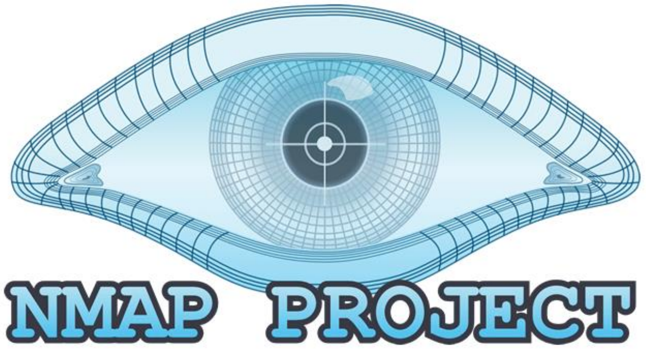
Experiment : **Website Penetration Testing Using "NMap" Tool in Kali Linux.**

Required Equipment:

- Computer/Laptop.
- Internet Connection.
- Kali Linux Operating System.
- NMap Tool.
- Metasploitable Tool.

Features Included:

- **Acclaimed:** Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details.
- **Well Documented:** Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- **Flexible:** Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.
- **Powerful:** Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- **Portable:** Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.



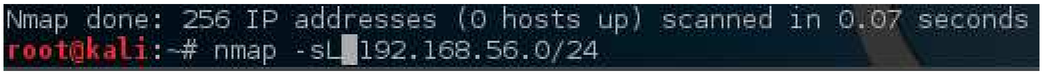
Experiment:

the whole experiment process described below with screenshots step by step……..

Step 1: Finding Live Hosts on My Network:

In this example, both of the machines are on a private **192.168.56.0 /24** network. The Kali machine has an IP address of **192.168.56.101** and the Metasploitable machine to be scanned has an IP address of **192.168.56.102**.

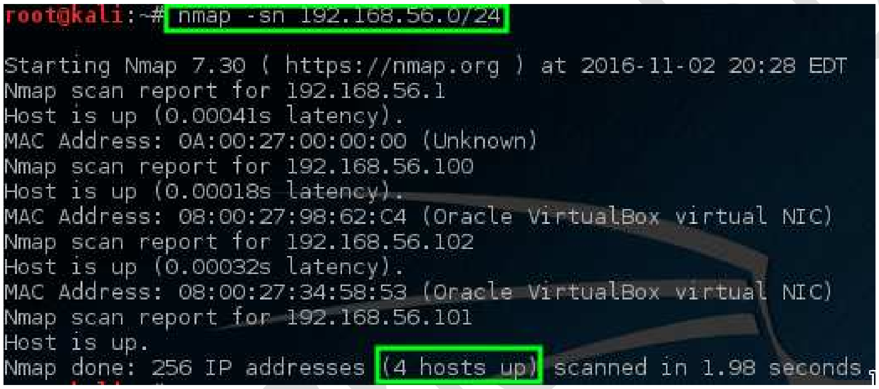
Let’s say though that the IP address information was unavailable. A quick nmap scan can help to determine what is live on a particular network. This scan is known as a ‘**Simple List**’ scan hence the -sL arguments passed to the nmap command.: nmap –sL 192.168.56.0/24



```
Nmap done: 256 IP addresses (0 hosts up) scanned in 0.07 seconds
root@kali:~# nmap -sL 192.168.56.0/24
```

Step 2: Finding and Pinging All Live Hosts on My Network:

