

MR. ROBOT

1. In this challenge there is a screenshot that shows the output of an Nmap scan. Its is up to use to find the useful information from this Nmap scan which includes the open port numbers and the Operating System that the host is.

Challenge 0 Solved ×

Holes in Security


400

Learning outcomes:

nmap is a very powerful port scanning tool and much more that can identify an OS and run different scripts to determine vulnerabilities. In this challenge there is a nmap scan done on a particular target and by the end of the challenge you will be able to understand the output of an output scan and the important information outputted to concentrate on

Seems to be an output of an nmap scan, holes in security, weakness's, exactly what a hacker wants to see in a system. Looks like the flag for this challenge is to name the open ports and the OS of this particular challenge.

Syntax EVILCORP_CTF{PORTNUMBER,PORTNUMBER,OS}
Example EVILCORP_CTF{21,23,WINDOWS}

 Screenshot....

Flag

Submit

2. So the Nmap scan can be seen below and looking at the scan the open ports can be seen in the first red box and these are port 22 and 5000. The next red box shows the Operating System this machine is running which is Linux so these are the answers to the flag.

```
$ nmap -sV -v -n 10.10.10.226
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-30 21:00 UTC
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 21:00
Scanning 10.10.10.226 [2 ports]
Completed Ping Scan at 21:00, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 21:00
Scanning 10.10.10.226 [1000 ports]
Discovered open port 22/tcp on 10.10.10.226
Discovered open port 5000/tcp on 10.10.10.226
Completed Connect Scan at 21:00, 0.17s elapsed (1000 total ports)
Initiating Service scan at 21:00
Scanning 2 services on 10.10.10.226
Completed Service scan at 21:01, 6.05s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.226.
Initiating NSE at 21:01
Completed NSE at 21:01, 0.06s elapsed
Initiating NSE at 21:01
Completed NSE at 21:01, 0.04s elapsed
Nmap scan report for 10.10.10.226
Host is up (0.0096s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
5000/tcp   open  httpd     Werkzeug httpd 0.16.1 (Python 3.8.5)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
```

- Put EVILCORP_CTF{22,5000,LINUX} to complete the challenge.

Challenge

0 Solves

×

Holes in Security


400

Learning outcomes:

nmap is a very powerful port scanning tool and much more that can identify an OS and run different scripts to determine vulnerabilities. In this challenge there is a nmap scan done on a particular target and by the end of the challenge you will be able to understand the output of an output scan and the important information outputted to concentrate on

Seems to be an output of an nmap scan, holes in security, weakness's, exactly what a hacker wants to see in a system. Looks like the flag for this challenge is to name the open ports and the OS of this particular challenge.

Syntax EVILCORP_CTF{PORTNUMBER,PORTNUMBER,OS}
Example EVILCORP_CTF{21,23,WINDOWS}

 Screenshot_...

EVILCORP_CTF{22,5000,LINUX}

Submit

