Introduction to the Course

Ethical hacking involves testing to see if an organization's network is vulnerable to outside threats. Denial-of-service (DoS) attacks are one of the biggest threats out there. Being able to mitigate DoS attacks is one of the most desired skills for any IT security professional—and a key topic on the Certified Ethical Hacker exam. In this course, I learn about the history of the major DoS attacks and the types of techniques hackers use to cripple wired and wireless networks, applications, and services on the infrastructure. I got explain what to Denial of Service is, demonstrated some of the more popular attack tools and then looked at how ransomware works. I finished by looking at how to protect our systems against Denial of Service. This course, covers the basic methods hackers use to flood networks and damage services, the rising threat of ransomware like Cryptolocker, mitigation techniques for detecting and defeating DoS attacks, and more.

Learning objectives

- What is denial of service?
- TCP SYN, Smurf, and UDP flooding
- Deauthenticating a wireless host
- Flooding HTTP
- Using BlackEnergy
- Flooding a SIP server
- Detecting P2P attacks with PeerShark
- Defeating DoS attacks

Screenshots

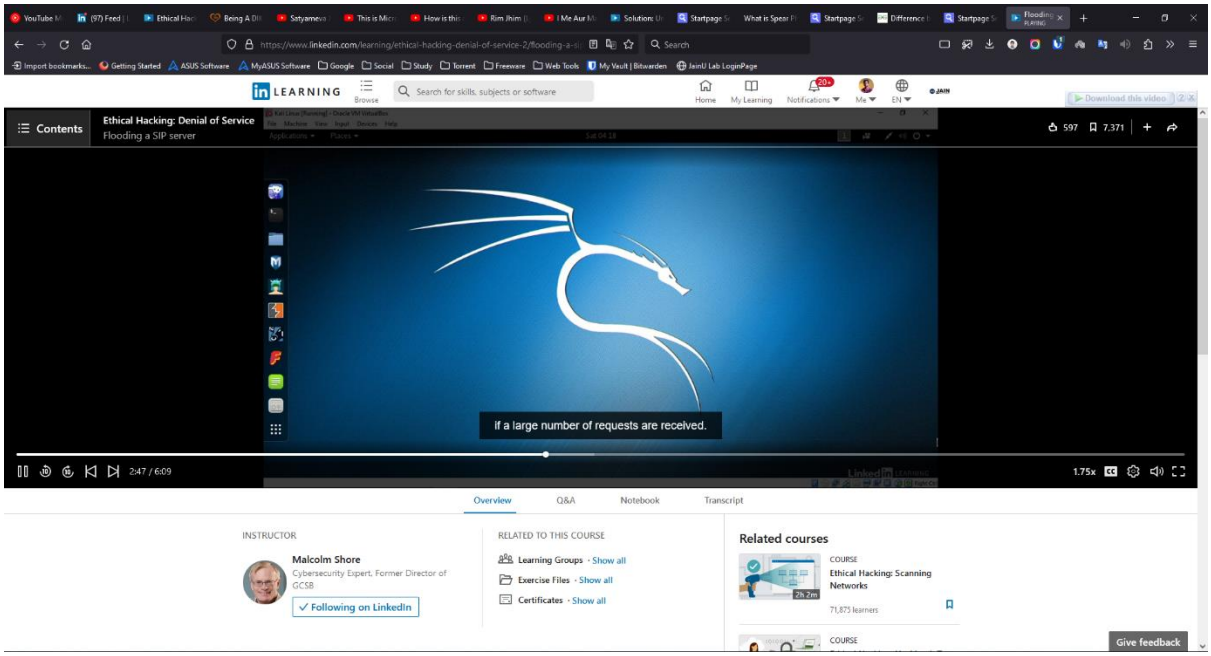


Figure: Section 05 – SIP Service Attacks

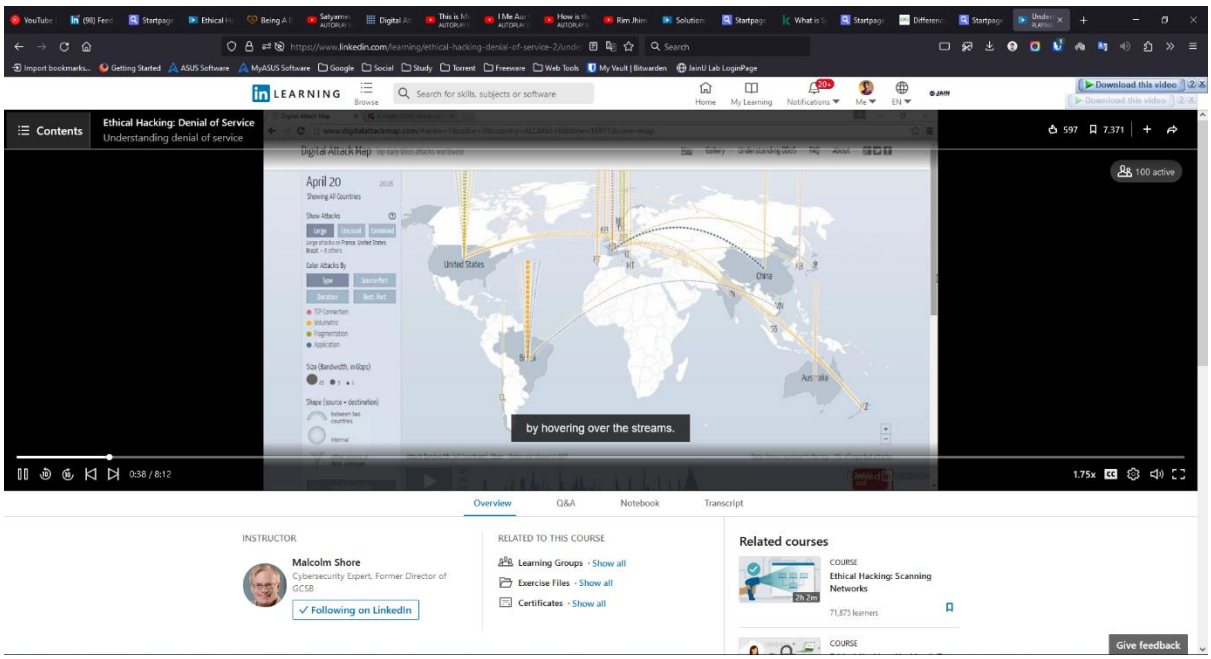


Figure: Section 01- What is a Denial of Service ?

