10.6.7-MariaDB.
Jan 05 21:22:26 kali /etc/mysql/debian-start[3086]: There is no need to run mysql_upgrade again for 10.6.7-MariaDB.
Jan 05 21:22:26 kali /etc/mysql/debian-start[3086]: You can use --force if you still want to run mysql_upgrade
Jan 05 21:22:27 kali /etc/mysql/debian-start[3094]: Checking for insecure root accounts.
Jan 05 21:22:28 kali /etc/mysql/debian-start[3098]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables
lines 1-28/28 (END)

```

We have configured our web on localhost. For access web we have to type [127.0.0.1/DVWA/] in web browser url.



- get the output of the network scanning and device discovery tools into the specified format.

We can get the different types of options for saving the results in different format

-o=saving output

Command :`nmap -sC -sV -A -o` , `nmap -sC -sV -A -oA`

```
[root@warmachine]~#  
#nmap -sC -sV -v 10.0.2.4 -o /nmap_results  
Warning: The -o option is deprecated. Please use -oN  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 20:57 IST  
NSE: Loaded 155 scripts for scanning.  
NSE: Script Pre-scanning.
```

Result file :`nmap_results`

```
[root@warmachine]~#  
#ls  
bin      dev      home      initrd.img.old  lib32  libx32  mnt      opt      root  sbin  sys  usr  vmlinuz  
boot    etc      initrd.img  lib             lib64  media  nmap_results  proc  run  srv  tmp  var  vmlinuz.old
```

```
nmap_results X  
1 # Nmap 7.92 Scan initiated Thu Jan 5 20:57:13 2023 as: nmap -sC -sV -v -o /nmap_results 10.0.2.4  
2 Nmap scan report for 10.0.2.4  
3 Host is up (0.020s latency).  
4 Not shown: 977 closed tcp ports (reset)  
5 PORT      STATE SERVICE      VERSION  
6 21/tcp    open  ftp          vsftpd 2.3.4  
7 |_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
8 |_ftp-syst:  
9 |_STAT:  
10 |_FTP server status:  
11 |_Connected to 10.0.2.15  
12 |_Logged in as ftp  
13 |_TYPE: ASCII  
14 |_No session bandwidth limit  
15 |_Session timeout in seconds is 300  
16 |_Control connection is plain text  
17 |_Data connections will be plain text  
18 |_vsFTPD 2.3.4 - secure, fast, stable  
19 |_End of status  
20 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
21 |_ssh-hostkey:  
22 |_1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
23 |_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
24 23/tcp    open  telnet       Linux telnetd  
25 25/tcp    open  smtp         Postfix smtpd  
26 |_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN  
27 |_sslv2:  
28 |_SSLv2 supported  
29 |_ciphers:  
30 |_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5  
31 |_SSL2_DES_64_CBC_WITH_MD5  
32 |_SSL2_RC4_128_WITH_MD5  
33 |_SSL2_DES_192_EDE3_CBC_WITH_MD5  
34 |_SSL2_RC4_128_EXPORT40_WITH_MD5  
35 |_SSL2_RC2_128_CBC_WITH_MD5  
36 |_ssl-date: 2023-01-05T15:11:03+00:00: -16m38s from scanner time.
```

This create the files in different files simple,xml,gmap

```
[root@warmachine]-[/]
#nmap -sC -sV -v 10.0.2.4 -oA /nmap_results_2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 20:59 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:59
Completed NSE at 20:59, 0.00s elapsed
```

```
[root@warmachine]-[/]
#ls
bin      etc      initrd.img.old  lib64    mnt      nmap_results_2.nmap  nmap_results.nmap  proc  sbin  tmp  vmlinuz
boot    home     lib             libx32   nmap_results  nmap_results_2.xml  nmap_results.xml   root  srv   usr  vmlinuz.old
dev      initrd.img  lib32          media    nmap_results_2.gnmap  nmap_results.gnmap  opt      run   sys  var
```

Simple file

```
nmap_results_2.nmap x
1# Nmap 7.92 scan initiated Thu Jan 5 20:59:19 2023 as: nmap -sC -sV -v -oA /nmap_results_2 10.0.2.4
2Nmap scan report for 10.0.2.4
3Host is up (0.010s latency).
4Not shown: 977 closed tcp ports (reset)
5PORT      STATE SERVICE      VERSION
621/tcp    open  ftp          vsftpd 2.3.4
7| ftp-syst:
8|   STAT:
9|   FTP server status:
10|    Connected to 10.0.2.15
11|    Logged in as ftp
12|    TYPE: ASCII
13|    No session bandwidth limit
14|    Session timeout in seconds is 300
15|    Control connection is plain text
16|    Data connections will be plain text
17|    vsFTPD 2.3.4 - secure, fast, stable
18|_End of status
19|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
2022/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
21| ssh-hostkey:
22|  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
23|  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
2423/tcp    open  telnet       Linux telnetd
2525/tcp    open  smtp         Postfix smtpd
26|_ssl-date: 2023-01-05T15:11:55+00:00; -17m52s from scanner time.
27|_sslv2:
28|   SSLv2 supported
29|   ciphers:
30|     SSL2_RC4_128_WITH_MD5
31|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
32|     SSL2_RC4_128_EXPORT40_WITH_MD5
33|     SSL2_RC2_128_CBC_WITH_MD5
34|     SSL2_DES_192_EDE3_CBC_WITH_MD5
35|     SSL2_DES_64_CBC_WITH_MD5
36|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```


