

IDS Module 1 Lab
Audrey Long
05/30/2020

1. Risks, Attacks and Observables

1. In two paragraphs or less, discuss the relationship between “risk” and “attack” as discussed in the lecture videos.

Essentially, according to the lectures an attack is an instance of a threat attempting to exploit an exposed vulnerability to compromise a protected asset. Incident is an indication of an attack either directly/indirectly and is a result of an attack which cannot be directly measured or observed, but incidents contain observable parts of an attack. Risk is a relationship between frequency which is the expected number of incidents per unit time and severity, being the expected damage based on an incident that was not mitigated. of an attack.

2. Give 3 or more concrete examples of “observables”.

Observables are evidence of the aftermath or real time observation of an attack. In general observables are artifacts that can be analyzed and deconstructed. Some examples are observables are Hash values from a file or key, a file is added or deleted, a restful API web request such as GET, ADD, DELETE has been received or an intrusion detection rule has been triggered.

2. Linux Warm-Up

This step will serve as a small Linux “warm-up”. On your Ubuntu VM, run the following commands and explain their output and what they accomplish. Please provide screenshots of your results.

1. which vim

```
student@student:~$ which vim
/usr/bin/vim
student@student:~$
```

This command returns the pathname of the files which would be executed in the current environment. This command searches the path for executable filenames matching the names of their POSIX arguments.

2. cat /etc/network/interfaces

```
student@student:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback
student@student:~$
```

This command concatenates files to a standard output and displays file contents to the screen.

3. apt-get install nmap

```
The following NEW packages will be installed:
liblinear3 nmap
0 upgraded, 2 newly installed, 0 to remove and 559 not upgraded.
Need to get 5,213 kB of archives.
After this operation, 24.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 liblinear3 amd64 2.
0-dfsg-2 [39.3 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 nmap amd64 7.60-1ub
ntu5 [5,174 kB]
Fetched 5,213 kB in 1s (4,733 kB/s)
Selecting previously unselected package liblinear3:amd64.
(Reading database ... 164149 files and directories currently installed.)
Preparing to unpack .../liblinear3_2.1.0-dfsg-2_amd64.deb ...
Unpacking liblinear3:amd64 (2.1.0-dfsg-2) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.60-1ubuntu5_amd64.deb ...
Unpacking nmap (7.60-1ubuntu5) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Setting up liblinear3:amd64 (2.1.0-dfsg-2) ...
Setting up nmap (7.60-1ubuntu5) ...
Processing triggers for libc-bin (2.27-3ubuntu1) ...
student@student:~$
```

This command installed the nmap package to the VM.

4. ls -l /tmp

```
student@student:~$ ls -l /tmp
total 28
-rw-r--r-- 1 student student 0 May 30 10:14 config-err-1cc53L
drwx-r--r-- 2 student student 4096 May 30 10:14 ssh-3LYP2ARZj8xA
drwx-r--r-- 3 root root 4096 May 30 10:14 system-private-65b47d1dea3f4b718
9926ba284bd2975-bolt.service-4FPdbc
drwx-r--r-- 3 root root 4096 May 30 10:14 system-private-65b47d1dea3f4b718
9926ba284bd2975-color.service-CrVall
drwx-r--r-- 3 root root 4096 May 30 10:14 system-private-65b47d1dea3f4b718
9926ba284bd2975-fwupd.service-bont5j
drwx-r--r-- 3 root root 4096 May 30 10:14 system-private-65b47d1dea3f4b718
9926ba284bd2975-rtkit-daemon.service-Hs3Nrc
drwx-r--r-- 3 root root 4096 May 30 10:14 system-private-65b47d1dea3f4b718
9926ba284bd2975-systemd-resolved.service-107Wb3
drwx-r--r-- 3 root root 4096 May 30 10:14 system-private-65b47d1dea3f4b718
9926ba284bd2975-systemd-timesyncd.service-kYhspc
student@student:~$
```

The ls command lists information about files alphabetically, the argument -l uses a long list format. Thus above we are displaying all information in the /tmp folder in a long listen format.

