Ex150 Submission

Gary Jones

Contents

Project Overview

In summary, once s chisel session was made on costumes.artstailor.com a proxy nmap scan was able to identify the relevant IP address of dbc.artstailor.com. Following this identification the IP address was scanned for smb-related vulnerabilities. Once this was accomplished the EternalBlue exploit in Metasploit was used to gain access to bdc.artstailor.com. Through migrating processes, the domain account of artstailor was acquired.

Goals

The goal of this exercise is to get Domain administrative privileges.

Risk Ranking/Profile

The risk ranking of this exploit is medium as the available exploit enables third party users to execute code. However, despite being documented online I was unable to replicate the exploit as described.

Summary of Findings

I was able to identify that the available exploit was SMBv1.

Technical Report

Introduction

Vulnerability Description

The identified vulnerability is SMBv1 which is an EternalSynergy exploit that allows the execution of code via packets. Access to bdc.artstailor.com is available through port 445.

Mitigation or Resolution Strategy

This exploit can be mitigated by updating the SMB server to the latest version that has been patched to against EternalBlue exploits.

Attack Narrative

I set up a remote desktop with Costumes.artstailor.com (see figure 1). Following this I used nmap against the IP address 10.70.184.* on port 445 as this port is associated with SMB and identified that bdc.artstailor.com is accessbile (see figures 2 and 3). After this I confirmed that that the ip address was vulnerable toSMB by running the -script vuln flag (see figures 4 and 5).

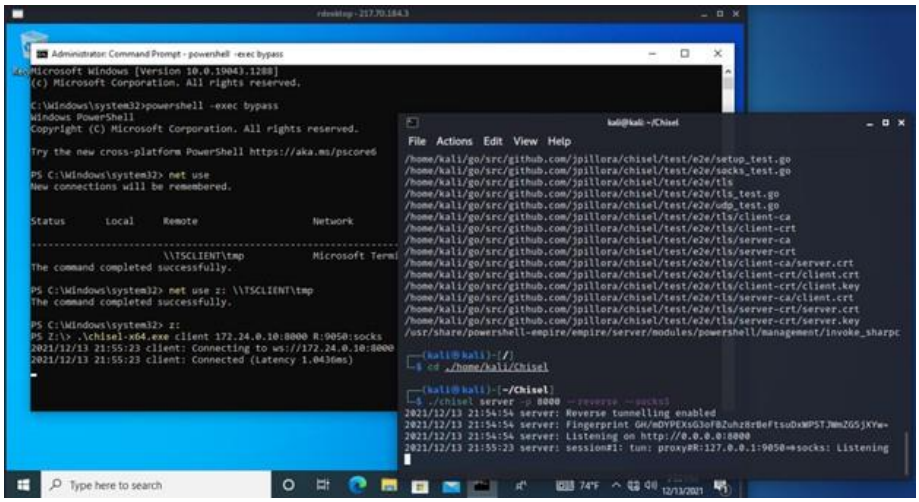

Figure 1:

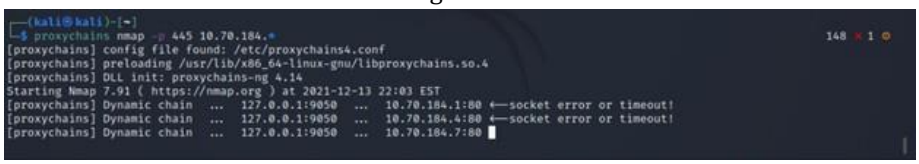

Figure 2:

Figure 3:

```
┌──(kali㉿kali)-[~]
└─$ proxychains nmap -Pn -sT -p 445 10.70.184.89 -script vuln
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-14 17:47 EST
```

Figure 4:

```
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:9050  ...  10.70.184.89:445  ...  OK
Nmap scan report for 10.70.184.89
Host is up (0.0064s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 30.15 seconds
```

Figure 5: