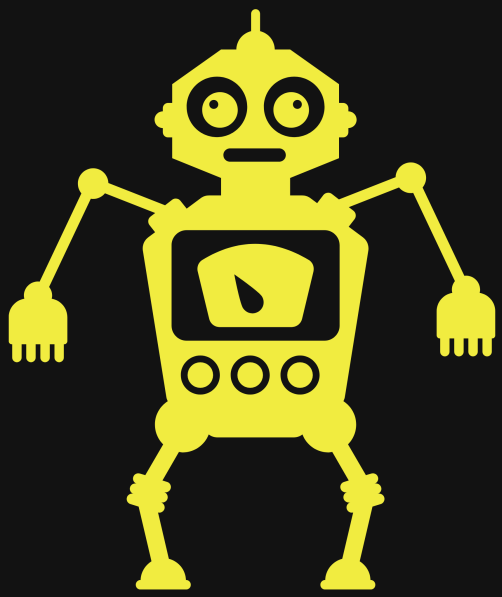
Intro

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

- Hostname1
  - www-data to user
    - *What version of OS?*
    - *Is the AV up and running?*
    - *What group does www-data belong too and what are its rights?*
    - *What other users are on the system and what are there groups?*
    - *What is the network topology to this Node?*
    - *What access do I have to files and folders?*
    - *What are the applications, services, programs and there versions?*
    - *From www-data to user*
  - user to admin
    - *What version of OS?*
    - *Is the AV up and running?*
    - *What group does www-data belong too and what are its rights?*
    - *What other users are on the system and what are there groups?*
    - *What is the network topology to this Node?*

- Entire Nessus Scan

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.

Certifications held by Robert Garcia

Scope

You have been chosen by Iron Corp to conduct a penetration test of their asset. They did system hardening and are expecting you not to be able to access their system.

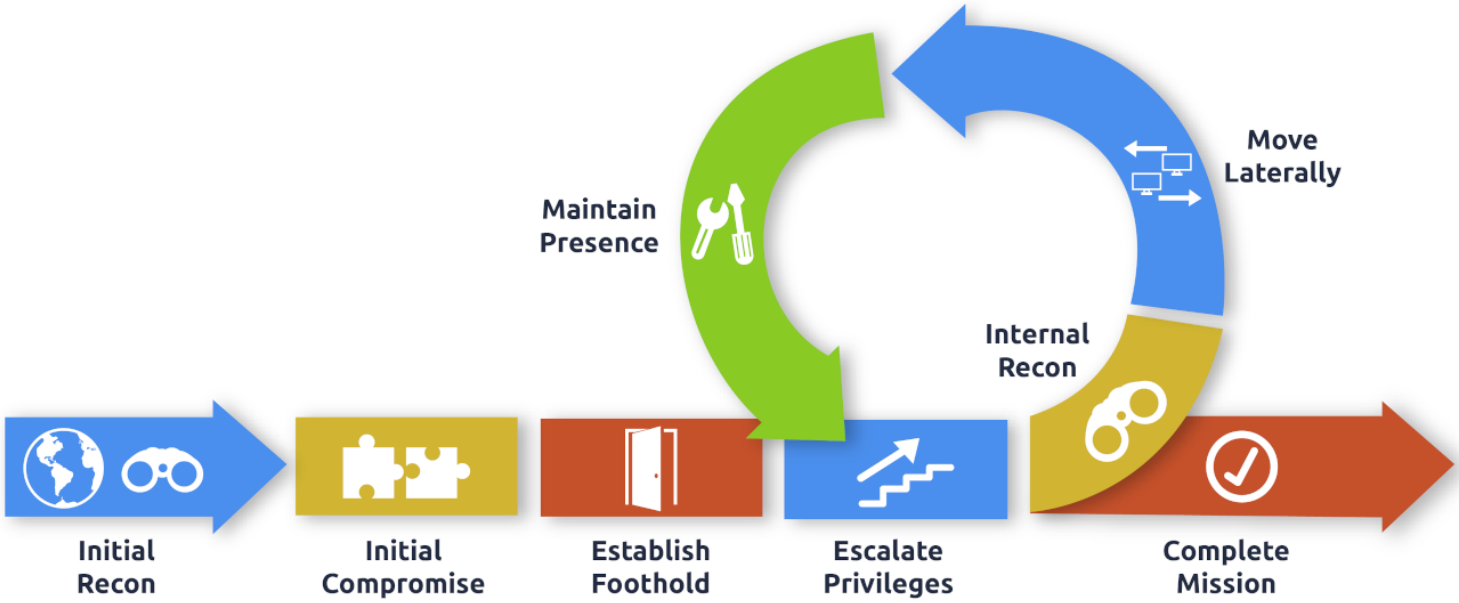
The asset in scope is: ironcorp.me

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.



