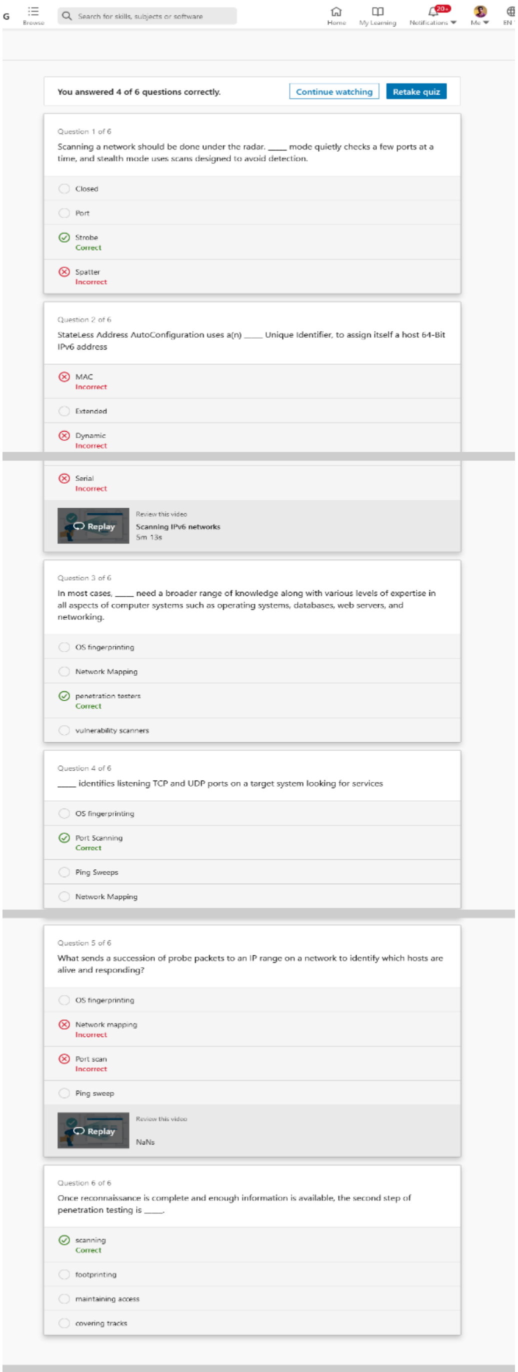
Introduction to the Course

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.

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
- ✓ Strobe
  Correct
- ⊗ Spatter
  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
- ⊗ Serial
  Incorrect

Review this video
Scanning IPv6 networks
5m 13s

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

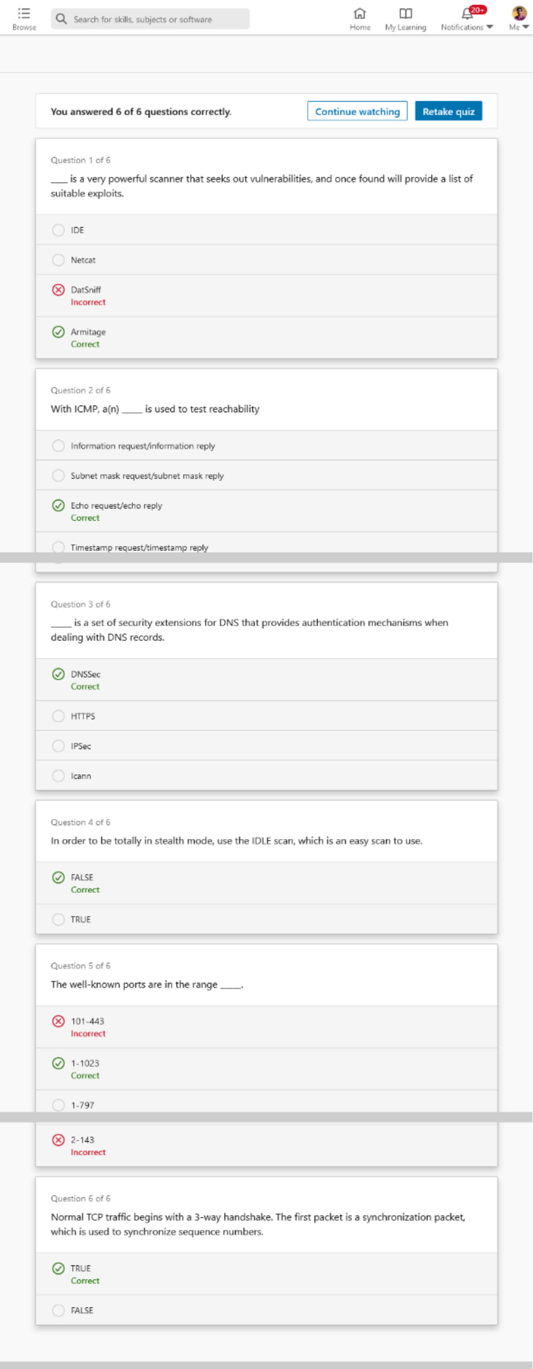
Review this video
NaNs

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.

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
- ⊗ DatSniff
  Incorrect
- ✓ 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
- ○ Icann

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 ____.

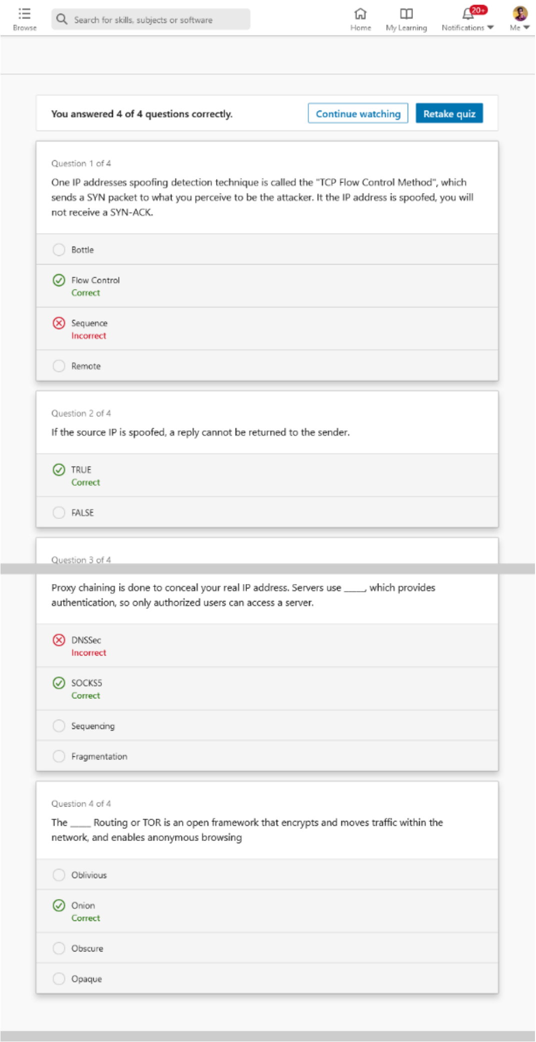
- ⊗ 101-443
  Incorrect
- ✓ 1-1023
  Correct
- ○ 1-797
- ⊗ 2-143
  Incorrect

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



You answered 4 of 4 questions correctly.

Question 1 of 4

One IP addresses spoofing detection technique is called the "TCP Flow Control Method", which sends a SYN packet to what you perceive to be the attacker. It the IP address is spoofed, you will not receive a SYN-ACK.

- ○ Bottle
- ✓ Flow Control
  Correct
- ☒ Sequence
  Incorrect
- ○ Remote

Question 2 of 4

If the source IP is spoofed, a reply cannot be returned to the sender.

- ✓ TRUE
  Correct
- ○ FALSE

Question 3 of 4

Proxy chaining is done to conceal your real IP address. Servers use ____, which provides authentication, so only authorized users can access a server.

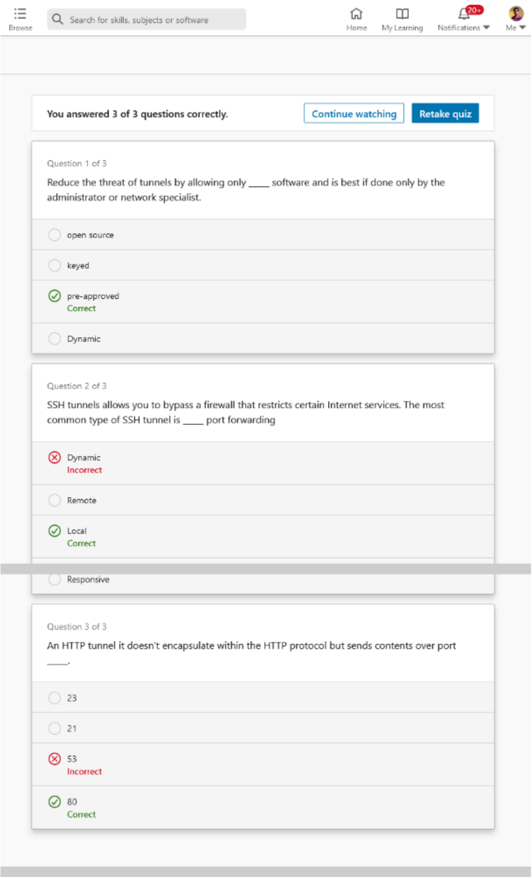
- ☒ DNSSec
  Incorrect
- ✓ SOCKS5
  Correct
- ○ Sequencing
- ○ Fragmentation

Question 4 of 4

The ____ Routing or TOR is an open framework that encrypts and moves traffic within the network, and enables anonymous browsing

- ○ Oblivious
- ✓ Onion
  Correct
- ○ Obscure
- ○ Opaque

Figure: Section 07 – Blueprint-the-Network-Assessment



You answered 3 of 3 questions correctly.

Question 1 of 3

Reduce the threat of tunnels by allowing only ____ software and is best if done only by the administrator or network specialist.

- ○ open source
- ○ keyed
- ✓ pre-approved
  Correct
- ○ Dynamic

Question 2 of 3

SSH tunnels allows you to bypass a firewall that restricts certain Internet services. The most common type of SSH tunnel is ____ port forwarding

- ☒ Dynamic
  Incorrect
- ○ Remote
- ✓ Local
  Correct
- ○ Responsive

Question 3 of 3

An HTTP tunnel it doesn't encapsulate within the HTTP protocol but sends contents over port ____.

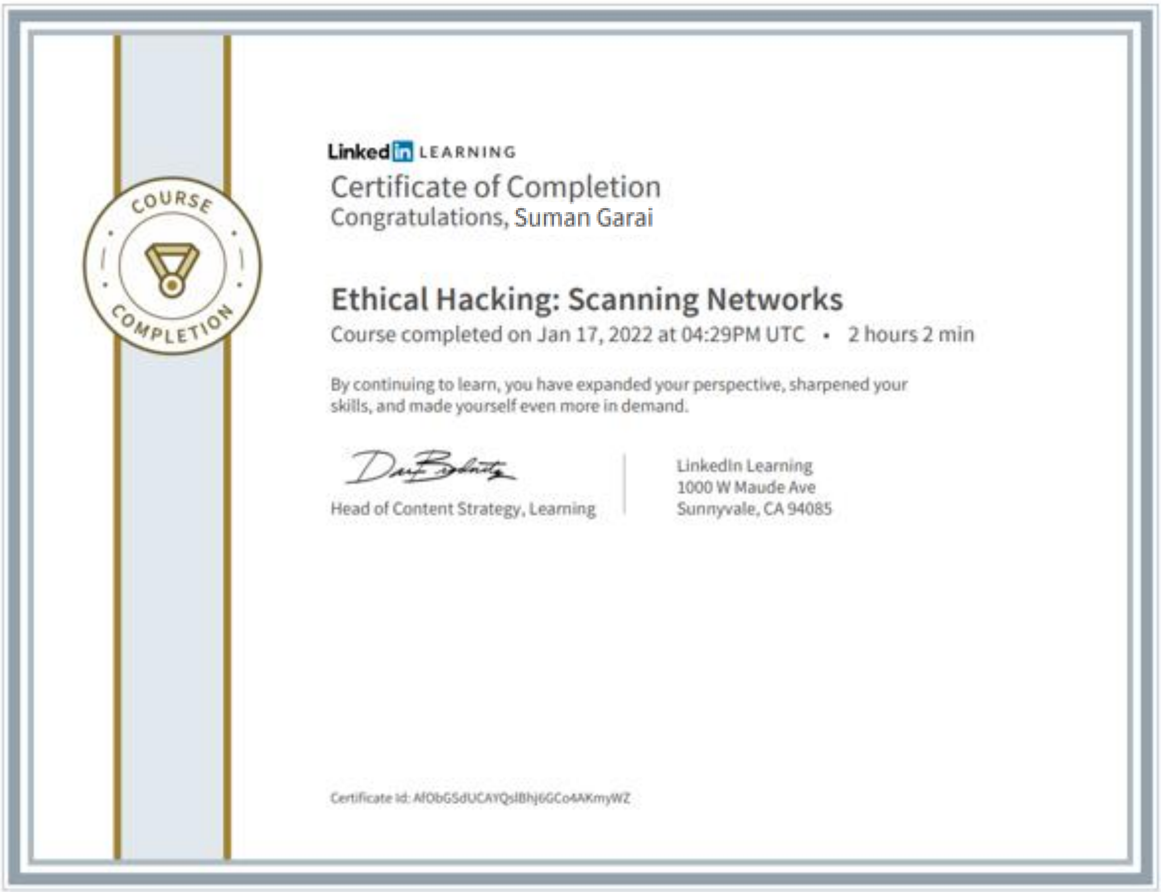
- ○ 23
- ○ 21
- ☒ 53
  Incorrect
- ✓ 80
  Correct

Figure: Section 08- Vulnerability-Scanning-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



Linked in LEARNING

Certificate of Completion

Congratulations, Suman Garai

COURSE
COMPLETION

Ethical Hacking: Scanning Networks

Course completed on Jan 17, 2022 at 04:29PM UTC • 2 hours 2 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: AfObGSdUCAYQslBhj6GCo4AKmyWZ