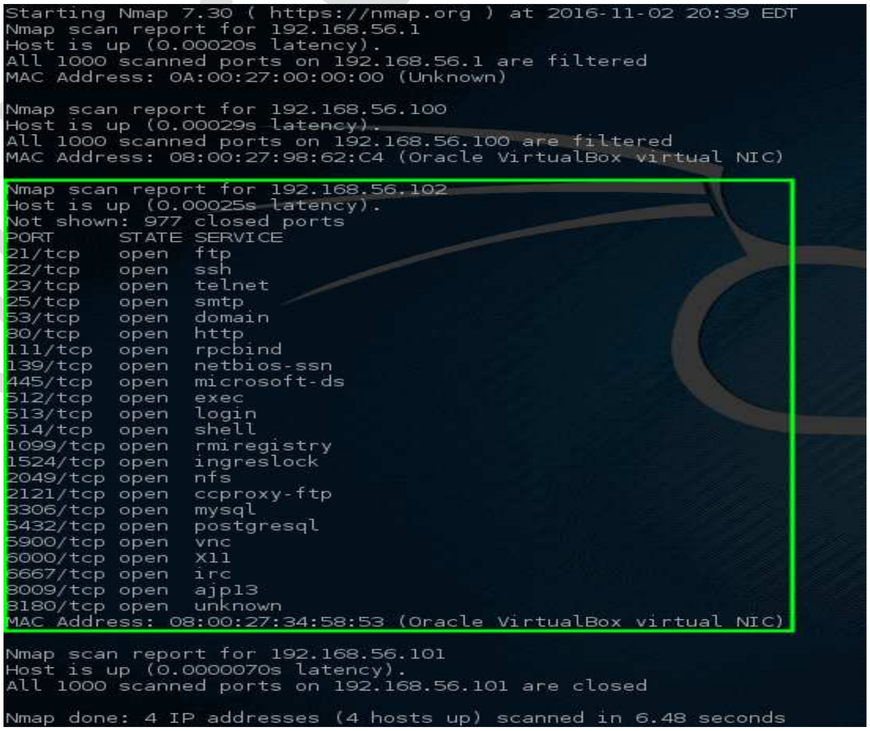
there are some tricks that nmap has available to try to find these machines. This next trick will tell nmap to simply try to ping all the addresses in the **192.168.56.0/24** network. This time nmap returns some prospective hosts for scanning! In this command, the -sn disables nmap’s default behavior of attempting to port scan a host and simply has nmap try to ping the host. Using Comman: nmap –sn 192.168.56.0/24



```
root@kali:~# nmap -sn 192.168.56.0/24

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:28 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00041s latency).
MAC Address: 0A:00:27:00:00:00 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00018s latency).
MAC Address: 08:00:27:98:62:C4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00032s latency).
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.98 seconds
```

Step 3: Find Open Ports on Hosts:

Let’s try letting nmap port scan these specific hosts and see what turns up. Command: # nmap 192.168.56.1,100-102



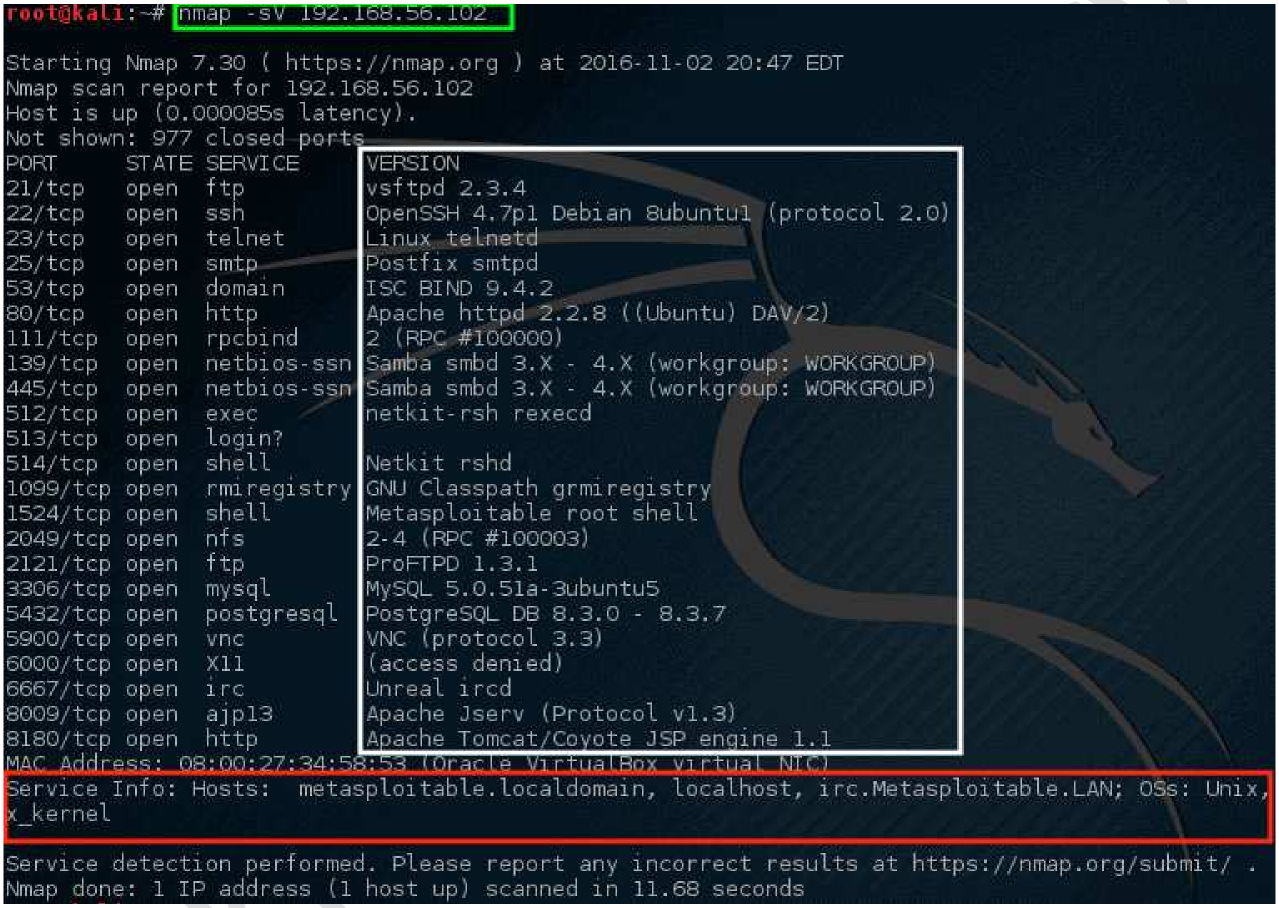
```
Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:39 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.56.1 are filtered
MAC Address: 0A:00:27:00:00:00 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:98:62:C4 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00025s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.56.101 are closed

Nmap done: 4 IP addresses (4 hosts up) scanned in 6.48 seconds
```

These ports all indicate some sort of listening service on this particular machine. Recalling from earlier, the 192.168.56.102 IP address is assigned to the metasploitable vulnerable machine hence why there are so many open ports on this host.

Step 4: Finding Services Listening on Ports on Hosts:

This next scan is a service scan and is often used to try to determine what service may be listening on a particular port on a machine.

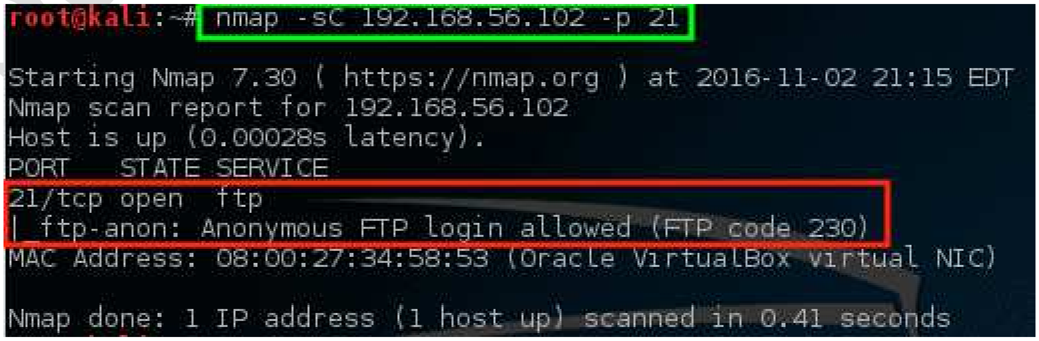
Nmap will probe all of the open ports and attempt to banner grab information from the services running on each port. Command Used: # nmap -sV 192.168.56.102



```
root@kali:~# nmap -sV 192.168.56.102

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:47 EDT
Nmap scan report for 192.168.56.102
Host is up (0.000085s latency).
Not shown: 977 closed 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?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       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         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, 
x_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds
```

Step 5: Find Anonymous FTP Logins on Hosts:

