TryHackMe

Julien ROYON CHALENDARD

CTF: Nmap

Catégorie : Network

Sommaire

1	\mathbf{Intr}	oduction	3
	1.1	What networking constructs are used to direct traffic to the right	
		application on a server?	3
	1.2	How many of these are available on any network-enabled computer?.	3
	1.3	[Research] How many of these are considered "well-known"? (These	0
		are the "standard" numbers mentioned in the task)	3
2	Nma	ap Switches	3
	2.1	What is the first switch listed in the help menu for a 'Syn Scan' (more	
		on this later!)?	3
	2.2	Which switch would you use for a "UDP scan"?	3
	2.3	If you wanted to detect which operating system the target is running	
		on, which switch would you use?	3
	2.4	Nmap provides a switch to detect the version of the services running	
		on the target. What is this switch?	3
	2.5	The default output provided by nmap often does not provide enough	
		information for a pentester. How would you increase the verbosity? .	3
	2.6	Verbosity level one is good, but verbosity level two is better! How	
		would you set the verbosity level to two?	4
	2.7	What switch would you use to save the nmap results in three major	
		formats?	4
	2.8	What switch would you use to save the nmap results in a "normal"	
		format?	4
	2.9	A very useful output format : how would you save results in a "gre-	
	2.40	pable" format?	4
		How would you activate this setting?	4
		How would you set the timing template to level 5?	4
		How would you tell nmap to only scan port 80?	4
		How would you tell nmap to scan ports 1000-1500?	4
		How would you tell nmap to scan all ports?	4
		How would you activate a script from the nmap scripting library (lots	4
	0.16	more on this later!)?	
	2.10	How would you activate all of the scripts in the "vuln" category?	5
3	[Sca	n Types TCP Connect Scans	5
	3.1	Which RFC defines the appropriate behaviour for the TCP protocol?	5
	3.2	If a port is closed, which flag should the server send back to indicate	
		this?	5
4	[Sca	n Types SYN Scans	5
-	4.1	There are two other names for a SYN scan, what are they?	5
	4.2	Can Nmap use a SYN scan without Sudo permissions (Y/N) ?	5

5	[Scan Types] UDP Scans			
	5.1	If a UDP port doesn't respond to an Nmap scan, what will it be	-	
	5.2	marked as?		
	• -	back a "port unreachable" message. Which protocol would it use to		
		do so?	5	
6	[Sca	n Types] NULL, FIN and Xmas	6	
	6.1	Which of the three shown scan types uses the URG flag?	6	
	6.2	Why are NULL, FIN and Xmas scans generally used?	6	
	6.3	Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?	6	
	_	v -		
7	-	n Types] ICMP Network Scanning	6	
	7.1	How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)	6	
_	[a.co	, <u> </u>		
8	[NS. 8.1	E Scripts] Overview What language are NSE scripts written in?	6	
	8.2	Which category of scripts would be a very bad idea to run in a pro-		
		duction environment?	6	
9	[NS	E Scripts Working with the NSE	6	
	•	What optional argument can the ftp-anon.nse script take?	6	
10	[NS	E Scripts Searching for Scripts	7	
	-	What is the filename of the script which determines the underlying	•	
	10.0	OS of the SMB server?	7	
	10.2	Read through this script. What does it depend on?	7	
11		ewall Evasion	7	
	11.1	Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?	-	
	11.2	[Research] Which Nmap switch allows you to append an arbitrary	(
		length of random data to the end of packets?	7	
12	Prac	ctical	7	
		Does the target (MACHINE_IP)respond to ICMP (ping) requests	•	
		(Y/N)?	7	
	12.2	Perform an Xmas scan on the first 999 ports of the target – how many ports are shown to be open or filtered?	7	
	12.3	Perform a TCP SYN scan on the first 5000 ports of the target – how	1	
		many ports are shown to be open?	7	
	12.4	Deploy the ftp-anon script against the box. Can Nmap login successfully to the ETP server on part 21.2 (V/N)	-	
		fully to the FTP server on port 21? (Y/N)	1	

1 Introduction

1.1 What networking constructs are used to direct traffic to the right application on a server?

Ports

1.2 How many of these are available on any network-enabled computer?

65535

1.3 [Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024

2 Nmap Switches

2.1 What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS

2.2 Which switch would you use for a "UDP scan"?

-sU

2.3 If you wanted to detect which operating system the target is running on, which switch would you use?

-O

2.4 Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

2.5 The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

 $-\mathbf{v}$

2.6 Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two? -VV 2.7 What switch would you use to save the nmap results in three major formats? -oA What switch would you use to save the nmap results in 2.8 a "normal" format? -oN A very useful output format: how would you save results in a "grepable" format? -oG How would you activate this setting? 2.10 -A 2.11How would you set the timing template to level 5? -T5 How would you tell nmap to only scan port 80? 2.12-р 80 How would you tell nmap to scan ports 1000-1500? 2.13 -р 1000-1500 How would you tell nmap to scan all ports? 2.14 -p-How would you activate a script from the nmap scrip-2.15

ting library (lots more on this later!)?

-script

2.16 How would you activate all of the scripts in the "vuln" category?

-script = vuln

3 [Scan Types] TCP Connect Scans

3.1 Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 793

3.2 If a port is closed, which flag should the server send back to indicate this?

RST

- 4 [Scan Types] SYN Scans
- 4.1 There are two other names for a SYN scan, what are they?

Half-Open, Stealth

4.2 Can Nmap use a SYN scan without Sudo permissions (Y/N)?

Ν

- 5 [Scan Types] UDP Scans
- 5.1 If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

open|filtered

5.2 When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?

ICMP

- 6 [Scan Types] NULL, FIN and Xmas
- 6.1 Which of the three shown scan types uses the URG flag? $_{\rm xmas}$
- 6.2 Why are NULL, FIN and Xmas scans generally used?

 Firewall Evasion
- 6.3 Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Microsoft Windows

- 7 [Scan Types] ICMP Network Scanning
- 7.1 How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

nmap -sn 172.16.0.0/16

- 8 [NSE Scripts] Overview
- 8.1 What language are NSE scripts written in? $_{\text{Lua}}$
- 8.2 Which category of scripts would be a very bad idea to run in a production environment?

intrusive

- 9 [NSE Scripts] Working with the NSE
- 9.1 What optional argument can the ftp-anon.nse script take? $_{
 m maxlist}$

10 [NSE Scripts] Searching for Scripts

10.1 What is the filename of the script which determines the underlying OS of the SMB server?

smb-os-discovery.nse

10.2 Read through this script. What does it depend on?
smb-brute

11 Firewall Evasion

- 11.1 Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

 ICMP
- 11.2 [Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

 -data-length

12 Practical

12.1 Does the target (MACHINE_IP)respond to ICMP (ping) requests (Y/N)?

Ν

- 12.2 Perform an Xmas scan on the first 999 ports of the target how many ports are shown to be open or filtered?
- 12.3 Perform a TCP SYN scan on the first 5000 ports of the target how many ports are shown to be open?
- 12.4 Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21 ? (Y/N)

Y

5