SecDojo - Westeros Lab

Exposed machine write up

Information

• Name: Westeros Lab - Exposed Machine

Profile: SecDojoDifficulty: Easy

• **Description:** Westeros is a network of vulnerable Windows servers. Each box suffers from a severe vulnerability that if properly exploited, will grant you administrator access and get you the root flag located at the Administrator desktop folder.

Enumeration

Nmap

We begin our reconnaissance by running an Nmap scan checking services and their versions also checking default scripts and testing for vulnerabilities.

```
1 $ nmap -Pn -sC -sV -T4 172.16.4.235
 2 Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-28 17:19 UTC
3 Nmap scan report for 172.16.4.235
4 Host is up (0.00033s latency).
5 Not shown: 990 filtered tcp ports (no-response)
6 PORT
            STATE SERVICE
7 80/tcp open http
                                       HttpFileServer httpd 2.3
8 | http-title: HFS /
9 _http-server-header: HFS 2.3
10 135/tcp open msrpc Microsoft Windows RPC
11 139/tcp open netbios-ssn Microsoft Windows netbios-ssn
12 445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 -
       2012 microsoft-ds
13 3389/tcp open ssl/ms-wbt-server?
14 | rdp-ntlm-info:
15
       Target_Name: WIN-NPIKVT9GRJD
16
       NetBIOS_Domain_Name: WIN-NPIKVT9GRJD
17 NetBIOS_Computer_Name: WIN-NPIKVT9GRJD
18
       DNS_Domain_Name: WIN-NPIKVT9GRJD
19
       DNS Computer Name: WIN-NPIKVT9GRJD
20
       Product_Version: 6.3.9600
21 | System_Time: 2022-12-28T17:20:47+00:00
   ssl-cert: Subject: commonName=WIN-NPIKVT9GRJD
22
   | Not valid before: 2022-12-27T14:21:48
24 | Not valid after: 2023-06-28T14:21:48
25 |_ssl-date: 2022-12-28T17:21:27+00:00; 0s from scanner time.
                            Microsoft Windows RPC
Microsoft Windows RPC
26 49152/tcp open msrpc
27 49153/tcp open msrpc
28 49154/tcp open msrpc Microsoft Windows RPC
```

```
29 49155/tcp open msrpc
                                    Microsoft Windows RPC
                                     Microsoft Windows RPC
30 49165/tcp open msrpc
31 Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:
      microsoft:windows
32
33 Host script results:
34  | _nbstat: NetBIOS name: WIN-NPIKVT9GRJD, NetBIOS user: <unknown>,
      NetBIOS MAC: 06:59:e3:a0:ce:ca (unknown)
35 | smb2-security-mode:
36
      3.0.2:
       Message signing enabled but not required
38 | smb-security-mode:
39 | account_used: guest
40
     authentication_level: user
41
       challenge_response: supported
42 _ message_signing: disabled (dangerous, but default)
43 | smb2-time:
       date: 2022-12-28T17:20:47
44
45 | start_date: 2022-12-28T14:20:25
46
47 Service detection performed. Please report any incorrect results at
      https://nmap.org/submit/ .
48 Nmap done: 1 IP address (1 host up) scanned in 109.70 seconds
49 zsh: segmentation fault nmap -Pn -sC -sV -T4 172.16.4.235
```

From the above output we can see that ports, **80**, **135**, **139**, **445**, **3389**, **49152**, **49153**, **49154**, **49155** and **49165** are the open ports.

Searchsploit

I tried to run searchsploit to find some vulnerable services and found *Remote Command Execution* vulnerability on **HttpFileServer 2.3** service running on port 80 which is a web server specifically designed for publishing and sharing files.

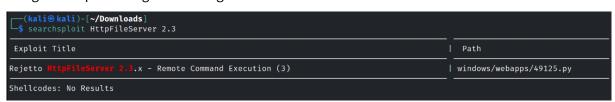


Figure 1: Searchsploit Results

Exploitation

Metasploit

I used metasploit to exploit RCE vulnerability.

Figure 2: *Metasploit meterpreter*

Root Flag

Figure 3: Administrator Desktop

Flag: Exposed_Sesco-r58l6r5xm6euy06vmn9gam12djyw2k8e