08 Networking-Fundamentals Homework

Phase 1:

* Determined IP ranges to scan were as follows:
* 15.199.95.91/28
* 15.199.94.91/28
* 203.0.113.32/28
* 161.35.96.20/32
* 192.0.2.0/28
* fping commands used to scan the above IP ranges:
* fping -g 15.199.95.91/28
* fping -g 15.199.94.91/28
* fping -g 203.0.113.32/28
* fping -g 161.35.96.20/32
* fping -g 192.0.2.0/28
* Results of fping commands (fping reading)
* Of all the servers pinged, only 161.35.96.20 is alive and accepting connections. OSI network layer 3 was used to find these results, as both IP and ICMP operate at the network layer.
* Recommend restricting ICMP traffic for IP 161.35.96.20 so it doesn't respond to ping requests.

Phase 2:

* nmap command: sudo nmap -sS 161.35.96.20
* 999 ports were closed, while port 22 (ssh) was open, and port 0 (smtp) and port 0 (park-agent) were filtered. These findings use the OSI transport layer (4) since they use the tcp protocol.
* Results of the SYN scan: (Jimi Hendrix)
* Determined a potential vulnerability for IP: port 161.35.96.20. Since the server at 161.35.96.20 accepts SSH connections, an attacker could potentially get SSH access to the server
* Recommend restricting SSH access on the server unless absolutely necessary. If it is indeed necessary, recommend restricting SSH access to key-only access for increased security.

Phase 3:

* Since 161.35.96.20 is open to SSH connections (on port 22), I tried ssh jimi@161.35.96.20 with the password hendrix. Following this, I got shell access to the server.
* The [/etc/hosts] file on the server has an entry for rollingstone.com and has it configured to go to 98.137.246.8
* Result of cat [/etc/hosts] nmap command
* Running [nslookup 98.137.246.8] yielded the following results:
* 8.246.137.98.in-addr.arpa name = unknown.yahoo.com.
* Running [nslookup rollingstone.com] yielded the following results:
* Name: rollingstone.com

Address: 151.101.128.69

* Name: rollingstone.com

Address: 151.101.64.69

* Name: rollingstone.com

Address: 151.101.0.69

* Name: rollingstone.com

Address: 151.101.192.69

* Results of both nslookup commands: nslookup
* The actual IP address of rollingstone.com is one of the following
* 151.101.0.69
* 151.101.128.69
* 151.101.192.69
* 151.101.64.69
* Recommend somebody with sudo permissions delete the entry in /etc/hosts that redirects rollingstone.com to the incorrect IP address.
* All of these findings are found at OSI layer 7, since DNS is an application layer protocol.

Phase 4

* The file indicates the packet capture files are located at: unknown.yahoo.com.
* Analysis of ARP packets in the packet capture file determined that two nodes are responding to the 192.168.47.200 IP address, located at the following MAC addresses:
* 00:0c:29:0f:71:a3
* 00:0c:29:1d:b3:b1
* While it is still unclear who the hacker is, he or she has the email address Hacker@rockstarcorp.com and their computer has the mac address 08:00:27:f8:42:a7. Hopefully, the hacker can be apprehended before any corporate secrets are stolen and any more damage is done.