

**Network Traffic Analysis**

**Lab NMAP – First Scan**

As a Network Administrator for your company you start your normal day by logging in to your machine in the morning at 7:30 AM. As soon as you login you see a message containing the following information:



**Network Anomaly Alert**

Potential Network Probe Detected By IP **97.79.245.16**

Time: 16:54:50

Your company owns one public network range (which means all of the IP addresses of)

**212.15.61.0 through 212.15.61.255 – this is important!**

**Questions**

**(Remember to clear your filters!)**

1. Your network is under a Denial-of-Service (DoS) attack. (1) What malicious IP addresses were performing this attack? (2) Which IP address in **your network** was ‘under attack’ (i.e. the one the attackers were going after)? (Statistics → IPv4 Statistics → All Addresses)

Hint: Look at the ‘Count’ column – filter (click the column tab) until the highest numbers show first; which three IP addresses have the highest ‘count’ (attackers)? Which IP address had the total *highest* count – does the IP address belong to your organization (see above) which may be under attack?

1. 208.117.253.91, 216.105.40.40 & 97.79.245.16 were the 3 highest attackers based on count.
2. 212.15.61.194. This IP Address does belong to our organization.

--------------------------------------------------------------------------------------------------------------------------------

1. How many total *TCP* hosts were targeted?

(Statistics → Conversations→TCP Tab)

1,162

----------------------------------------------------------------------------------------

1. Which port(s)/service(s) were targeted in these scans by two of the attacking IPs?

(Statistics → Conversations → TCP)

Hint: Look at the ‘Port B’ column. These numbers are network port numbers.

Ports 21, 22, 80 & 443 were the targeted ports

----------------------------------------------------------------------------------------

1. What was *your* company’s main IP address the hackers were trying to attack to cause the DoS and what *port number* were they going after?

(Use this filter: tcp.flags == 0x12)

Hint: Look at the “Destination IP”; then look at the first number in the ‘Info’ column

The attackers were mainly targeting IP Address 212.15.61.194. The port number the attackers were going after was port 80.

----------------------------------------------------------------------------------------

1. What makes the **time** of the event significant for this DoS attack?

(Hint: see alert above)

Hint: The time is identified in military time - its 4:54pm in the afternoon

It was towards the end of the workday, so if the network administrator had been off his/her machine prior to 4:54PM there would have been a lot of time until signing on again at 7:30AM the next morning. This allows for a lot of time for disruption to the network.

----------------------------------------------------------------------------------------

1. Were there any outside connections made? If so, what *port* was used and how *many* were there?

(Hint: Analyze → Expert Information)

Hint: Review the ‘Chat – HTTP/1.1 200 OK\r\n’ row under the Severity Column, then look at the ‘Protocol’ and ‘Count’ columns.

Yes, outside connections were made. HTTP was used and 363 connections were made.

----------------------------------------------------------------------------------------

1. What **time** did the DoS attack end and what was the **source** and **destination** IP addresses?

(Hint: Clear filters review the ‘No.’ tab, look at the last packet #22240 for the source and destination; then select the ‘Frame’ and look at Arrival Time)

The source is 212.15.61.194 and the destination is 208.117.253.91. The time shown under ‘Frame’ is 5:57PM.

----------------------------------------------------------------------------------------

1. Which part of the *Three-Way Handshake* was the major cause of this attack?

(Hint: Clear the filter and just look at the ‘Info’ column – what to you see? We discussed the Three-Way Handshake in Week 3)

It seems as though the tear down of the session was never initiated, so the session is still active. Another reason may be that the attacker masked their port number in order to gain access.

----------------------------------------------------------------------------------------

1. What ***frame #*** was the first DNS requested and what was the **website** requested from the query?

(Hint: use filter frame.protocols == "eth:ethertype:ip:udp:dns", then review the first packet and the info column – what part of a website do you see?)

Frame 12804 was the first requested. The website shown is ads.bluelithium.com

----------------------------------------------------------------------------------------

1. What ‘**Ethernet II**” Layer 2 *product device* name is used for IP 212.15.61.194? (Hint: use filer ip.addr == 212.15.61.194, look in Window Panel #2)

Cisco

----------------------------------------------------------------------------------------