Open in app 7 Sign up Sign in

Medium Q Search







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

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free



Domain Controller computer account. This effectively allows a regular domain user to take control of a domain controller.

Adversaries will likely add this attack vector to their post exploitation and privilege escalation tradecraft. While mitigation should be the defenders main focus, detection and hunting controls can help to catch attackers attempting exploitation. This quick blog post highlights detection opportunities threat hunters can use to identify exploitation activity,.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

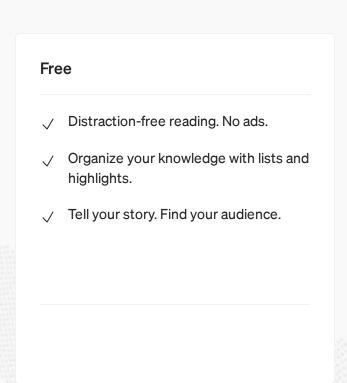


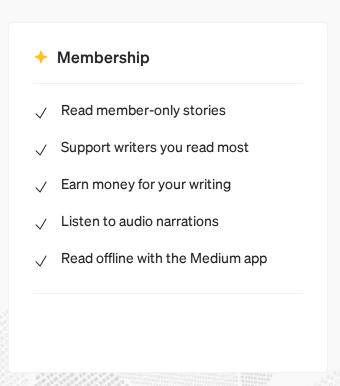
Hunting for samAccountName Spoofing (CVE-2021–42278) & Domain Controller Impersonation (CVE-2021–42287) | by Mauricio Velazco | Medium - 01/11/2024 12:47 https://medium.com/@mvelazco/hunting-for-samaccountname-spoofing-cve-2021-42287-and-domain-controller-impersonation-f704513c8a45

```
(kali⊕ kali)-[~/sam-the-admin]
 $ python sam_the_admin.py 'attackrange/reed_schmidt:Passw@rd12345!' -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
```

Medium

Sign up to discover human stories that deepen your understanding of the world.





This section provides a few hunting ideas leveraging the previously shown Event Ids. They are by no means flawless. Feedback is welcome!

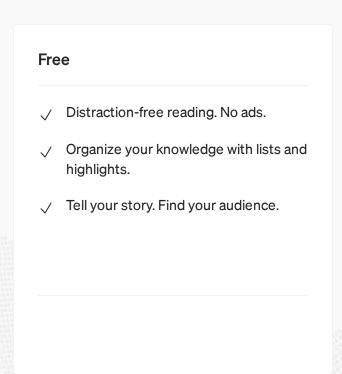
To test these ideas, I generated and used this dataset using public exploits: windows-security.log

Suspicious Computer Account Name Change

As part of the exploitation chain, attackers need to create a new computer account and rename it to match the name of a domain controller account without the ending '\$' Computer account names always end with `\$` and a

Medium

Sign up to discover human stories that deepen your understanding of the world.





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
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free ✓ Distraction-free reading. No ads. ✓ Organize your knowledge with lists and highlights. ✓ Tell your story. Find your audience.



Hunting for samAccountName Spoofing (CVE-2021–42278) & Domain Controller Impersonation (CVE-2021–42287) | by Mauricio Velazco | Medium - 01/11/2024 12:47 https://medium.com/@mvelazco/hunting-for-samaccountname-spoofing-cve-2021-42287-and-domain-controller-impersonation-f704513c8a45

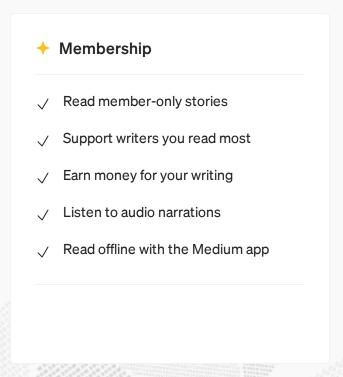
```
| search suspicious = TRUE
| table _time, ComputerName, EventCode,
Account_Name,RenamedComputerAccount, suspicious
```

Happy Hunting and Happy Holidays

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free Distraction-free reading. No ads. Organize your knowledge with lists and highlights. Tell your story. Find your audience.







261 Followers

@mvelazco #AdversarySimulation #ThreatDetection #PurpleTeam

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Membership
 ✓ Read member-only stories
 ✓ Support writers you read most
 ✓ Earn money for your writing
 ✓ Listen to audio narrations
 ✓ Read offline with the Medium app