Xml file

```
1<?xml version="1.0" encoding="UTF-8"?>
2<!DOCTYPE nmaprun>
3<?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="text/xsl"?>
4<!-- Nmap 7.92 scan initiated Thu Jan 5 20:59:19 2023 as: nmap -sC -sV -v -oA /nmap_results_2 10.0.2.4 -->
5<nmaprun scanner="nmap" args="nmap -sC -sV -v -oA /nmap_results_2 10.0.2.4" start="1672932559" startstr="Thu Jan 5 20:59:19 2023" version="7.92" xmloutputversion="1.05">
6<scaninfo type="syn" protocol="tcp" numservices="1000"
  services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,348,349,354,355,359,360,363,367,369,370,373,376,379,381,384,385,389,390,393,396,398,401,402,405,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000"/>
7<verbose level="1"/>
8<debugging level="0"/>
9<taskbegin task="NSE" time="1672932560"/>
10<taskend task="NSE" time="1672932560"/>
11<taskbegin task="NSE" time="1672932560"/>
12<taskend task="NSE" time="1672932560"/>
13<taskbegin task="NSE" time="1672932560"/>
14<taskend task="NSE" time="1672932560"/>
15<taskbegin task="ARP Ping Scan" time="1672932560"/>
16<hosthint><status state="up" reason="arp-response" reason_ttl="0"/>
17<address addr="10.0.2.4" addrtype="ipv4"/>
18<address addr="08:00:27:6C:25:8E" addrtype="mac" vendor="Oracle VirtualBox virtual NIC"/>
19<hostnames>
20</hostnames>
21</hosthint>
22<taskend task="ARP Ping Scan" time="1672932560" extrainfo="1 total hosts"/>
23<taskbegin task="Parallel DNS resolution of 1 host." time="1672932560"/>
24<taskend task="Parallel DNS resolution of 1 host." time="1672932560"/>
25<taskbegin task="SYN Stealth Scan" time="1672932560"/>
26<taskend task="SYN Stealth Scan" time="1672932562" extrainfo="1000 total ports"/>
27<taskbegin task="Service scan" time="1672932562"/>
28<taskend task="Service scan" time="1672932574" extrainfo="23 services on 1 host"/>
29<taskbegin task="NSE" time="1672932574"/>
30<taskend task="NSE" time="1672932587"/>
31<taskbegin task="NSE" time="1672932587"/>
32<taskend task="NSE" time="1672932589"/>
33<taskbegin task="NSE" time="1672932589"/>
```

Gnmap file

```
1# Nmap 7.92 scan initiated Thu Jan 5 20:59:19 2023 as: nmap -sC -sV -v -oA /nmap_results_2 10.0.2.4
2# Ports scanned:
TCP(1000):1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,360,363,367,369,370,373,376,379,381,384,385,389,390,393,396,398,401,402,405,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000
UDP(0): SCTP(0): PROTOCOLS(0)
3Host: 10.0.2.4 () Status: Up
4Host: 10.0.2.4 () Ports: 21/open/tcp//ftp//vsftpd 2.3.4/, 22/open/tcp//ssh//OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)/, 23/open/tcp//telnet//Linux telnetd/, 25/open/tcp//smtp//Postfix smtpd/, 53/open/tcp//domain//ISC BIND 9.4.2/, 80/open/tcp//http//Apache httpd 2.2.8 (Ubuntu) DAV[2]/, 111/open/tcp//rpcbind//2 (RPC #100000)/, 139/open/tcp//netbios-ssn//Samba smbd 3.X - 4.X (workgroup: WORKGROUP)/, 445/open/tcp//netbios-ssn//Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)/, 512/open/tcp//exec//netkit-rsh rexecd/, 513/open/tcp//login?///, 514/open/tcp//tcpwrapped///, 1099/open/tcp//java-rmi//GNU Classpath grmiregistry/, 1524/open/tcp//bindshell//Metasploitable root shell/, 2049/open/tcp//nfs//2.4 (RPC #100003)/, 2121/open/tcp//ftp//ProFTPD 1.3.1/, 3306/open/tcp//mysql//MySQL 5.0.51a-3ubuntu5/, 5432/open/tcp//postgresql//PostgreSQL DB 8.3.0 - 8.3.7/, 5900/open/tcp//vnc//VNC (protocol 3.3)/, 6000/open/tcp//X11// (access denied)/, 6667/open/tcp//irc//UnrealIRCd/, 8009/open/tcp//ajp13//Apache Jserv (Protocol v1.3)/, 8180/open/tcp//http//Apache Tomcat[Coyote JSP engine 1.1/ Ignored State: closed (977)]
5# Nmap done at Thu Jan 5 20:59:49 2023 -- 1 IP address (1 host up) scanned in 29.75 seconds
```

