Renato Campos

November 3, 2020

Cybersecurity HW#8

Network Vulnerability Assessment

Start-Of-Report

Phase 1: *"I'd like to Teach the World to `Ping`"*

- Determined the IPs for the Hollywood office and added them to a text file called `hollywoodIPs.txt` :

```
# hollywoodIPs.txt
15.199.95.91
15.199.94.91
11.199.158.91
167.172.144.11
11.199.141.91
```

- Ran `fping -f hollywoodIPs.txt` against the IP ranges in order to determine which IP is accepting connections over layer 3, the *Network* layer.

  It appears that `167.172.144.11` is accepting connections.

  The results of `fping -f hollywoodIPs.txt` are:

```
167.172.144.11 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable
```

- Determined the IPs for all Rock Star Corp servers and added them to a text file called `rockStarCorpIPs.txt` :

```
# rockStarCorpIPs.txt
12.205.151.91
15.199.151.91
```

```
15.199.158.91
15.199.141.91
15.199.131.91
15.199.121.91
15.199.111.91
15.199.100.91
15.199.99.91
15.199.98.91
15.199.97.91
15.199.96.91
15.199.95.91
15.199.94.91
11.199.158.91
167.172.144.11
11.199.141.91
11.199.131.91
11.199.121.91
11.199.111.91
11.199.100.91
11.199.99.91
11.199.98.91
```

- Ran `fping -f rockStarCorpIPs.txt` against the IP ranges in order to determine which IP is accepting connections over layer 3, the *Network* layer.

  It appears that `167.172.144.11` is again the only IP accepting connections.

  The results of `fping -f rockStarCorpIPs.txt` are:

```
167.172.144.11 is alive
12.205.151.91 is unreachable
15.199.151.91 is unreachable
15.199.158.91 is unreachable
15.199.141.91 is unreachable
15.199.131.91 is unreachable
15.199.121.91 is unreachable
15.199.111.91 is unreachable
15.199.100.91 is unreachable
15.199.99.91 is unreachable
15.199.98.91 is unreachable
15.199.97.91 is unreachable
15.199.96.91 is unreachable
15.199.95.91 is unreachable
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable
```

```
11.199.131.91 is unreachable
11.199.121.91 is unreachable
11.199.111.91 is unreachable
11.199.100.91 is unreachable
11.199.99.91 is unreachable
11.199.98.91 is unreachable
```

- **Migitation:** It is suggested that ports and services that are accepting incoming connections for the Hollywood IP, `167.172.144.11`, be analyzed and closed if the connection is unnecessary.

Phase 2: *"Some `Syn` for Nothin`"*

`SYN SCAN`

- Using `nmap` on the only IP accepting connections, `167.172.144.11`, we see the results below show the port number / TCP / UDP , the state of the port, and the service / protocol for the ports that are either open or filtered (stopped by a firewall). This scan operates on the *Transport* layer, or layer 4.
- Open ports:

  ```
  PORT    STATE    SERVICE
  22/tcp  open     ssh
  25/tcp  filtered smtp
  135/tcp filtered msrpc
  139/tcp filtered netbios-ssn
  445/tcp filtered microsoft-ds
  ```