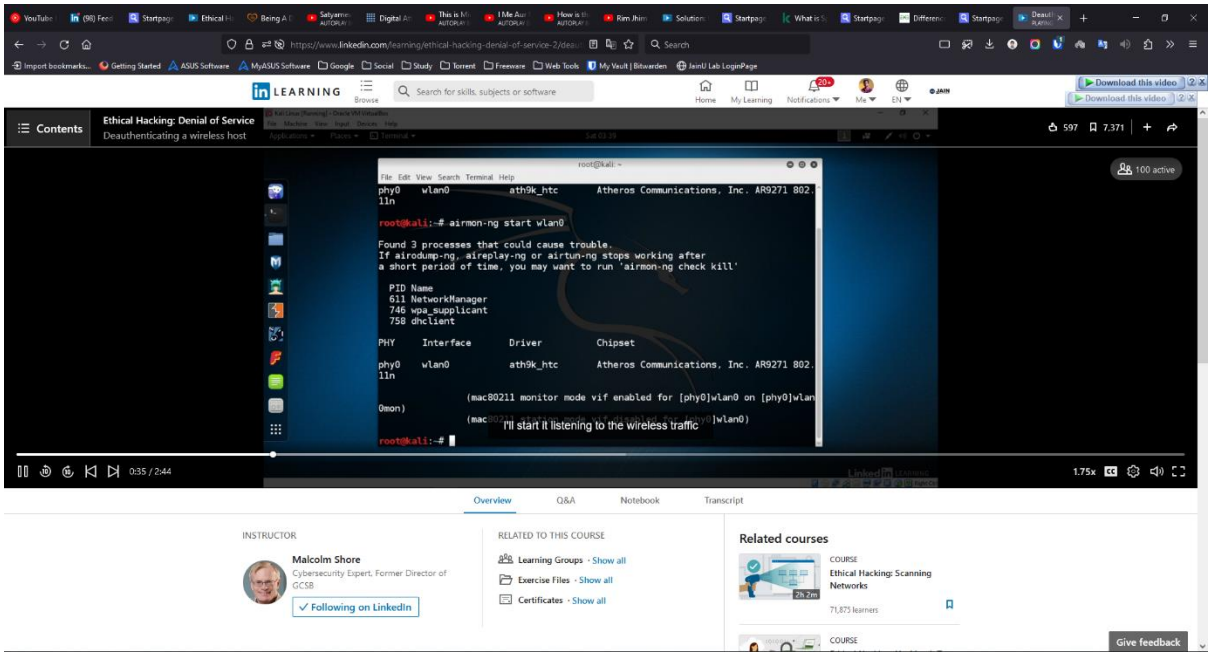


Figure: Section 03 – Wireless denial of Service

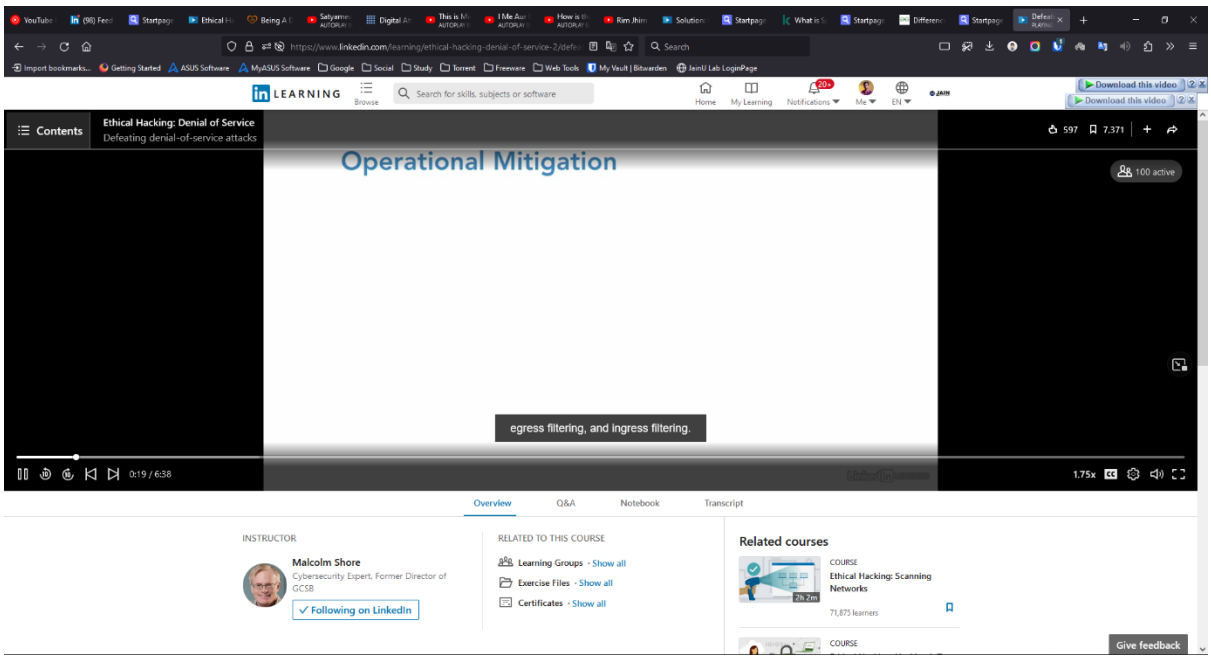
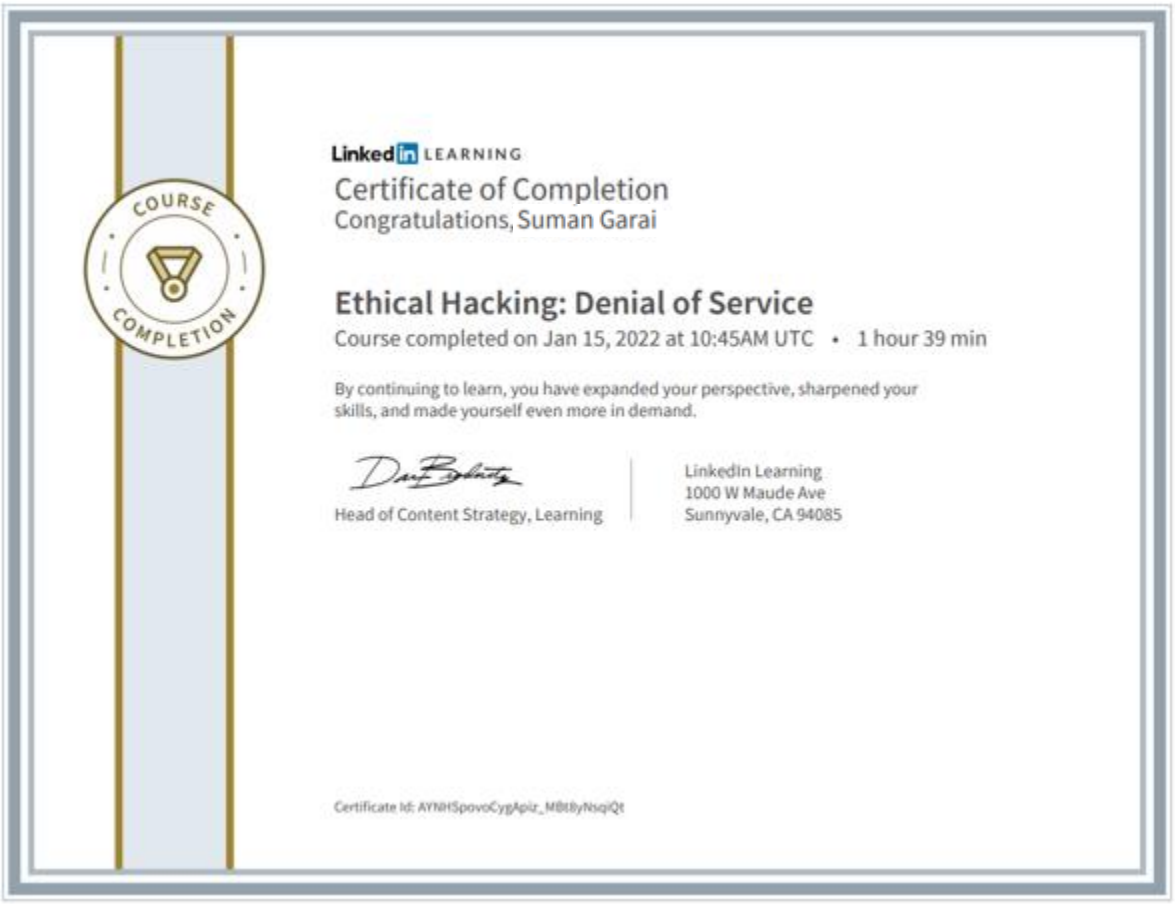


Figure: Section 07- Mitigation Techniques

Conclusion

I got provided an overview on denial-of-service attacks. We took a look at Python tool for DDOS Attack and analysed the power of the code. We looked at TCP SYN flooding using hping3 and using hyena to run a reflection attack. We learnt about tools and its using mechanisms and procedures like UDP LOIC, ARP Poisoning with Ettercap, amplifying attacks using NTP and Memcached. We took a look at procedure for deauthenticating wireless hosts. We then looked at some of the tools to help in application of DOS like, flooding using HTTP using GoldenEye, testing web apps using OWASP SwitchBlade, killing FTP service & RangeAmp attacks on CDN, and how to flood SIP server. We learnt about ransomwares and malwares, such as Petya. Then we studied ways to prevent denial-of-service. We looked at countermeasures for DDOS attacks, and then ways to detect and protect from those.

Certificate



LinkedIn LEARNING

Certificate of Completion

Congratulations, Suman Garai

Ethical Hacking: Denial of Service

Course completed on Jan 15, 2022 at 10:45AM UTC • 1 hour 39 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate Id: AYNHSpovoCygApiz_MBtByNsqiQt