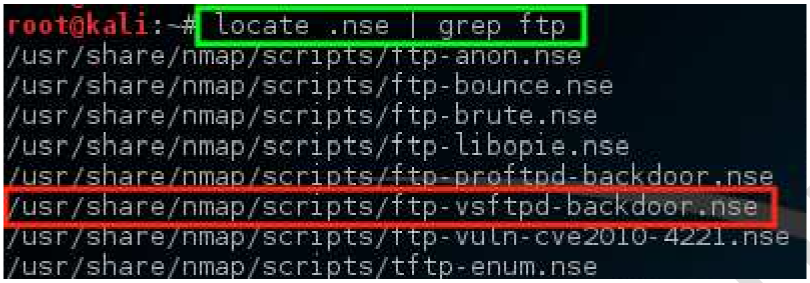
Command Used: # nmap -sC 192.168.56.102 -p 21



```
root@kali:~# nmap -sC 192.168.56.102 -p 21

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 21:15 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00028s latency).
PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

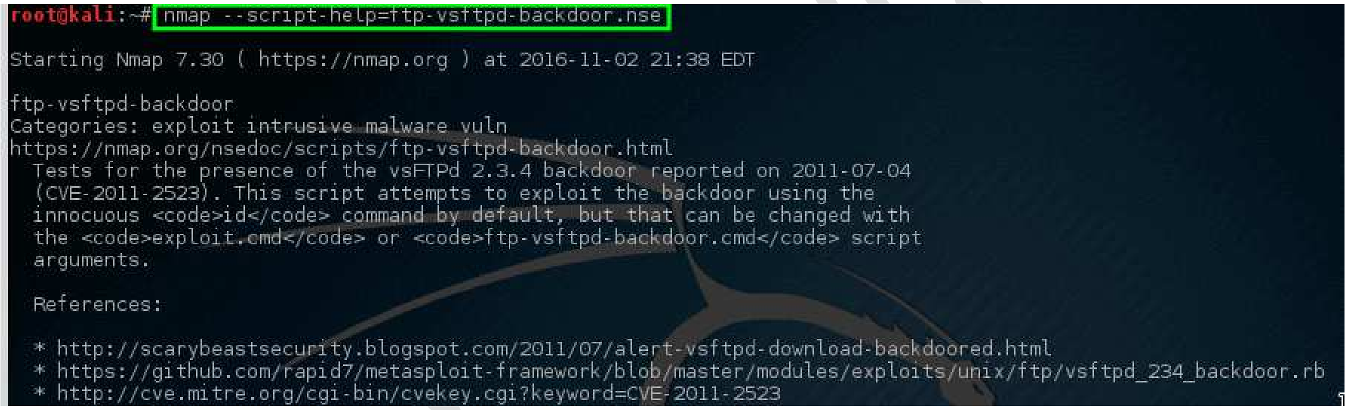
Step 6: Check for Vulnerabilities on Hosts:

This paired with the earlier knowledge about VSftd having an old vulnerability should raise some concern though. Let’s see if nmap has any scripts that attempt to check for the VSftpd vulnerability.
Command Used: # locate .nse | grep ftp



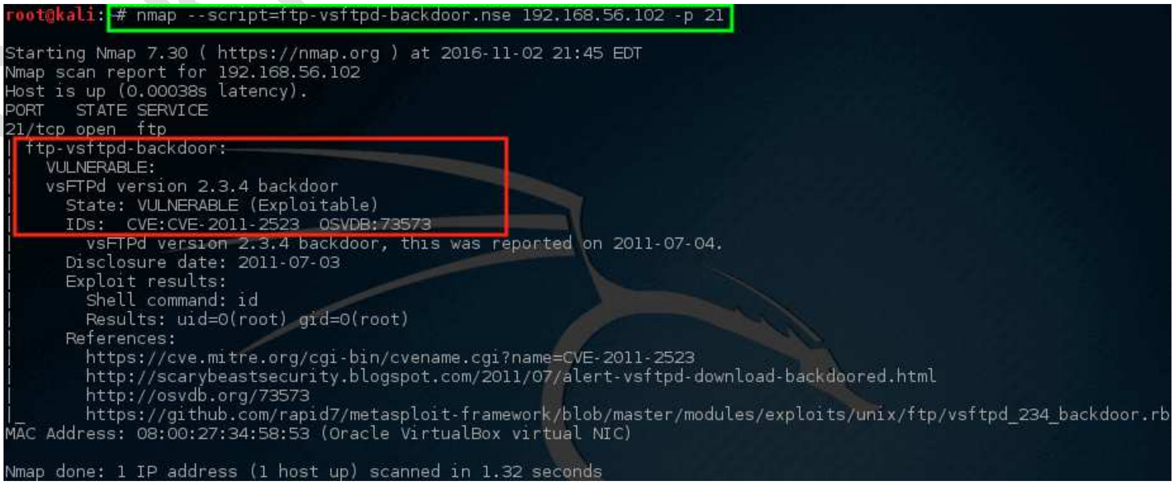
```
root@kali:~# locate .nse | grep ftp
/usr/share/nmap/scripts/ftp-anon.nse
/usr/share/nmap/scripts/ftp-bounce.nse
/usr/share/nmap/scripts/ftp-brute.nse
/usr/share/nmap/scripts/ftp-libopie.nse
/usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
/usr/share/nmap/scripts/tftp-enum.nse
```

Notice that nmap has a **NSE** script already built for the VSftpd backdoor problem! Let’s try running this script against this host and see what happens but first it may be important to know how to use the script.
Command Used: # nmap --script-help=ftp-vsftd-backdoor.nse



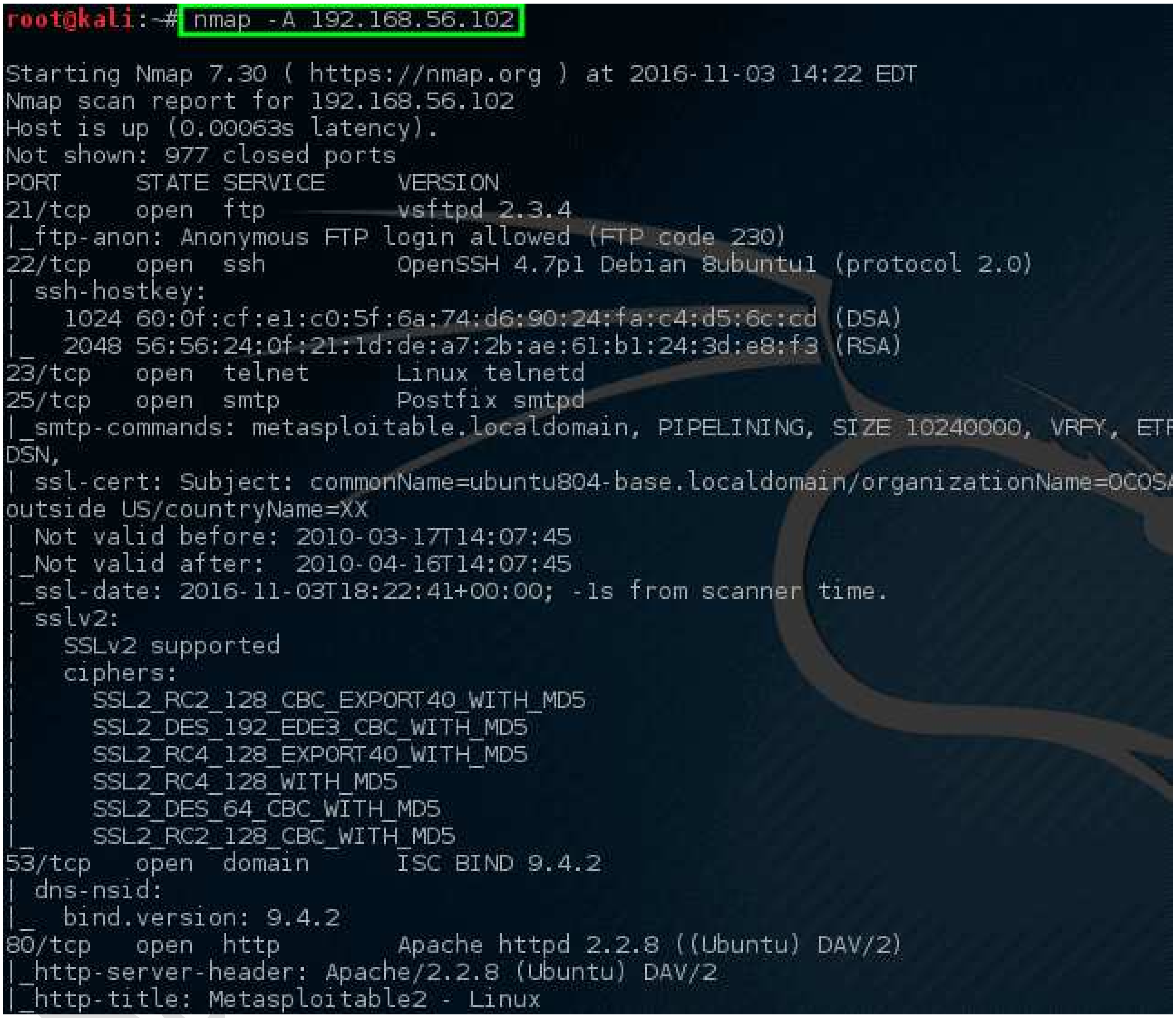
```
root@kali:~# nmap --script-help=ftp-vsftpd-backdoor.nse