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

Timeline

Finding's & Remediation

HOSTNAME (IP)

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

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

Remediation

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

---

Attack Narrative

OSINT

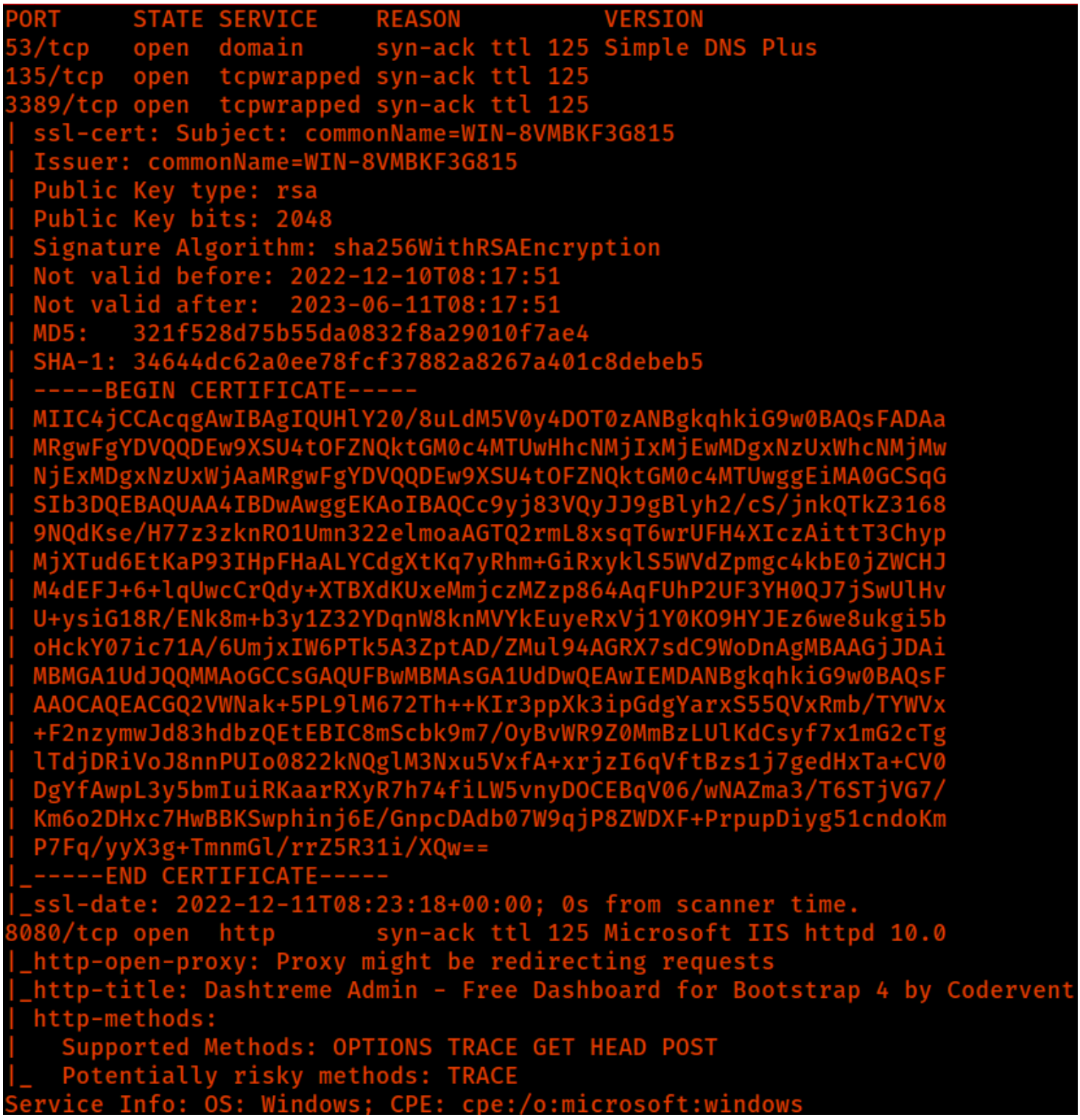
Target IP can change during engagement

```
export TargetIP=10.10.20.22
```