5. Mount

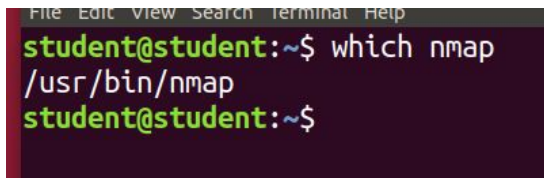
```
coredump on /sys/kernel/debug/coredump type cgroup rw,nosuid,nodev,noexec,relatime,cgroup
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relative,fds=24,pgp=1,timeouts=0,nlproto=5,nmapproto=5,direct
pipe-lto=12748)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relative,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,relative)
squashfs on /dev/mqueue type mqueue (rw,relative)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relative)
configfs on /sys/kernel/config type configfs (rw,relative)
/var/lib/snapd/snap/gnome-logs_100.snap on /snap/gnome-logs/100 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-system-monitor_37.snap on /snap/gnome-system-monitor/37 type squashfs (ro,nodev,relative
,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-3-26-1604_70.snap on /snap/gnome-3-26-1604/70 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/core_6259.snap on /snap/core/6259 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-3-26-1604_100.snap on /snap/gnome-3-26-1604/100 type squashfs (ro,nodev,relative,x-gdu.h
ide)
/var/lib/snapd/snap/gtk-common-themes_319.snap on /snap/gtk-common-themes/319 type squashfs (ro,nodev,relative,x-g
du.hid
e)
/var/lib/snapd/snap/gnome-3-34-1804_33.snap on /snap/gnome-3-34-1804/33 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-calculator_748.snap on /snap/gnome-calculator/748 type squashfs (ro,nodev,relative,x-gd
u.hid
e)
/var/lib/snapd/snap/gnome-system-monitor_145.snap on /snap/gnome-system-monitor/145 type squashfs (ro,nodev,relat
ive,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-calculator_180.snap on /snap/gnome-calculator/180 type squashfs (ro,nodev,relative,x-gd
u.hid
e)
/var/lib/snapd/snap/gtk-common-themes_1586.snap on /snap/gtk-common-themes/1586 type squashfs (ro,nodev,relative,x
-gdu.hid
e)
/var/lib/snapd/snap/core_6130.snap on /snap/core/6130 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-characters_539.snap on /snap/gnome-characters/539 type squashfs (ro,nodev,relative,x-gd
u.hid
e)
/var/lib/snapd/snap/gnome-characters_139.snap on /snap/gnome-characters/139 type squashfs (ro,nodev,relative,x-gd
u.hid
e)
/var/lib/snapd/snap/gnome-3-26-1604_74.snap on /snap/gnome-3-26-1604/74 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-logs_45.snap on /snap/gnome-logs/45 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-calculator_260.snap on /snap/gnome-calculator/260 type squashfs (ro,nodev,relative,x-gd
u.hid
e)
/var/lib/snapd/snap/gnome-logs_37.snap on /snap/gnome-logs/37 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/gtk-common-themes_818.snap on /snap/gtk-common-themes/818 type squashfs (ro,nodev,relative,x-g
du.hid
e)
/var/lib/snapd/snap/gnome-system-monitor_51.snap on /snap/gnome-system-monitor/51 type squashfs (ro,nodev,relative
,x-gdu.hid
e)
/var/lib/snapd/snap/gnome-characters_183.snap on /snap/gnome-characters/183 type squashfs (ro,nodev,relative,x-gd
u.hid
e)
/var/lib/snapd/snap/core_9866.snap on /snap/core/9866 type squashfs (ro,nodev,relative,x-gdu.hid
e)
/var/lib/snapd/snap/core18_1754.snap on /snap/core18/1754 type squashfs (ro,nodev,relative,x-gdu.hid
e)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relative,size=284188k,mode=700,uid=1000,gid=1000)
gfsd-fuse on /run/user/2000/gfs type fuse.gfsd-fuse (rw,nosuid,nodev,relative,user_id=1000,group_id=1000)
student@student:~$
```

This command prints all files which are accessible in a Unix system which are then arranged in a tree structure with the file hierarchy starting at the root node. The mount command specifically serves to attach the file system found on the device to the file tree.

3. Nmap – Network Mapper

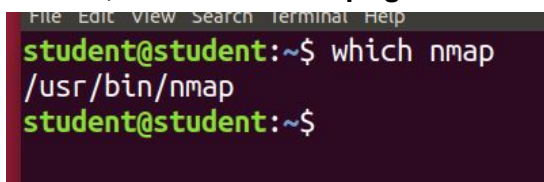
Complete each of the following steps (on your Ubuntu VM, setup instructions are under Module 1 in Blackboard) and provide answers for the questions listed. Where applicable, please provide screenshots of your outputs.

