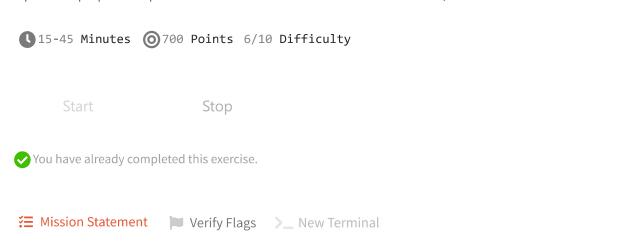
Labs

♦ back to dashboard

Lab 2 [Part 1] - Exploring Network Traces ♥ EXPIRED

Explore sample packet capture files to extract useful information about network, clients and traffic



Analyse the pcap file stored in /root/Desktop/pcap-analysis/dump.pcap with Wireshark and answer the questions from the Verify Flags section.

Make sure to answer all questions to mark the lab as "Completed"

Note

In case the lab fails to connect, hit Refresh from your browser to reload and auto-connect to the lab instance

1. Which device MAC was found sending DNS probes for doma	in d.d	lropbox	.com.eecs.umich.edu ?
00:1f:c6:8f:29:17		~	◎ 50 Points
2. Identify the manufacturer for device MAC: a4:2b:8c:f6:eb:81			
Netgear		~	30 Points
a Which do in MAC found in the interest of the control of th	,		
 Which device MAC was found inactive in the packet capture? Hint: Possibly a Wireless LAN controller 	:		
			8
00:1f:6d:e8:18:00			◎ 50 Points
4. Which 2 network ranges are discovered from the packet cap	ture?		
Hint: 10.1.1.1/24 172.17.1.1/24 , exclude 192.168.1.1			
10.0 2.1/24.102.122.104.1/24			(a) 40 Points
10.0.2.1/24 192.122.184.1/24		J	9 101 22
5. Identify the MAC address of the Class-C router gateway			
a4:2b:8c:f6:eb:81		~	⊚ 50 Points
6. Which device seems to be a uPnP device? Enter IP			
Try to filter udp.port==1900			
239.255.255.250	~	() 40 Pc	ints
7. One of the clients connects to an FTP server during the trace. What is	s the DN		
dl.xs4all.nl	*	◎ 50 Po	ints
8. Is the connection using Active or Passive FTP?			
Active FTP	~	(40 Pc	ints
9. Which username was discovered from the FTP packet capture?			
laticia.langhans	*	③ 30 Po	ints
10. Which item is used as a password as per the packet capture?			
Enter variable name or the Response arg text			
E-mail	~	(40 Pc	ints

11. Name at least two network protocols that can be used in place of FTP to provide secure file transfer					
Syntax: <protocol 1=""> <protocol 2=""></protocol></protocol>					
SFTP MFTP	~	⊚ 20 F	oints		
12. What is the domain name of the SSL encrypted site the client is connecting to of	ther tha	n facebo	ok.com		
www.pnc.com	~	⊚ 30 F	oints		
13. During the TLS handshake, the client provides a list of supported cipher suites.	Name a	ny one o	f the cip	her suites	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	~	⊚ 40 F	Points		
14. What cipher-suite does the server choose for the connection?					
TLS_RSA_WITH_RC4_128_MD5	~	⊚ 60 F	Points		
15. What version of TLS is being used for facebook.com?					
TLS 1.1	~	⊚ 30 F	oints		
16. Which version of TLS is suggested to prevent the SSL downgrade attacks in the I	PCAP?				
TLS 1.3	~	⊚ 30 F	Points		
17. Identify the URL user visited after visiting http://www.facebook.com	n/hom	e.php?			
/ai.php?ego=AT5yExWqpbjx3PTD4iwwQGJBCTx0kHyHnVvUCl	R5szU	sZTc	~	O 40 Points	
18. Which user's profile did the target user looked at apart from his own	n? Nan	ne userr	name		
zakirbpd			Y	30 Points	