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 10.10.20.22 --min-rate 5000
```

Screenshot: (Find entire scans in appendix)



After our basic scan we are going to do a deeper

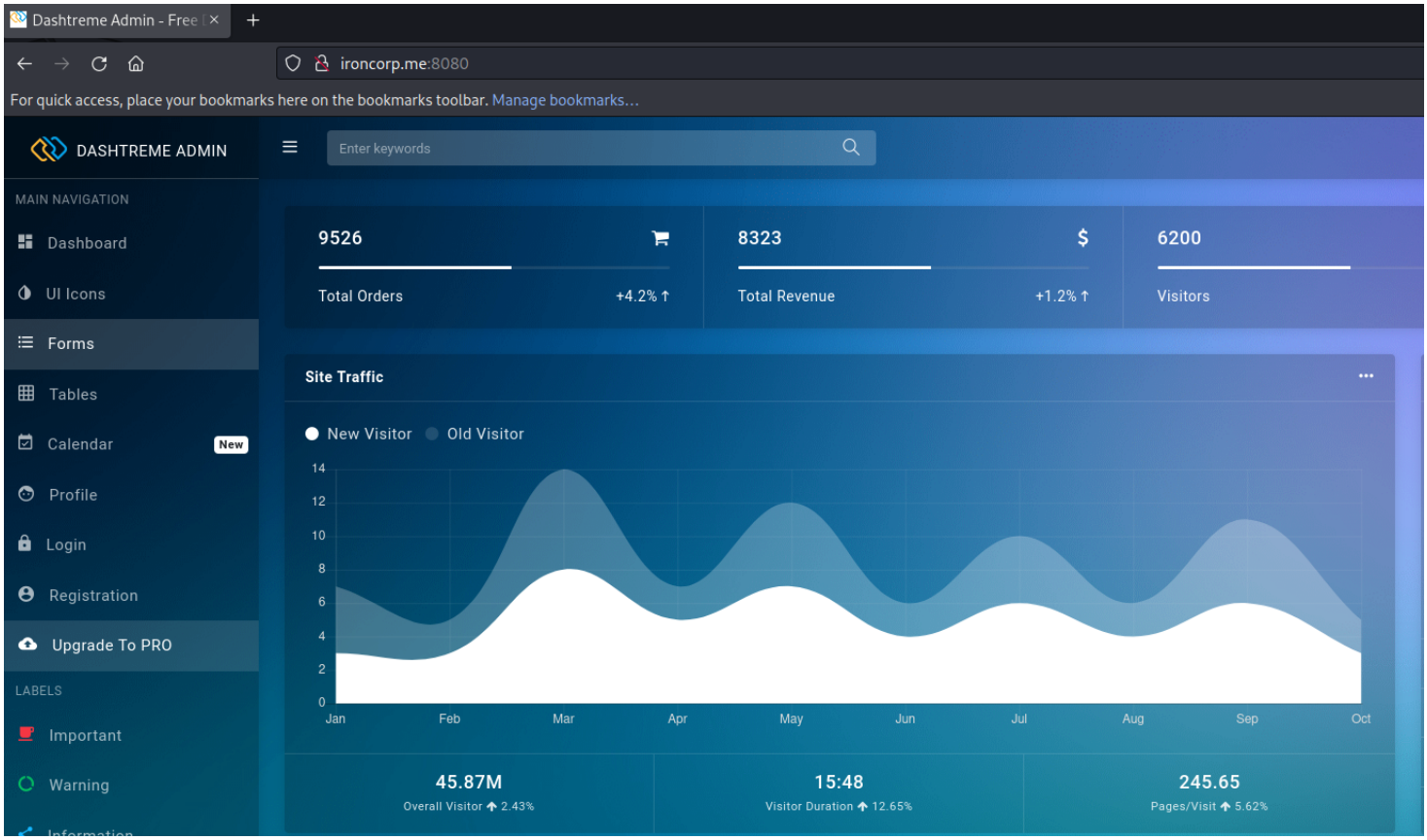
scan to see if we can pickup any extra services that I might have missed.

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln  $TargetIP
```

Screenshot: (Find entire scans in appendix)

Discovery

I wanted to take a look at the website since we know something is being hosted on port 8080.



