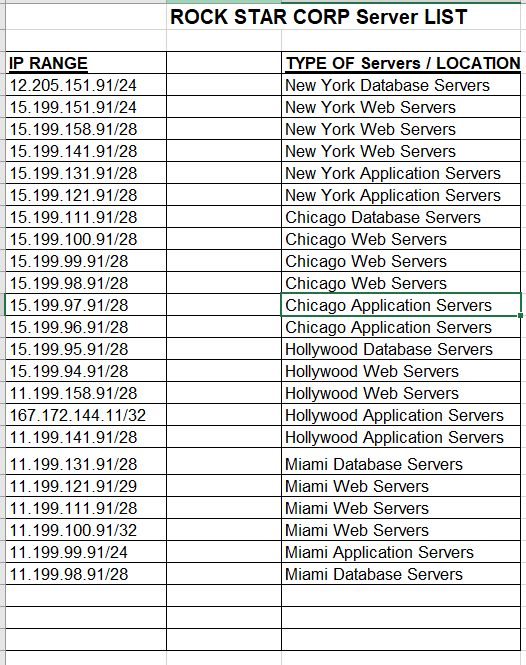
JD Haynes Unit 7 Homework – Networking Vulnerability Assessment

Using nmap and Wireshark – based on list of IP Ranges provided by “Customer”



**PHASE 1**

* **Research:** Determined the IP ranges to scan were 15.199.95.91, 15.199.94.91, 11.199.158.91, 167.172.144.11, 11.199.141.91, then ran fping against all of those IP addresses.
  + Used the following command to run fping:
    - fping -c10 15.199.95.91 15.199.94.91 11.199.158.91 167.172.144.11 11.199.141.9
  + Determined a potential vulnerability that IP 167.172.144.11 is responding.
* **Vulnerabilities:** Since RockStar Corp doesn't want to respond to any requests, this is a vulnerability.
* **Recommendations:** Recommend to restrict allowing ICMP echo requests against IP 167.172.144.11 to prevent successful responses from PING requests.
* **Network Layer:** This occurred on the network layer (layer 3) as Ping uses IP addresses and IPs are used on the Network Layer.

**PHASE 2**

* **Research:** Checked for open ports on the available IP address 167.172.144.11.
  + Used the following command to scan the most common 1000 ports by running nmap with TCP SYN option:
    - nmap -sS 167.172.144.11
  + Determined a potential vulnerability that the following 5 ports are open:
    - 22 (ssh)
    - 25 (smtp)
    - 139 (netbios-ssn)
    - 445 (Microsoft-ds)
    - 514 (filtered shell)
* **Vulnerabilities:** Each of these open ports present their own vulnerabilities allowing bad actors to potentially access systems, particularly port 22 via SSH and through port 25 via SMTP, with exploits that are readily available on the internet.
* **Recommendation:** Recommend to close ports. For any ports that must remain open other mitigation includes setting up a firewall and whitelisting approved IPs.
* **Network Layer:** This occurred on the transport layer (layer 4) as nmap performs port scanning.

**PHASE 3**

* **Research:** Checked if 167.172.144.11 could be accessed using SSH since port 22 is open
  + Used the following command to ssh into system
    - ssh [jimi@167.172.144.11](mailto:jimi@167.172.144.11)
    - When asked for password used “hendrix”
    - Used directory traversal to view the “passwd” file in the /etc directory.
  + Used the nslookup command to check the rollingstone.com domain. Checked the rollingstone.com domain by running nslookup using the following command:
    - nslookup
    - set type=ns
    - rollingstone.com
  + Discovered that the rollingstone.com domain is redirecting to 192.168.220.2 with two nameservers:
    - * kurt.ns.cloudflare.com
      * elaine.ns.cloudlflare.com (need to add recommendation
  + Was able to open the /etc/hosts file using nano which would have allowed me to change the DNS or IP addresses stored there.
* **Vulnerabilities**: Port 22 being open makes the system vulnerable to access. Simple passwords like “hendrix” make it easy for bad actors to hack in to a system. User names can be gathered by viewing the “passwd” file. Allowing the /etc/hosts file to be modified by non-admins provides ways to redirect users to different IPs and Domains.
* **Recommendations:** Filter the ports using a firewall. Enforce use of complex passwords and do not re-use any passwords. Require admin password to access /etc/passwd file and /etc/hosts file.
* **Network Layer:** SSH occurred on the Application layer (layer 7) as ssh allows remote login and other network services to operate securely over an unsecured network. NSLOOKUP occurred on the Session layer (layer 5) as nslookup provides info about DNS authorization.