1. Use the “which” command to see if NMAP is currently installed on your system. Is it?



```
File Edit View Search Terminal Help
student@student:~$ which nmap
/usr/bin/nmap
student@student:~$
```

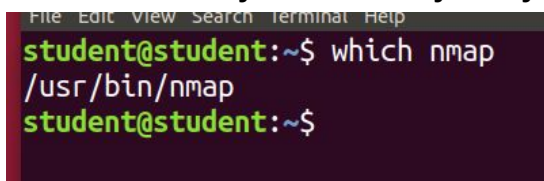
2. If not, install it: `sudo apt-get install nmap` (user: student, password: student)



```
File Edit View Search Terminal Help
student@student:~$ which nmap
/usr/bin/nmap
student@student:~$
```

3. Verify NMAP was installed successfully: which nmap item Use the “which” command to see if

NMAP is currently installed on your system. Is it?



```
File Edit View Search Terminal Help
student@student:~$ which nmap
/usr/bin/nmap
student@student:~$
```

Please answer the following questions and provide screenshots of your outputs. You can safely run your commands against the servers at: scanme.nmap.org

1. What is “heavy scanning” and why is it considered a potential threat on the internet?

Heavy scanning essentially points to vigorously scanning a network or system of networks for multiple vulnerabilities such as open ports, patch vulnerabilities, insecure passwords, and other vulnerabilities contained in a network environment to be presented to a bad actor as potential opportunities to exploit a system. Heavy scanning is considered a potential threat of the internet because developers generally do not create secure applications, instead they mostly focus on functionality, therefore heavily scanning can provide multiple avenues for bad actors to exploit systems. Heavy scanning provides a means for more information being gathered to put together a plan of obtaining the information or takeover of a system from a bad actor.

2. Provide the command for using NMAP to scan all reserved TCP ports on a target host. Execute your command on the address above.

```

student@student:~$ nmap -v scanme.nmap.org
Starting Nmap 7.60 ( https://nmap.org ) at 2020-05-30 12:05 EDT
Initiating Ping Scan at 12:05
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 12:05, 3.00s elapsed (1 total hosts)
Nmap scan report for scanme.nmap.org (45.33.32.156) [host down]
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
student@student:~$

```

The command `<nmap -v scanme.nmap.org>` was used to scan all reserved TCP ports on the domain provided. The argument `-v` displays the information in a verbose manner.

3. What is “OS fingerprinting” and what NMAP command can be used to perform it? Execute your command on the address above. Which OS do you think the server is running?

According to the nmap documentation one of Nmaps widely known functions is the ability to remote OS detect using TCP/IP stack fingerprinting where the nmap command sends out a series of TCP and UDP packets to the remote host and examines practically every bit in the response. After a large sample has been obtained nmap compares the data against its database with over 2,600 known OS fingerprints and prints out details about the OS if any match has been hit. Some of the information obtained can include vendor names, operating systems being used, the generations of the OS, device type, and common platform enumeration among other information such as the last time the OS was rebooted. From the OS command provided below It seems there is a 97% chance the OS is Oracle VirtualBox

```

student@student:~$ sudo nmap -O scanme.nmap.org
[sudo] password for student:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-05-30 12:22 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.041s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 937 filtered ports, 59 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.95 seconds

```

4. Think of 2 different scans that might be interesting that have not already been mentioned. Tell why they are interesting from a security perspective, write the commands and perform them, and execute them against the address above. Please provide screenshots and an explanation of your results.

The command `<name -A -T4 -F scanme.nmap.org>` The “-A” argument enables OS detection, version detection, script scanning, and traceroute. The “-T4” argument is for the speed template which tells nmap how quickly to perform the scan (range from 0 - 5). The “-F” argument tells nmap to scan 100 of the most common ports. The results below show the following information we did not see with the previous scans such as the version of SSH used on the virtual machine along with the ssh-hostkey and encryption algorithm associated with the finding. This command also shows the port 80 is open along with the version and Apache service on http along with a traceroute using the common port 80 along with the address and version.

```
student@student:~$ sudo nmap -A -T4 -F scanme.nmap.org
Starting Nmap 7.60 ( https://nmap.org ) at 2020-05-30 12:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.013s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 98 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (EdDSA)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge[general purpose]
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.59 ms _gateway (10.0.2.2)
2 0.77 ms scanme.nmap.org (45.33.32.156)

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 17.66 seconds
```

The command `<nmap -sV scanme.nmap.org>` displays the information provided below. It is a standard service detection command. This command can also be given flags to do a more aggressive service detection scan for example `<--version-intensity 5>`. The screenshot below shows the standard version command which displays more information about the versions and services being used per open TCP port.


```
student@student:~$ sudo nmap -sV scanme.nmap.org

Starting Nmap 7.60 ( https://nmap.org ) at 2020-05-30 12:41 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.015s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 847 filtered ports, 149 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped

Service Info: OS: 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 35.51 seconds
student@student:~$
```

References:

<https://www.whatsupgold.com/blog/port-scanning-101-what-it-is-what-it-does>
<https://resources.infosecinstitute.com/must-know-os-fingerprinting/#gref>
<https://nmap.org/book/man-os-detection.html>
<https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts>