DOS ATTACK ACTIVITY

Vedant Brahmbhatt

Scenario

You are a cybersecurity analyst working at a company that specializes in providing IT consultant services. Several customers contacted your company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error "**destination port unreachable**" after waiting for the page to load.

You are tasked with analysing the situation and determining which network protocol was affected during this incident. To start, you visit the website and you also receive the error "destination port unreachable." Next, you load your network analyser tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyser. The analyser shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: "udp port 53 unreachable."

Analysis

1) Explain how IT team became aware of the attack?

   IT team received complain from HR department that, when they are trying to access the website, it is not reachable and showing some error. (also sends some photos clicked from phone)

2) Explain the actions taken by the IT department to investigate the incident.

   IT team sees the message. Now, they open tcpdump (command line network packet analyser), opens the browser and search for www.yummyrecipesforme.com. They received error message from ICMP (internet message control protocol) that port 443 is unreachable. (port 443 – HTTPS port, well known port). They also verify the fireball configuration if firewall blocking the website but, it was clean.

   On further investigation they find out that, DNS was out of service. Browser was expecting IP address for the website. They suspect a DDOS attack.

Conclusion

This report shows about how security team got the information and did initial investigation. This process can be considered in computer forensics and chain of custody when culprit is found.

Disclaimer

This Activity was part of Google's Professional cyber security course. Except the solution all the details (i.e. scenario) given inside the google paid course.