I wanted to see if we can grab what we can from the website.

```
wget -r --no-parent http://ironcorp.me:8080/
```

```
ironcorp.me:8080/reset-password.html    100%[===================================================

2022-12-11 03:44:32 (821 MB/s) - 'ironcorp.me:8080/reset-password.html' saved [3563/3563]

FINISHED --2022-12-11 03:44:32--
Total wall clock time: 2m 24s
Downloaded: 576 files, 13M in 1.5s (8.35 MB/s)

┌──(kali㉿kali)-[~/…/Scan/Internal_Network/Manual_scans/Port_8080]
```

Seems we got a few files to look at here. Another

tool I ran was Photon. This is to collect any end points or interesting files I might have missed from the wget scan.

```
photon -u http://ironcorp.me:8080/ -l 3 -t 100
```

![[Pasted image 20221211034848.png]] From looking at the Tables section of the website we can see users of some sort. ![[Pasted image 20221211035805.png]] We found another page as well that seems to have users. ![[Pasted image 20221211041120.png]] We start to build a username list with what we found above. After digging around we found a username format to the website. ![[Pasted image 20221211041325.png]] We can see the the name convention is last name and then first name.

Initial Foot hold

Hostname1

---

www-data to user

Username:Password

```
```

Proof of www-data

What version of OS?

CMD used:

```
```

Screenshot of output

Is the AV up and running?

CMD used:

```
```

Screenshot of output

What group does www-data belong too and what are its rights?

CMD used:

```
```

Screenshot of output

What other users are on the system and what are there groups?

CMD used:

```
```

Screenshot of output

What is the network topology to this Node?

CMD used:

```
```

Screenshot of output

What access do I have to files and folders?

CMD used:

```
```

Screenshot of output

What are the applications, services, programs and there versions?

CMD used:

```
```

Screenshot of output

From www-data to user

CMD used:

```
[redacted]
```

Screenshot of output

user to admin

Username:Password

```
[redacted]
```

Proof of www-data

What version of OS?

CMD used:

```
[redacted]
```

Screenshot of output

Is the AV up and running?

CMD used:

```
[redacted]
```

Screenshot of output

What group does www-data belong too and what are its rights?

CMD used:

```
[redacted]
```

Screenshot of output

What other users are on the system and what are there groups?

CMD used:

Screenshot of output

What is the network topology to this Node?

CMD used:

Screenshot of output

What access do I have to files and folders?

CMD used:

Screenshot of output

What are the applications, services, programs and there versions?

CMD used:

