Assignment 2 – Offensive network security

Assignment reports must be submitted by ***Thursday, August 12, 2021****.*

Assignment Description

In this assignment you will carry out exercises related to lectures on offensive and defensive network security. You will use nmap to carry out reconnaissance and set up a firewall for defensive network features.

Assignment Requirements and Setup

You will need to use the Kali virtual machine in this assignment. If you have not downloaded and installed it yet, please check the "Assignment 0" document.

To Hand In

Answer the questions labelled "2-1", "2-2", etc.

1 Offensive network security

In this section we will carry out some network reconnaissance and attacks. **Please remember the ethical and legal considerations discussed in class. When running the scans and attacks in this section, be sure that you are directing them towards your computer/VM, and nowhere else. For extra safety, you can turn off your host computer's outgoing network connection to ensure your attack traffic remains between your VM and your computer.**

1.1 nmap scan

In this exercise you will use nmap to identify running services. You have a choice for what you scan: you can either scan the SEED VM from the Kali VM, or you can scan your own computer from itself. Scanning your own computer may yield some interesting information about what is running on your computer, but is slightly trickier because you will need to download and install nmap on your own computer (outside of the VMs). There are versions available for Windows, Mac, and Linux: `http://nmap.org/download.html`.

2-1. **[5 marks]** Using the nmap tool from inside your Kali Linux virtual machine, run a scan of your host computer to see which ports are open and which software is running on those ports.

This may seem a little confusing at first. VirtualBox has set up a simulated network between the Kali Linux virtual machine and your host computer. We are going to scan *from* the Kali Linux VM *to* the host computer that the VM is running on. You will need to find out the IP address that the Kali Linux VM uses to refer to the host computer – it is not the same as the IP address that the host computer uses to get out to the Internet. Open a command-line terminal on Kali Linux and type `traceroute google.com`. You should get something like this:

```
root@kali:~# traceroute google.com
traceroute to google.com (172.217.1.174), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.323 ms  0.254 ms  0.106 ms
 2  v1020-wn-rt.ns.uwaterloo.ca (10.20.0.1)  2.435 ms  2.443 ms  3.302 ms
 3  po42-40-wn-rt.ns.uwaterloo.ca (172.16.34.33)  3.533 ms  4.122 ms  4.049 ms
 4  v1055-wn-rt.ns.uwaterloo.ca (172.16.34.57)  3.977 ms  3.993 ms  3.904 ms
 5  po40-cn-rt-mc.ns.uwaterloo.ca (172.16.34.1)  4.270 ms  4.201 ms  4.343 ms
 6  te0-0-2-0-ext-rt-mc.ns.uwaterloo.ca (172.16.32.149)  5.714 ms  3.276 ms  3.592 ms
 7  unallocated-static.rogers.com (72.142.108.181)  4.040 ms  3.573 ms  3.858 ms
```

The IP address of the host computer is the address next to `_gateway`, in my example it was `10.0.2.2`.
Run the nmap scan against your host computer. Report at least 5 open ports, which application and versions were running on those 5 ports, and what the purposes of those applications are. Were any of the services unexpected/insecure/obsolete? If so, how can you disable them? If you scan your personal computer and it has less than 5 services, include additional results from scanning my website (www.douglas.stebila.ca) to get more results. Here is a database of assigned and typical port usages: `http://www.speedguide.net/ports.php` Include a screenshot of your nmap results to help us check them.

2 Defensive network security

In this section we will configure a firewall on the Kali Linux VM.

2.1 Egress filtering

We will set up egress filtering, to prevent certain types of outgoing connections. A network administrator might do this reduce the chance that their network will be used to launch attacks against others, or to prevent valuable data being exfiltrated.

In our example, we will prevent naive students from trying to enrol in or learn anything about an enemy university. Use `nslookup` to lookup the IP address for `mcmaster.ca`, then use the search box on `http://whois.arin.net/` to search for that IP address. Click on the link beside "Organization" then "Related networks" to see the IPv4 range(s) assigned to McMaster.

Recall from the lectures that `ufw` is a simple firewall program for Linux. Use `ufw` to deny outgoing access to this range of IP addresses. Take a look at the rule syntax section

of the ufw man page. You may find it helpful know the syntax to describe a range of IP addresses: `a.b.c.0/24` captures all addresses in the range `a.b.c.(0-255)`, and `a.b.0.0/16` captures all addresses in the range `a.b.(0-255).(0-255)`.

You will first need to install `ufw` on Kali Linux, by typing `apt install ufw` and then `ufw enable`.

2-2. **[2 marks]** What command did you use to prevent outgoing access to the target IP addresses? How did you confirm that your command was effective? You might need to `ufw reload` after making any changes to the rules.

Now we will set up one other firewall rule. This time we will set up a rule that presents any insecure outgoing web connections. Specifically, we want to deny all outgoing connections to port 80 (which you might recall was the port for HTTP).

2-3. **[2 marks]** What command did you use to prevent outgoing access for insecure web connections? How did you confirm that your command was effective – that it had that effect, and only that effect? You might need to `ufw reload` after making any changes to the rules.

Once you've completed the exercises involving egress filtering, disable the firewall, as we may need to access the services later: `ufw disable`.

2.2 Ingress filtering

At this point it would be natural for us to also set up ingress filtering in our firewall, to prevent external connections from reaching protected services on our computer. However, Kali Linux doesn't have any services running by default. It is possible to install a second Linux virtual machine that has services running on it, set up a virtual network connection between your Kali VM and the second VM, and then do nmap scans and firewall settings to see how ingress filtering works, but that is outside the scope of this module.

In general, ingress filtering is just the flip of egress filtering: our rules ban connections coming *in* rather than *out*. The rules we set up would be exactly like the rules in the egress filtering section, except with the keyword *in* rather than *out*. We could do this to filter out all traffic coming from a specific attacker (the network range of our enemy, McMaster University), or all traffic trying to reach a specific application (our private web server on port 80, or our SSH server on port 22, etc.).

With ingress filtering, it is common to ban all incoming traffic, and then add firewall rules allowing only the few applications we want.