- The out-of-the-network scanning and device discovery tools on the web page hosted on the Apache2 server

```
(root@kali)-[/]
# nmap -sV -sC -A 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 21:45 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.53 ((Debian))
|_ http-server-header: Apache/2.4.53 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
3306/tcp  open  mysql     MySQL 5.5.5-10.6.7-MariaDB-3
mysql-info:
|_ Protocol: 10
|_ Version: 5.5.5-10.6.7-MariaDB-3
|_ Thread ID: 37
|_ Capabilities flags: 63486
|_ Some Capabilities: InteractiveClient, IgnoreSpaceBeforeParenthesis, Support41Auth, Speaks41ProtocolOld, SupportsCompression, SupportsTransactions, IgnoreS
|_ gpipes, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, ODBCClient, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag, FoundRows, SupportsMultipl
|_ eResults, SupportsMultipleStatements, SupportsAuthPlugins
|_ Status: Autocommit
|_ Salt: yj+3^_Ds9^QZNZW(^,WQ
|_ Auth Plugin Name: mysql_native_password
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

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 10.62 seconds
```

- Automate the process of embedding the network scanning and device discovery output result into the active web page.

Open browser and visit your nmap result file

```
Kali Linux x 127.0.0.1/DVWA/nmap.txt x +
127.0.0.1/DVWA/nmap.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 09:10 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.53 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.53 (Debian)
3306/tcp  open  mysql     MySQL 5.5.5-10.6.7-MariaDB-3
mysql-info:
|_ Protocol: 10
|_ Version: 5.5.5-10.6.7-MariaDB-3
|_ Thread ID: 48
|_ Capabilities flags: 63486
|_ Some Capabilities: FoundRows, Support41Auth, SupportsCompression, Speaks41ProtocolOld, IgnoreSgipipes, SupportsTransactions, ODBCClient, InteractiveClient, LongColumnFlag, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, SupportsLoadDataLocal,
|_ ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsAuthPlugins, SupportsMultipleStatements, SupportMultipleResults
|_ Status: Autocommit
|_ Salt: ossg+9p9k.Bm4d49
|_ Auth Plugin Name: mysql_native_password
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

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 8.43 seconds
```


- **Access the webpage within the network with the result of network scanning and device discovery updated every 10 minutes with the time stamp**

We can achieve automation using crontab in linux

Crontab

Commands: crontab -l

Crontab -e

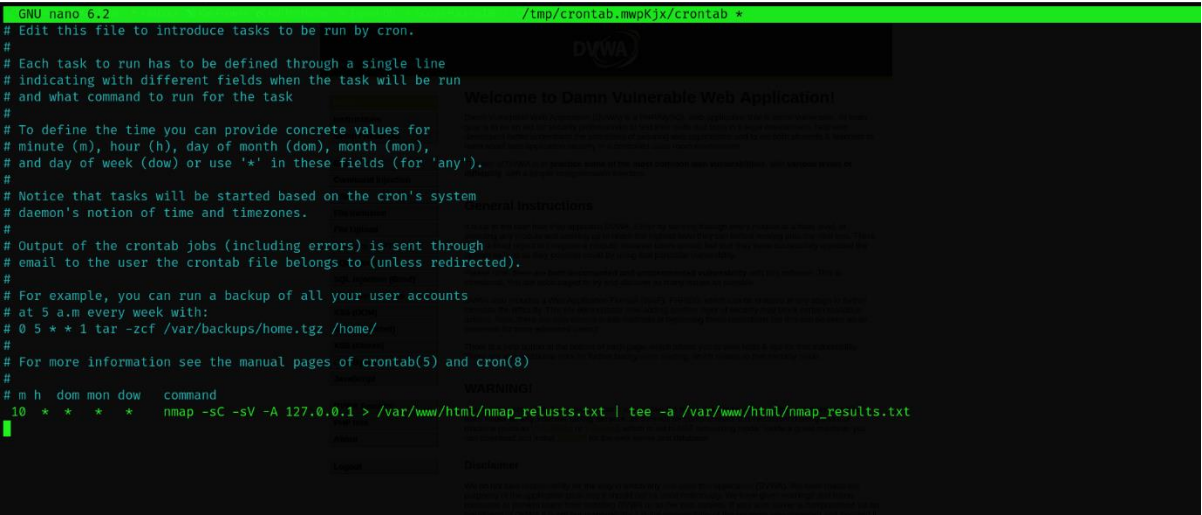
Crontab -e for crating new task

```
(root@kali)-[/]  
# crontab -e
```