**PHASE 4**

* **Research:** Checked /etc directory and found a file called packetcaptureinfo.txt
* Used nano to open the file and it contained a message that said “Captured packets are here:”

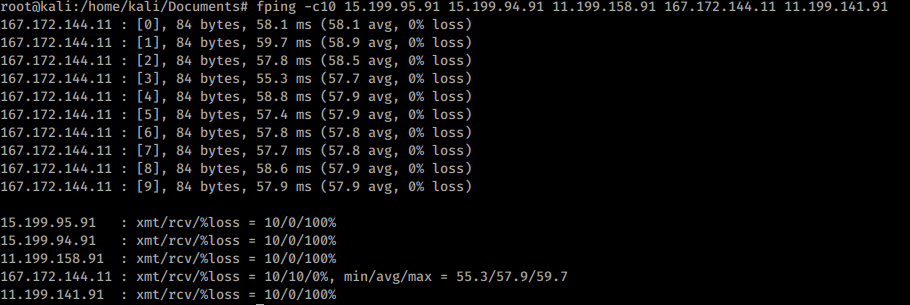
<https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view>

* Navigated to the URL above and found a file called secretlogs.pcapng
* Downloaded the pcappng file and opened it Wireshark
* In Wireshark, observed that the source IP address 192.168.47.200 is initially used by MAC address 00:0c:29:0f:71:a3 per frames 1 - 4.
* Then in frame 5 same source IP address 192.168.47.200 is used by MAC address 00:0c:29:1d:b3:b1. This is an indicator of ARP spoofing that allows IP 192.168.47.200 to be read as being at the spoofed MAC address of 00:0c:29:1d:b3:b1. This can enable a bad actor to intercept traffic intended for IP 192.168.47.200 and send it to a malicious IP.
* Frames 12 - 15 the client is using an HTTP GET request to access [www.gottheblues.yolasite.com](http://www.gottheblues.yolasite.com) through port 80.
* In frame 16 an HTTP POST request indicates Mr. Hacker at [Hacker@rockstarcopr.com](mailto:Hacker@rockstarcopr.com) has inserted some text that says he is a hacker at Rock Star. It tells people that port 22 is open for SSH hacking and that he will sell the username and password for 1 million dollars.
* The referrer is <http://www.gottheblues.yolasite.com>
* Frame 17 contains an HTTP code 303 which is the code for a redirect of an HTTP application to a new URL, particularly after a POST has occurred. This occurs on port 80 and comes from <http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true>
* In frame 18, the GET request has been redirected to IP 104.16.161.215.
* In frame 19, there is a TCP payload of 3599 bytes
* In frame 20 the client wireshark has flagged an “expert information” incident which is used to indicate anomalies in a packet capture file. This one had severity level “chat” and group “sequence” which indicates that a protocol sequence number was suspicious, e.g. it wasn’t continuous or a retransmission was detected. (reference: <https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html> )

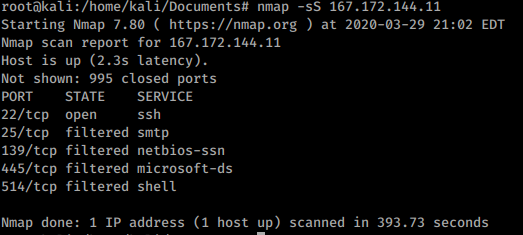
* **Vulnerabilities:** Redirection of users to a different IP using ARP spoofing can allow bad actors to capture information about the user and the company, putting both at risk.
* **Recommendations:** Recommend to filter port 80 with a firewall or start using port 443 for secure https connection. Can consider creating a static ARP address. Educate users on how to recognize redirection of websites.
* **Network Layer:** The ARP transactions occurred on the Data Link layer (layer 2) used to transfer network traffic within a local layer. The TCP transactions occurred on the Transport layer (layer 4) which is used by TCP to establish a connection via 3-way handshake. The HTTP transactions operate at the Application layer (Layer 7) because it’s a protocol for a shared communication.

**BACKUP SCREEN SHOTS FOR EACH PHASE**

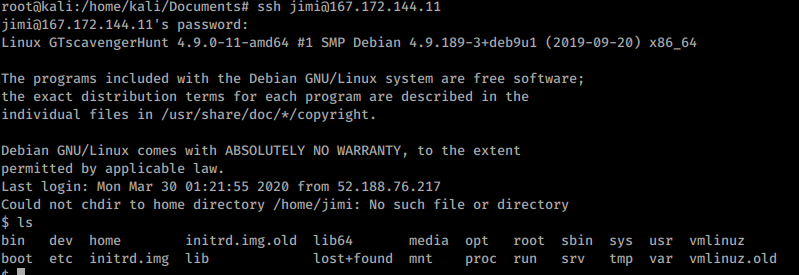
**PHASE 1 – SCREEN SHOT**

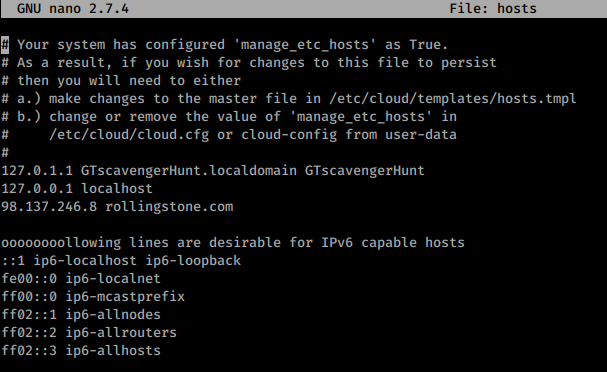


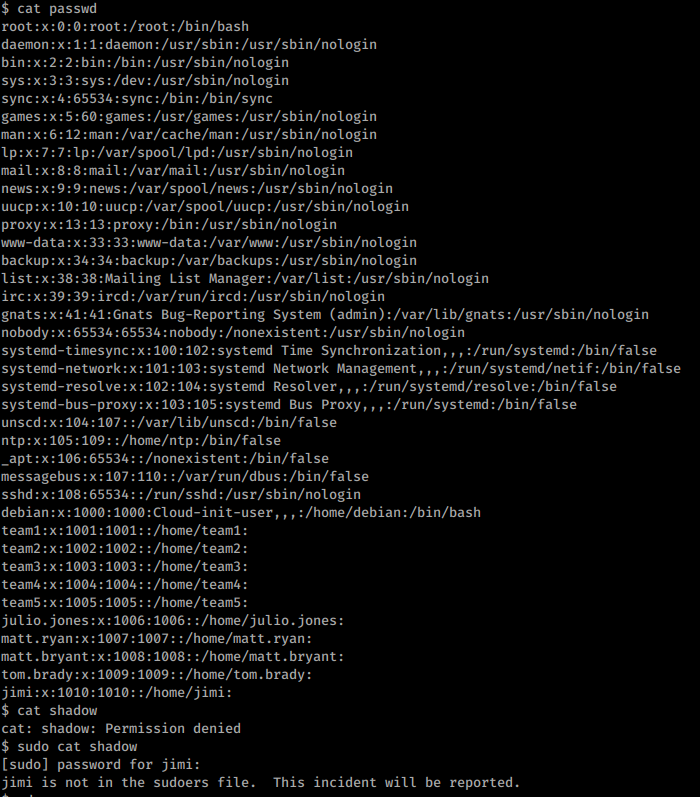
**PHASE 2 – SCREEN SHOT**

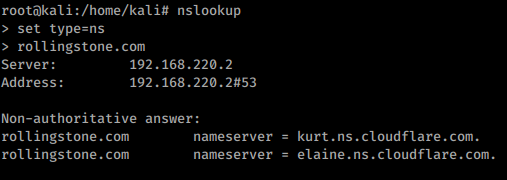


**PHASE 3 – SCREEN SHOTS**

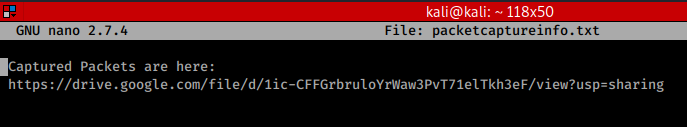




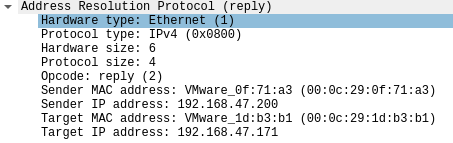




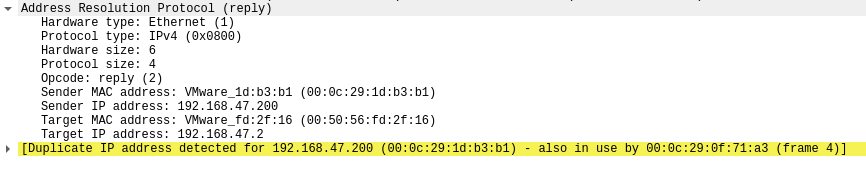
**PHASE 4 – SCREEN SHOTS**



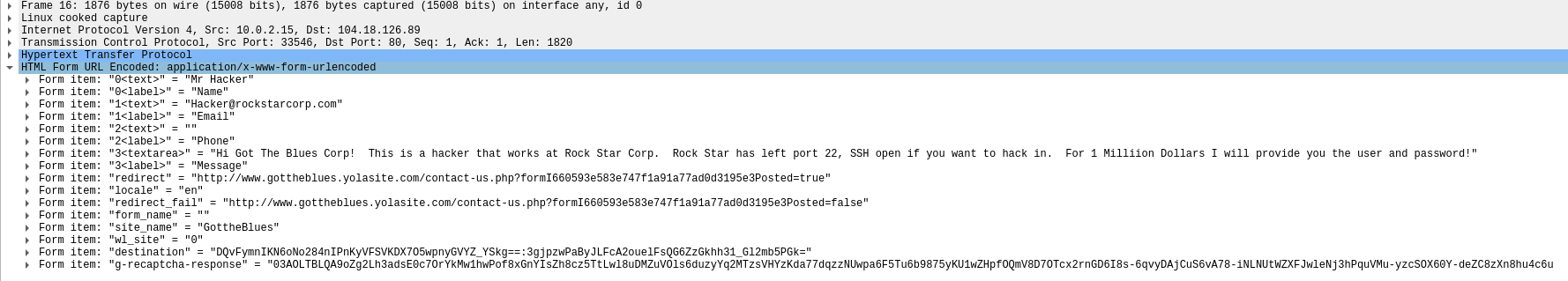
**Frame 4 PCAP**



**Frame 5 in PCAP**



**Frame 16 - HTTP POST**



**Frame 17 – Redirect (HTTP/1.1 303)**



**Frame 18 & 19**

