Penetration Test Exercise 09

Esteban Calvo

2023-10-17

Contents

1 Technical Report

Feel free to include an introduction if it suits your communication style. You may omit it if you prefer to do so.

1.1 Finding: *Root Access and Password Hashing*

Severity Rating

Critical
CVSS Base Severity Rating: 9.9 AV:N AC:L PR:L UI:N S:C C:H I:H A:H

Vulnerability Description

After running some scripts, I have root access to the local remote machine and potential access to other domain wide users account and information. Immediate action is required

Confirmation method

Create a new port forward to allow remote access to costumes rdp port when hitting mail.artstailor.com rdp port. Then copy our PowerDown.ps1 powershell to a filesystem to mount to remote destkop using the credentials previously found.

```
rdesktop mail.artstailor.com -r disk:win32=/tmp/<tmp>/
```

Open command prompt and navigate to mounted filesystem. Then run following commands

```
Import-Module \\TSCLIENT\win32\PowerDown.ps1
Do-ServiceAbuse -Name "VSS" -User <Username> -Password <Password>
```

Use these credentials to log back in as root user and then use Mimikatz to dump password hashes as follows

```
lsadump::sam
```

Mitigation or Resolution Strategy

It is once again imperative to make sure all users change their passwords to not allow any sort of access to the remote desktop. If an attacker were to gain access however, there should be checks in place to make sure no one but administrators can run powershell or command prompt scripts. Even stronger measures such as no access to powershell to all non-administrative users can be enforced.

2 Attack Narrative

2.1 Mounting Filesystem

To get access to the machine, the same steps as previously followed to gain access were taken. That is, a new port forward firewall rule was created and the same credentials as last time were used. This time though, a new flag was used to pass in a mounted directory to the desktop. A new file was created in tmp using mktmp -d and then PowerUp.ps1 was passed to this directory. Later discovery revealed that we instead needed PowerDown.ps1 to be passed into the tmp directory. To pass in the mounted directory with PowerDown.ps1 module, we can run the command

```
mktmp -d
cp Powershell/PowerDown.ps1 /tmp/<tmp>/
rdesktop mail.artstailor.com -r disk:win32=/tmp/<tmp>/
```

From here, we can switch to the mounted filesystem using the following commands from the command line

```
net use z: \\TSCLIENT\win32
powershell -exec bypass
z:
```

We now have access to the filesystem that was mounted from the local kali VM.

2.2 Root Access

We can now see the PowerDown.ps1 script that we copied over to the mounted filesystem. To run the script using powershell, we can use the following commands

```
Import-Module \\TSCLIENT\win32\PowerDown.ps1
Do-AllChecks
```

Which reveals a possible attack vector that will give us root access with the following function

```
Do-ServiceAbuse -Name "VSS" -User Esteban -Password G4t0r!=
```

We can now use these User and Password credentials to sign in and when we log back in, we can see that we have admin privileges that we did not have before.

2.3 Mimikatz

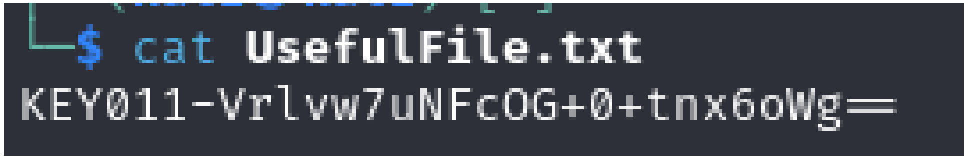
We can now go to the virus & threat protection section in the settings and disable real time protection as well as all the other virus protection policies set in place by Windows defender. The next step was to spin up an instance of command prompt as an administrator. On the local kali VM, we also want to make sure to move the mimikatz.exe executable to the mounted filesystem. Once we can see the executable on the remote desktop, we can then run it and use the following commands

```
.\mimikatz.exe
privilege::debug
lsadump::sam
```

This gives us a list of hashes for passwords on both the local machine as well as some domain login hashes that we can seek to exploit later.

2.4 Key

Because we now have administrator privileges, we can look around the directory for all users. Looking in the Administrator directory, a curious file by the name of UsefulFile.txt was found in the documents directory. Copying this to the z drive and opening on kali revealed the following key



```
└─$ cat UsefulFile.txt
KEY011-Vrlvw7uNFcOG+0+tnx6oWg==
```

2.5 MITRE ATT&CK Framework TTPs

TA0004: Privilege Escalation
    T1068: Exploitation for Privilege Escalation

TA0043: Reconnaissance
    T1595: Active Scanning
        .002: Vulnerability Scanning

TA0007: Discovery

- **T1087:** Account Discovery
  - **.001:** Local/Domain Account

TA0006: Credential Access

- **T1003:** Credential Access
  - **.002:** Security Account Manager