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 21:38 EDT

ftp-vsftpd-backdoor
Categories: exploit intrusive malware vuln
https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html
  Tests for the presence of the vsFTPd 2.3.4 backdoor reported on 2011-07-04
  (CVE-2011-2523). This script attempts to exploit the backdoor using the
  innocuous <code>id</code> command by default, but that can be changed with
  the <code>exploit.cmd</code> or <code>ftp-vsftpd-backdoor.cmd</code> script
  arguments.

  References:

  * http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
  * https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
  * http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2011-2523
```

Reading through this description, it is clear that this script can be used to attempt to see if this particular machine is vulnerable to **ExploitDB** issue identified earlier.
Let’s run the script and see what happens.
Command used: # nmap --script=ftp-vsftpd-backdoor.nse 192.168.56.102 -p 21



```
root@kali:~# nmap --script=ftp-vsftpd-backdoor.nse 192.168.56.102 -p 21

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 21:45 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00038s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  OSVDB:73573
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       http://osvdb.org/73573
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

Nmap's script returned some dangerous news. This machine is likely a good candidate for a serious investigation. This doesn't mean that the machine is compromised and being used for horrible/terrible things but it should bring some concerns to the network/security teams.
Nmap has the ability to do a much more aggressive scan that will often yield much of the same information but in one command instead of several. Let's take a look at the output of an aggressive scan.
Command used: # nmap -A 192.168.56.102



```
root@kali:~# nmap -A 192.168.56.102

Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-03 14:22 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00063s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETR
DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2016-11-03T18:22:41+00:00; -1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
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
```

Notice this time, with one command, nmap has returned a lot of the information it returned earlier about the open ports, services, and configurations running on this particular machine. Much of this information can be used to help determine how to protect this machine as well as to evaluate what software may be on a network. This was just a short, short list of the many useful things that nmap can be used to find on a host or network segment. It is strongly urged that individuals continue to experiment with nmap in a controlled manner on a network that is owned by the individual

Commands Used In This Experiment:

```
kali> nmap –sL 192.168.56.0/24
kali> nmap –sn 192.168.56.0/24
kali> nmap 192.168.56.1,100-102
kali> nmap -sV 192.168.56.102
kali> nmap -sC 192.168.56.102 -p 21
kali> locate .nse | grep ftp
kali> nmap --script-help=ftp-vsftd-backdoor.nse
kali> nmap --script=ftp-vsftpd-backdoor.nse 192.168.56.102 -p 21
kali> nmap -A 192.168.56.102
```

Website Used In This Experiment:

Http:// 192.168.56.102

Discussion:

- Internet Connection should be Okay.
- We should not practice by scanning other entities**.**
- Nmap commands should be appropriate and logical.
- We must need to use manual proxy to check vulnerability of websites or web applications.

Sakkar Chowdhury