Unit 14 - Week 12

Assignment 12

Due on 2019-10-03 22:58:05

Course outline
Announcements About the Course Ask a Question Progress 

Assignment 12

How does NMAP perform host discovery using TCP SYN packets?

- Send an ICMP port-unreachable packet to the target and look for an ICMP reply packet.
- Send an ICMP port-unreachable packet to the target and look for a TCP SYN packet.
- Send an ICMP echo-request packet to the target and look for a corresponding ICMP echo-reply packet.
- Send a TCP SYN packet to the target.

1 point

TCP SYN flood DoS? NMAP sends a TCP SYN packet to a target on a particular port number and connects to that target on a port number.

- A TCP reply packet with the AC and TOS flags set.
- A TCP SYN packet with the AC and TOS flags set.
- A TCP SYN packet with the EEC flag set.
- None of these.

1 point

Which MAP option comes on a UDP flood host discovery?

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

What is the basic principle behind TCP Connect Scan in NMAP?

- Start a random number of TCP connection requests using some source with the target using some random number to identify the port to scan.
- Start a random number of TCP connection requests using some source with the target using some random number to identify the port to scan.
- Start a random number of TCP connection requests using some source with the target using some random number to identify the port to scan.
- None of these.

1 point

If it is requested too many ports from 50 to 5000, how is this specified in NMAP?

- TCP/50-5000
- TCP/50:5000
- None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

What does the following NMAP command do?

- Start a random number of TCP connection requests using some source with the target using some random number to identify the port to scan.
- Start a random number of TCP connection requests using some source with the target using some random number to identify the port to scan.
- Start a random number of TCP connection requests using some source with the target using some random number to identify the port to scan.
- None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.

1 point

None of these.