Introduction to the Course

In this course, I explored the second phase of ethical hacking, scanning. I reviewed scanning techniques and the variety of tools used to obtain information from our target system, including specially crafted packets, TCP flags, UDP scans, and ping sweeps. She discussed mapping the network and vulnerability scanning and investigate some tools such as Nmap, Nitco, and other tools. Finally, she discussed ways to evade detection using onion routing and tunnelling techniques, along with ways to identify and counter port scanning. I explored many of the tools and techniques of scanning and also the logic behind the scans. She discusses scanning techniques and their objectives, then goes over vulnerability scanning and how to predict possible attack paths. She introduces scanning tools for port scans, fingerprinting OS, time syncs, and more, then shows you some ways that hackers counter detection via evasion, concealment, and spoofing. She also addresses how to reduce the threat of tunnelling; a method hackers use to circumvent network security.

Learning objectives

- Using Scanning overview
- Port scanning countermeasures
- Scanning and querying DNS
- Scanning with ICMP
- Mapping (or blueprinting) a network
- Scanning for vulnerabilities
- Using tools such as hping and NetScan
- Evading detection
- Concealing your network traffic
- Preventing tunneling

Screenshots

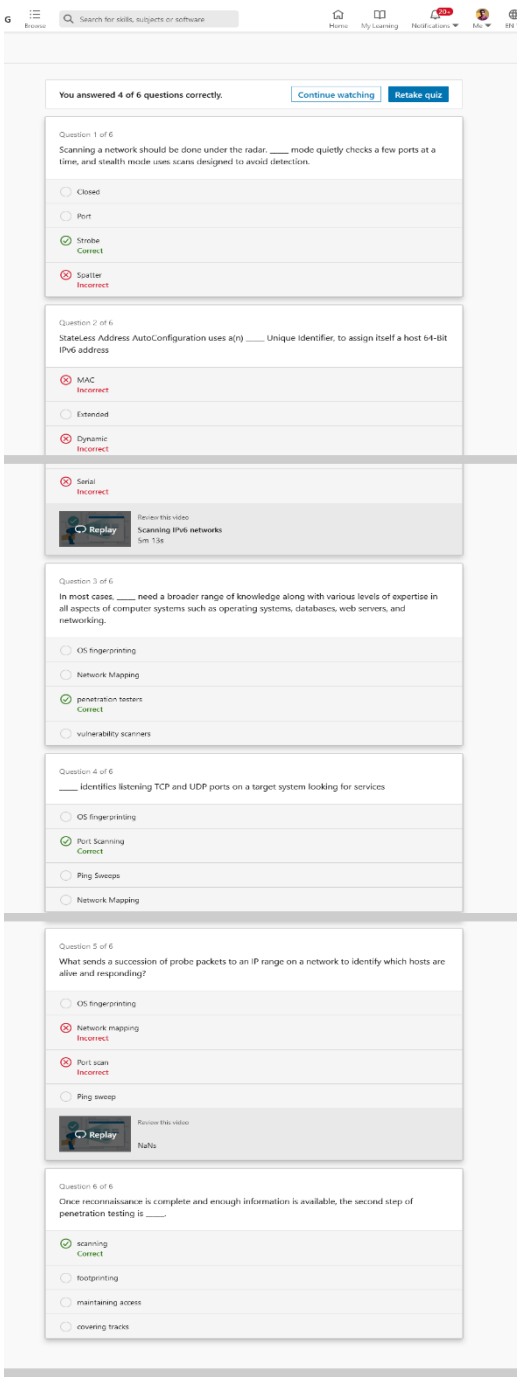

Figure: Section 01 – Scanning-Overview-and-Methodology-Assessment

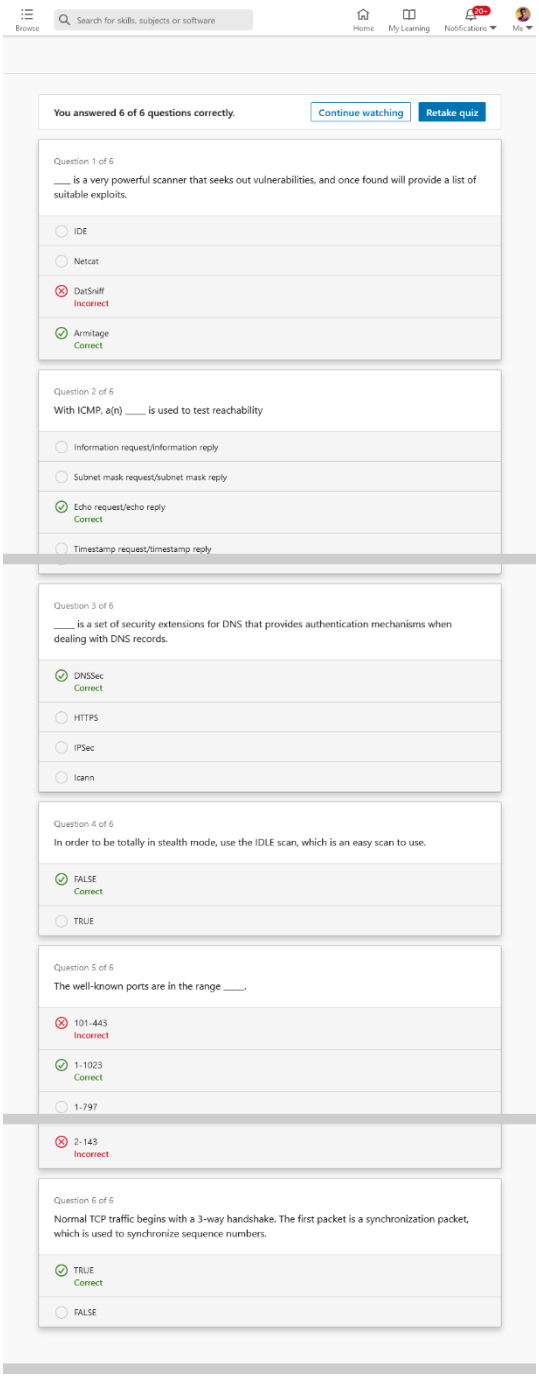

Figure: Section 02- Identifying-Live-Systems-Using-Protocols-Assessment

