Enumeration

2021年7月26日 15:16

1: Use autorecon to enumerate its services, **21, 242, 3145, 3389** are open
2: FTP supports **anonymous** login, the root folder looks like **zFTP**'s root folder
3: Port **242** is a **HTTP** service, it has **basic authentication**
4: Weak and common default credentials do not work for the basic authentication
5: Look back FTP's list, there are **3 uac files**, indicating **existed three users**: anonymous, **admin**, Offsec.
6: Try to use another pair of credential to log in FTP, **admin:admin**. And it works.
7: This time, the folder looks like the **same folder** as HTTP service's.
8: There are two interesting files, **.htaccess** and **.htpasswd**. .htaccess is used for **implementing basic authentication**, while .htpasswd store offsec's **hashed password**
9: Use hashcat to crack the hash, the plaintext password is **elite**
10: Try to use this pair of credential to log in FTP service on port 21 and 3145, and all failed.
11: Use it to log in HTTP service's basic authentication, it works, however, there is **nothing interesting**

Foothold

2021年7月26日 15:17

1: Look back to user **admin's** FTP folder, try to upload a php shell, and it succeeds.
2: Access its URL, and I can execute command with the shell
3: Upload nc to target server, set up a netcat listener, use target server's netcat to connect back
4: Get a reverse shell. The user is **apache**

Privilege Escalation

2021年7月26日 15:17

1: Upload winpeas.exe to target server, and run it. However, there is **no response**.
2: Manually enumerate some basic info, and I notice its **system version** is quite **old**, which has a **local privilege escalation exploit**. The exploit can be found here (https://github.com/abatchy17/WindowsExploits/blob/master/MS11-046/MS11-046.exe)
3: Run the exploit, get a system shell

Review

2021年7月26日 15:17

1: Target **FTP** service
2: Not only anonymous account can log in FTP, but also **other users**. They have **different root folders**
3: Identify anonymous user's folder to realize **existed other users**
4: Switch to **admin's** folder (guess a **weak password** or brute force it), upload a web shell
5: Identify the **old system version**, exploit its **kernel's vulnerability**