

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

You answered 4 of 6 questions correctly. [Continue watching](#) [Retake quiz](#)

Question 1 of 6
Scanning a network should be done under the radar. ____ mode quietly checks a few ports at a time, and stealth mode uses scans designed to avoid detection.

- ☐ Closed
- ☐ Port
- ☒ Shrobe
Correct
- ☒ Spaffler
Incorrect

Question 2 of 6
Stateless Address AutoConfiguration uses a(n) ____ Unique Identifier, to assign itself a host 64-bit IPv6 address

- ☒ MAC
Incorrect
- ☐ Extended
- ☒ Dynamic
Incorrect

Question 3 of 6
In most cases, ____ need a broader range of knowledge along with various levels of expertise in all aspects of computer systems such as operating systems, databases, web servers, and networking.

- ☐ OS fingerprinting
- ☐ Network Mapping
- ☒ penetration testers
Correct
- ☐ vulnerability scanners

Question 4 of 6
____ identifies listening TCP and UDP ports on a target system looking for services

- ☐ OS fingerprinting
- ☒ Port Scanning
Correct
- ☐ Ping Sweeps
- ☐ Network Mapping

Question 5 of 6
What sends a succession of probe packets to an IP range on a network to identify which hosts are alive and responding?

- ☐ OS fingerprinting
- ☒ Network mapping
Incorrect
- ☒ Port scan
Incorrect
- ☐ Ping sweep

Question 6 of 6
Once reconnaissance is complete and enough information is available, the second step of penetration testing is ____.

- ☒ scanning
Correct
- ☐ footprinting
- ☐ maintaining access
- ☐ covering tracks

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

You answered 6 of 6 questions correctly. [Continue watching](#) [Retake quiz](#)

Question 1 of 6
____ is a very powerful scanner that seeks out vulnerabilities, and once found will provide a list of suitable exploits.

- ☐ IDE
- ☐ Netcat
- ☒ DarSniff
Correct
- ☒ Armitage
Correct

Question 2 of 6
With ICMP, a(n) ____ is used to test reachability

- ☐ Information request/information reply
- ☐ Subnet mask request/subnet mask reply
- ☒ Echo request/echo reply
Correct
- ☐ Timestamp request/timestamp reply

Question 3 of 6
____ is a set of security extensions for DNS that provides authentication mechanisms when dealing with DNS records.

- ☒ DNSSEC
Correct
- ☐ HTTPS
- ☐ IPsec
- ☐ Icanh

Question 4 of 6
In order to be totally in stealth mode, use the IDLE scan, which is an easy scan to use.

- ☒ FALSE
Correct
- ☐ TRUE

Question 5 of 6
The well-known ports are in the range ____.

- ☒ 101-443
Incorrect
- ☒ 1-1023
Correct
- ☐ 1-797
- ☒ 2-143
Incorrect

Question 6 of 6
Normal TCP traffic begins with a 3-way handshake. The first packet is a synchronization packet, which is used to synchronize sequence numbers.

- ☒ TRUE
Correct
- ☐ FALSE

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

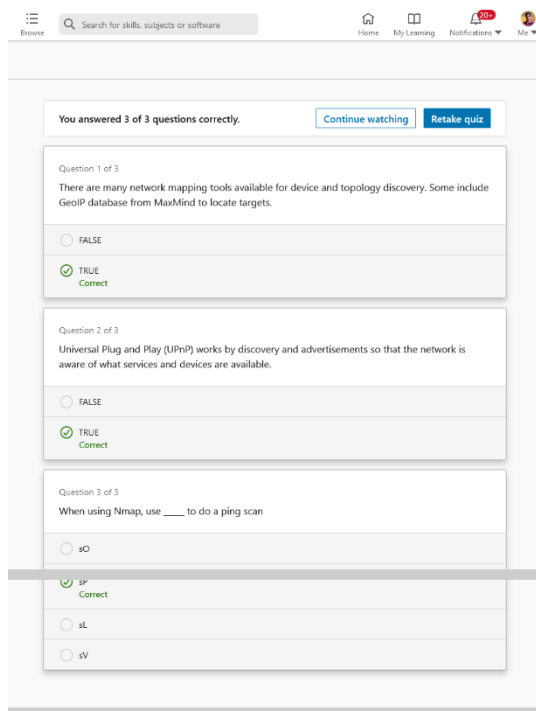


Figure: Section 03 – Blueprint-the-Network-Assessment

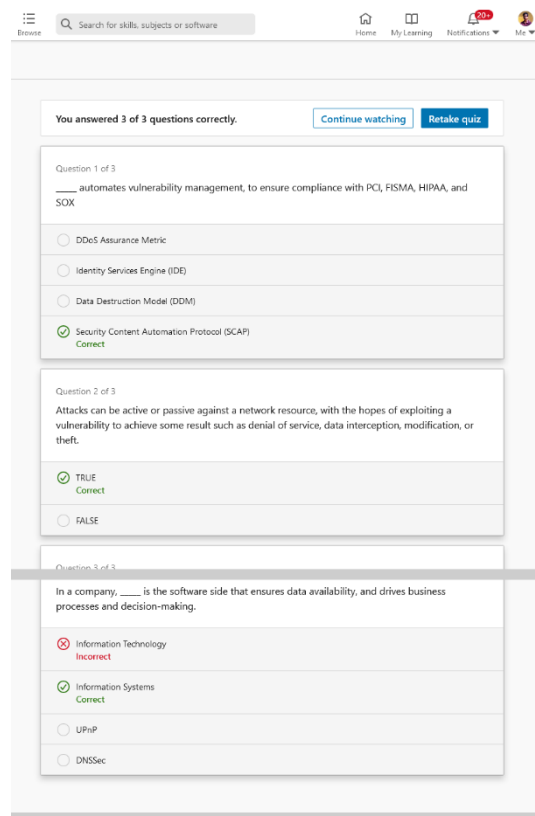


Figure: Section 04- Vulnerability-Scanning-Assessment

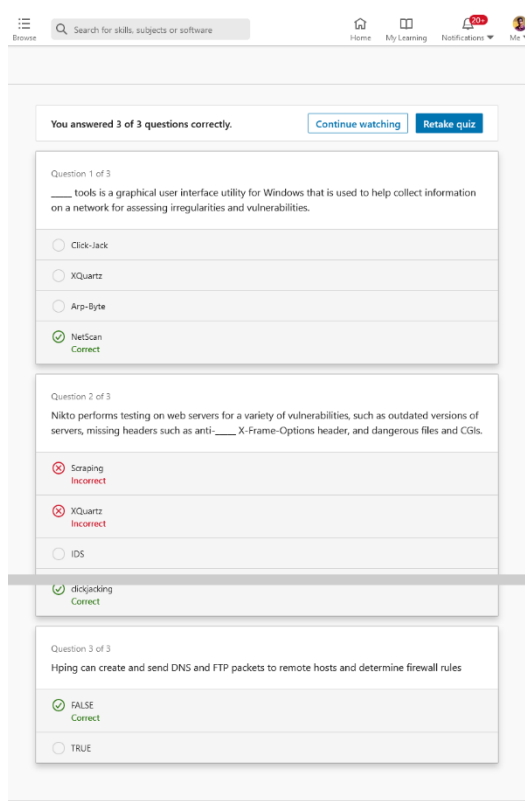


Figure: Section 05 – Scanning-Tools-Assessment

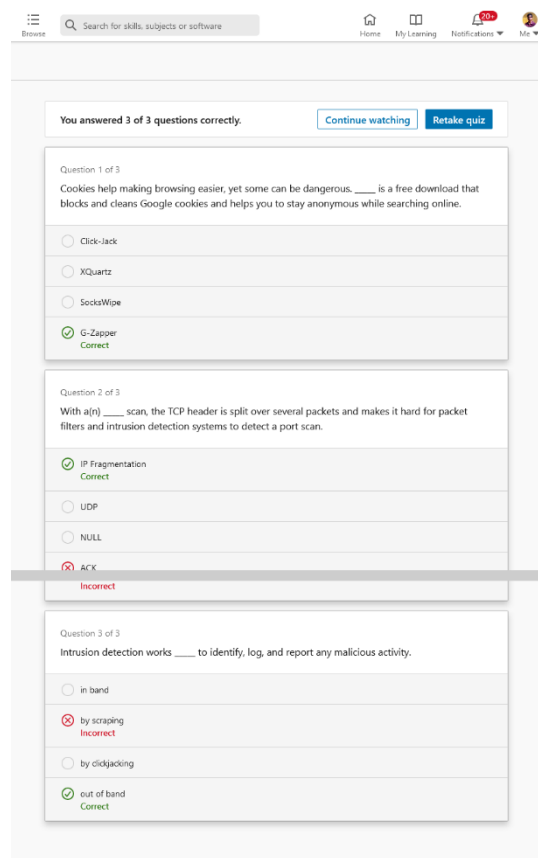


Figure: Section 06- Evading-Detection-Assessment

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