- Closed ports not shown: `995 closed ports`.
- **Full Results:**

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-28 22:02 EDT
Nmap scan report for 167.172.144.11
Host is up (0.080s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 266.70 seconds
```

- **Analysis:**

    - It appears that the Hollywood IP, `167.172.144.11`, is accepting connections for *SSH*, *SMTP*, *MSRPC*, *NETBIOS-SSN*, and *MICROSOFT-DS* services.
    - With the correct credentials, a threat actor can gain shell access to `167.172.144.11` using *SSH* and potentially make administrative changes to the server. Likewise with *SMTP*, a threat actor could upload a potentially harmful file into the server.
- **Mitigation:**
    - Do not create or use accounts with username/password combinitions that are easily recognizable or part of popular culture. Moreover, it is highly recommended that passwords follow a particular characteristic scheme to keep authentication and privacy secure.
    - **If** *SSH* or *SMTP* are absolutely necessary, it would be best to host these services on ports that are not the default values for the services. Else, these ports should be closed.

Phase 3: *"I Feel a `DNS` Change Comin' On"*

With the findings from Phase 2, we can access the Hollywood server (`167.172.144.11`) that is accepting connections through *SSH* (using the default port, 22).

- The default RockStar username and password are:
    - **Username:** `jimi`
    - **Password:** `hendrix`
- Using these credentials above, a successful attempt was made to *SSH* into the Hollywood server using: `ssh jimi@167.172.144.11 -p 22` .

  (*Note*: *A terminal with a different default SSH port was used, so this is why the port is particularly specifed here.*)

Due to the fact that RockStar Corp is reporting that they are unable to access `rollingstone.com` in the Hollywood office, while logged into the RockStar server it was determined that the `/etc/hosts` file was modified on this system. The viewing of `rollingstone.com` within the browser appears to be associated with the IP `98.137.246.8` . The information below was recovered using the command `cat /etc/hosts` .

- **Full Results:**

```
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
```

```
98.137.246.8 rollingstone.com

oooooooollowing lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

- After terminating the *SSH* session to the RockStar Corp server, the CLI `nslookup` was used to determine the real domain of the IP address found in the `/etc/hosts` file. In particular, the command used was `nslookup -type=any 98.137.246.8` .
- **Full Results:**

```
Server:   192.168.2.11
Address:  192.168.2.11#53

Non-authoritative answer:
8.246.137.98.in-addr.arpa name = media-router-
fp72.prod.media.vip.gq1.yahoo.com.

Authoritative answers can be found from:

```

- `nslookup` operates at the *Application* layer, or layer 7 of the OSI model.
- **Mitigation/Solution:**
  - Remove the line `98.137.246.8 rollingstone.com` from `/etc/hosts` to prevent redirection and disassociate the domain `rollingstone.com` from the IP `98.137.246.8` .

Phase 4: *"Sh`ARP` Dressed Man"*

It has come to our attention that in the same directory as the configuration file from **Phase 3**, `/etc/`, the hacker left a note as to where he stored away network packet captures.

- Content of the directory `/etc/`were viewed using `ls /etc/` to search for any suspicious files that might contain packet captures.
- Results:

```
adduser.conf    fail2ban   localtime    pam.conf      services
alternatives    fstab    logcheck   pam.d       shadow
apparmor    gai.conf   login.defs   passwd        shadow-
apparmor.d    group    logrotate.conf   passwd-       shadow_class
```

```
apt     group-     logrotate.d    passwd_class  shells
bash.bashrc   grub.d     machine-id   profile       skel
bash_completion   gshadow    magic      profile.d     ssh
bash_completion.d gshadow-   magic.mime   protocols     ssl
bindresvport.blacklist  gss    mailcap    python        staff-group-for-usr-
local
binfmt.d    host.conf  mailcap.order    python2.7     subgid
ca-certificates   hostname   mime.types   python3       subgid-
ca-certificates.conf  hosts    mke2fs.conf    python3.5     subuid
calendar    hosts.allow  modprobe.d   rc0.d       subuid-
cloud     hosts.deny   modules    rc1.d       sudoers
cron.d      init     modules-load.d   rc2.d       sudoers.d
cron.daily    init.d     monit      rc3.d       sysctl.conf
cron.hourly   initramfs-tools  motd     rc4.d       sysctl.d
cron.monthly    inputrc    mtab     rc5.d       systemd
crontab     iproute2   nanorc     rc6.d       terminfo
cron.weekly   issue    network    rcS.d       timezone
dbus-1      issue.net  NetworkManager   resolv.conf   tmpfiles.d
debconf.conf    joe    networks   rmt       ucf.conf
debian_version    kernel     newt     rpc       udev
default     ld.so.cache  nscd.conf    rsyslog.conf  ufw
deluser.conf    ld.so.conf   nsswitch.conf    rsyslog.d     update-motd.d
dhcp      ld.so.conf.d   ntp.conf   screenrc      vim
dpkg      libaudit.conf  opt      securetty     wgetrc
environment   locale.alias   os-release   security      X11
euca2ools   locale.gen   packetcaptureinfo.txt  selinux       xdg
```