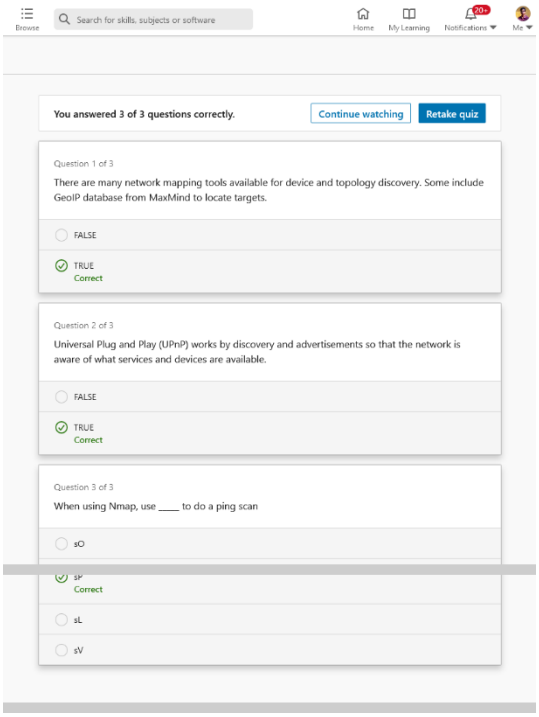

Figure: Section 03 – Blueprint-the-Network-Assessment

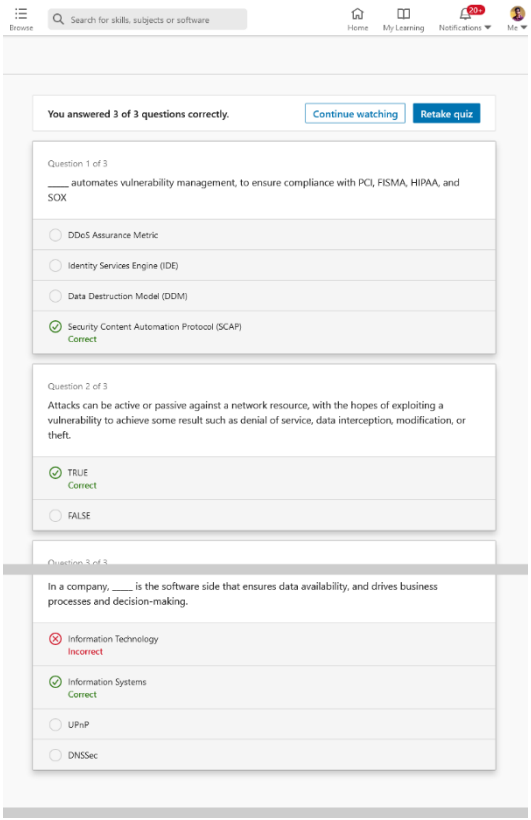

Figure: Section 04- Vulnerability-Scanning-Assessment

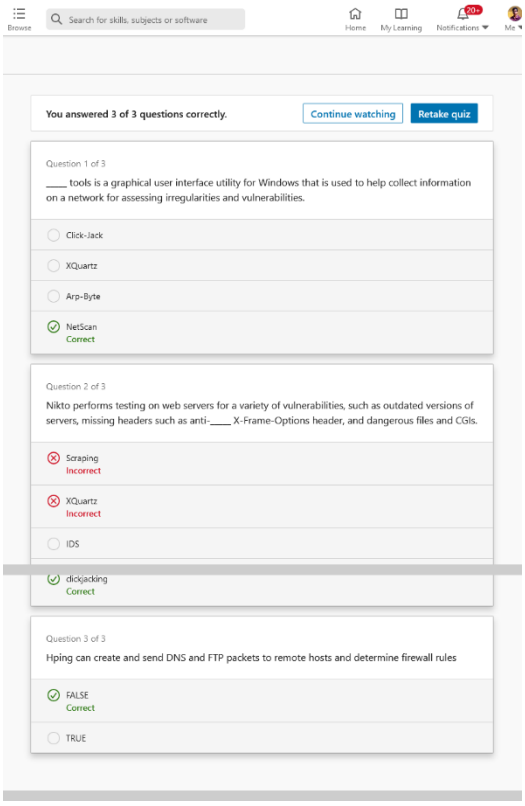

Figure: Section 05 – Scanning-Tools-Assessment

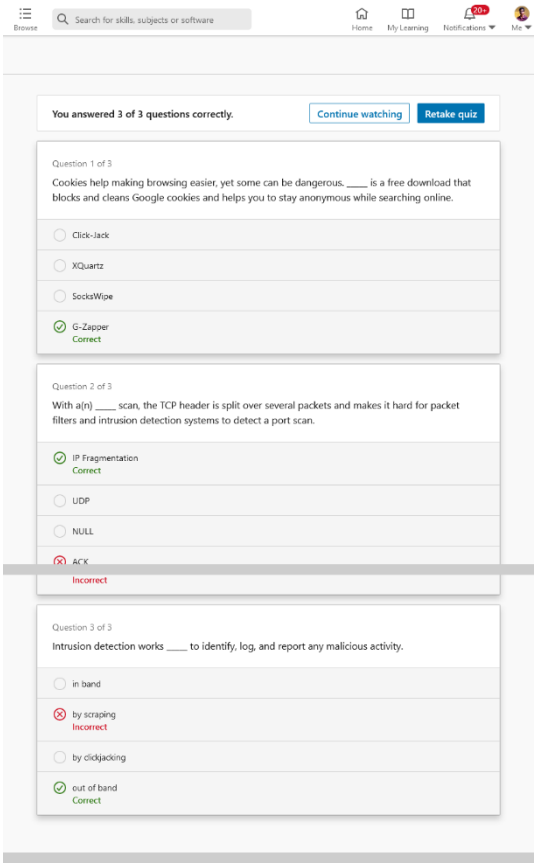

Figure: Section 06- Evading-Detection-Assessment

Conclusion

In this course, we covered some of the ways to scan networks with hping, Nikto, NetScan, identify live hosts, blueprint the network with Nmap, SSDP and conduct vulnerability scanning. I covered a wide variety of tools and techniques along with methods to evade intrusion detection systems using IP fragmentation, conceal and spoof your existence with Proxifier, SocksChain, Onion routing and tunnelling techniques in HTTP and SSH.

Certificate