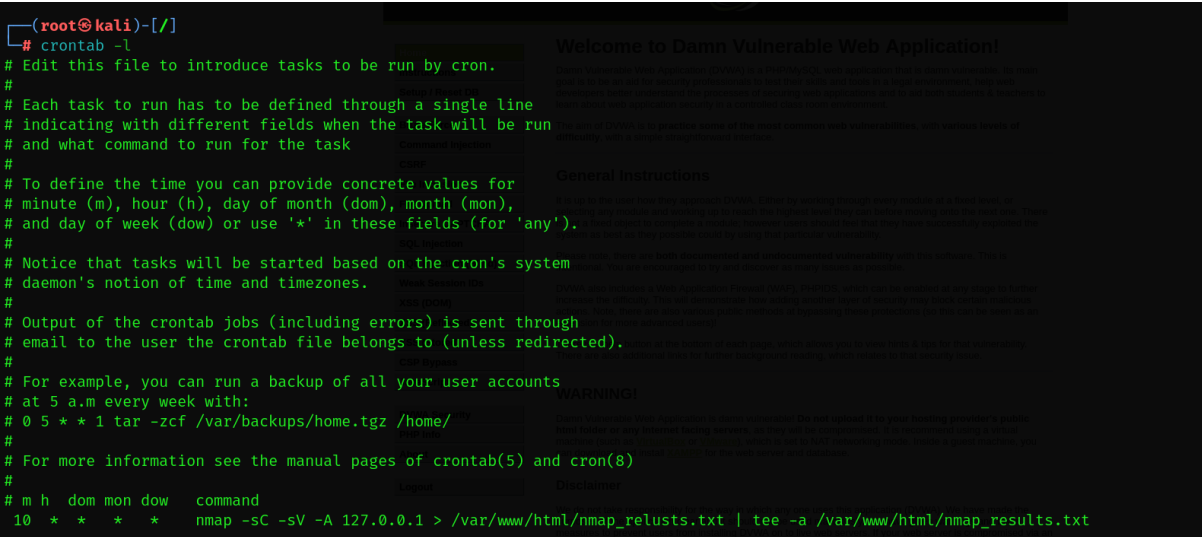
m(minute), h(hour), dom (day of month),mon (month),
dow(day of weak)

command:

```
nmap -sC -sV -A 127.0.0.1 > /var/www/html/nmap_results.txt | tee -a /var/www/html/nmap_results.txt
```



List of crontab



Crontab installing...


```
(root@kali)-[/]
# crontab -e
crontab: installing new crontab
```

Output:

```
(root@kali)-[/var/www/html]
# ls
DVWA index.html index.nginx-debian.html nmap_relusts.txt nmap_results.txt

(root@kali)-[/var/www/html]
# cat nmap_relusts.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-06 09:10 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000056s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.53 ((Debian))
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.53 (Debian)
3306/tcp  open  mysql     MySQL 5.5.5-10.6.7-MariaDB-3
|_ mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.6.7-MariaDB-3
|   Thread ID: 46
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, Support41Auth, SupportsCompression, Speaks41ProtocolOld, IgnoreSigpipes, SupportsTransactions, ODBCClient,
adDataLocal, ConnectWithDatabase, IgnoreSpaceBeforeParenthesis, SupportsAuthPlugins, SupportsMultipleStatements, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ossg+97p9k.BBaEs4FD
|_ Auth Plugin Name: mysql_native_password
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

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 8.43 seconds
```



Welcome to Damn Vulnerable W

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is intended to be used by security professionals to test their skills and developers better understand the processes of securing web applications. It is a controlled class room environment.

The aim of DVWA is to practice some of the most common web application security issues, with a simple straightforward interface.

General Instructions

Please note, there are both documented and undocumented vulnerabilities. You are encouraged to try and discover as many issues as you can. DVWA also includes a Web Application Firewall (WAF), PHPIDS, and a CAPTCHA to increase the difficulty. This will demonstrate how adding another layer of security can make a system more difficult to exploit. Note, there are also various public methods of bypassing these security measures (for more advanced users).

There is a help button at the bottom of each page, which allows you to view the help text.