- There are multiple suspicious files and directories that have been looked over, including the directory `/etc/joe` (which itself contains suspicous shell scripts), and the file `packetcaptureinfo.txt`.
- After futher investigation, using the command `cat /etc/packetcaptureinfo.txt` the following message was found.

```
 Captured Packets are here:
 https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?
usp=sharing
```

- After the above URL was visited, a `pcapng` file called `secretlogs.pcapng` was downloaded. Using Wireshark to analyze this pcap file, it has been determined that all suspicious activity that could be attributed to a hacker, potentially an employee..
  - The focus on the packets was mostly on ARP and HTTP protocols, thus the filters `arp` and `http` were used. Recall the different types of HTTP request methods and be sure to thoroughly examine the contents of these packets.

- **Results:**
  - After filtering packets with `arp` in Wireshark, there appears to be ARP spoofing happening, as the IP `192.168.47.200` is associated with two different MAC addresses; `00:0c:29:0f:71:a3` and `00:0c:29:1d:b3:b1`. It is also somehwhat odd that the address `192.168.47.171` is asking who has the IP `192.168.47.1`, as this address is usually the router and the one who should be broadcasting WHOIS requests, not the other way around. ARP requests happen within the *Data Link* layer, or layer 2.
  - After filtering packets with `http`, the *permanently moved* or *redirection* code 301 seemed to stand out. HTTP requests happen at the *Application* layer, or layer 7. After further investigation, when following the TCP stream of the packet, the following text was recovered:

    ```
    0%3Ctext%3E=Mr+Hacker&0%3Clabel%3E=Name&1%3Ctext%3E=Hacker%40rockstarcorp.
    com&1%3Clabel%3E=Email&2%3Ctext%3E=&2%3Clabel%3E=Phone&3%3Ctextarea%3E=Hi+
    Got+The+Blues+Corp%21++This+is+a+hacker+that+works+at+Rock+Star+Corp.++Roc
    k+Star+has+left+port+22%2C+SSH+open+if+you+want+to+hack+in.++For+1+Milliio
    n+Dollars+I+will+provide+you+the+user+and+password%21&3%3Clabel%3E=Message
    &redirect=http%3A%2F%2Fwww.gottheblues.yolasite.com%2Fcontact-
    us.php%3FformI660593e583e747f1a91a77ad0d3195e3Posted%3Dtrue&locale=en&redi
    rect_fail=http%3A%2F%2Fwww.gottheblues.yolasite.com%2Fcontact-
    us.php%3FformI660593e583e747f1a91a77ad0d3195e3Posted%3Dfalse&form_name=&si
    te_name=GottheBlues&wl_site=0&destination=DQvFymnIKN6oNo284nIPnKyVFSVKDX7O
    5wpnyGVYZ_YSkg%3D%3D%3A3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31_Gl2mb5PGk%3D&g-
    recaptcha-
    response=03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls
    6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-
    6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6uW0-
    aWc711YdgRnK3yOFlHy7cZEciuwkE_Hx_7ZyrbZBhdGF8_z6F9LIq6tk-OLs6HBp-
    6GG0yWy7A2iD0NmnO2TBDPBe9Si54sGlzVNP-
    RLm1mazWyu4GzBRk5GfJNOcJxa30c20coEIgEIYGCSCFbJhfAHTTP/1.1 303 See Other
    ```

- Analysis: The following message was exctrated from the text above.

  ```
  Hi. Got The Blues Corp. This is a hacker that works at Rock Star Corp. Rock
  Star has left port 22 SSH open if you want to hack in. For 1 Milliion Dollars
  I will provide you the user and password.
  ```

  It appears that the hacker may actually be an employee.

- **Migitation:**
  - Investigate employees by analyzing outgoing messages logs from their machines.

End-Of-Report