Screenshot of output

From user to admin

CMD used:

```
```

Screenshot of output

Clean UP

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 Scan Full

```
 sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 10.10.20.22 --min-rate 5000

Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-11
03:22 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:22
Completed NSE at 03:22, 0.00s elapsed
Initiating SYN Stealth Scan at 03:22
```

```
Scanning ironcorp.me (10.10.20.22) [65535 ports]
Discovered open port 8080/tcp on 10.10.20.22
Discovered open port 3389/tcp on 10.10.20.22
Discovered open port 135/tcp on 10.10.20.22
Discovered open port 53/tcp on 10.10.20.22
Increasing send delay for 10.10.20.22 from 0 to 5 due to
11 out of 21 dropped probes since last increase.
Completed SYN Stealth Scan at 03:22, 26.77s elapsed
(65535 total ports)
Initiating Service scan at 03:22
Scanning 4 services on ironcorp.me (10.10.20.22)
Completed Service scan at 03:23, 9.82s elapsed (4
services on 1 host)
NSE: Script scanning 10.10.20.22.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:23
Completed NSE at 03:23, 17.71s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:23
Completed NSE at 03:23, 8.13s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:23
Completed NSE at 03:23, 0.00s elapsed
Nmap scan report for ironcorp.me (10.10.20.22)
Host is up, received user-set (0.20s latency).
Scanned at 2022-12-11 03:22:23 EST for 63s
Not shown: 65531 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 125 Simple DNS Plus
135/tcp  open  tcpwrapped syn-ack ttl 125
```

```
3389/tcp open  tcpwrapped syn-ack ttl 125
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Issuer: commonName=WIN-8VMBKF3G815
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-12-10T08:17:51
| Not valid after:  2023-06-11T08:17:51
| MD5:   321f528d75b55da0832f8a29010f7ae4
| SHA-1: 34644dc62a0ee78fcf37882a8267a401c8debeb5
| -----BEGIN CERTIFICATE-----
|
MIIC4jCCAcqgAwIBAgIQUHlY20/8uLdM5V0y4DOT0zANBgkqhkiG9w0BA
QsFADAa
|
MRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwHhcNMjIxMjEwMDgxNzUxW
hcNMjMw
|
NjExMDgxNzUxWjAaMRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwggEiM
A0GCSqG
|
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCc9yj83VQyJJ9gBlyh2/cS/jnkQ
TkZ3168
|
9NQdKse/H77z3zknRO1Umn322elmoaAGTQ2rmL8xsqT6wrUFH4XIczAit
tT3Chyp
|
MjXTud6EtKaP93IHpFHaALYCdgXtKq7yRhm+GiRxyklS5WVdZpmgc4kbE
0jZWCHJ
|
M4dEFJ+6+lqUwcCrQdy+XTBXdKUxeMmjczMZzp864AqFUhP2UF3YH0QJ7
jSwUlHv
```

```
|
U+ysiG18R/ENk8m+b3y1Z32YDqnW8knMVYkEuyeRxVj1Y0KO9HYJEz6we
8ukgi5b
|
oHckY07ic71A/6UmjxIW6PTk5A3ZptAD/ZMul94AGRX7sdC9WoDnAgMBA
AGjJDAi
|
MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9
w0BAQsF
|
AAOCAQEACGQ2VWNak+5PL9lM672Th++KIr3ppXk3ipGdgYarxS55QVxRm
b/TYWVx
|
+F2nzymwJd83hdbzQEtEBIC8mScbk9m7/OyBvWR9Z0MmBzLUlKdCsyf7x
1mG2cTg
|
lTdjDRiVoJ8nnPUIo0822kNQglM3Nxu5VxfA+xrjzI6qVftBzs1j7gedH
xTa+CV0
|
DgYfAwpL3y5bmIuiRKaarRXyR7h74fiLW5vnyDOCEBqV06/wNAZma3/T6
STjVG7/
|
Km6o2DHxc7HwBBKSwphinj6E/GnpcDAdb07W9qjP8ZWDXF+PrpupDiyg5
1cndoKm
| P7Fq/yyX3g+TmnmGl/rrZ5R31i/XQw==
|_-----END CERTIFICATE-----
|_ssl-date: 2022-12-11T08:23:18+00:00; 0s from scanner
time.
8080/tcp open  http       syn-ack ttl 125 Microsoft IIS
httpd 10.0
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Dashtreme Admin - Free Dashboard for
```

```
Bootstrap 4 by Codervent
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 0s

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 03:23
Completed NSE at 03:23, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 03:23
Completed NSE at 03:23, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 03:23
Completed NSE at 03:23, 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 62.86
seconds
           Raw packets sent: 131086 (5.768MB) | Rcvd: 10
(440B)
```

Nmap Scan Vul

```
# Nmap 7.93 scan initiated Sun Dec 11 03:26:57 2022 as:
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.10.20.22
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: dec333e8-37c8-49bf-bcfe-
38fa81689360
|         Address: http://192.168.202.1:5357/a12ace66-
c55b-467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
in Robtex's API. See https://www.robtex.com/api/
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: eth0
|     IP Offered: 192.168.202.130
|     DHCP Message Type: DHCPOFFER
```

```
|     Server Identifier: 192.168.202.254
|     IP Address Lease Time: 30m00s
|     Subnet Mask: 255.255.255.0
|     Router: 192.168.202.2
|     Domain Name Server: 192.168.202.2
|     Domain Name: localdomain
|     Broadcast Address: 192.168.202.255
|     NetBIOS Name Server: 192.168.202.2
|     Renewal Time Value: 15m00s
|_    Rebinding Time Value: 26m15s
| ipv6-multicast-mld-list:
|   fe80::922c:adf3:509:4b65:
|     device: eth0
|     mac: 005056c00008
|     multicast_ips:
|       ff02::1:ff09:4b65         (NDP Solicited-node)
|       ff02::1:ff59:8ceb         (Solicited-Node
Address)
|       ff02::1:3                 (Link-local Multicast
Name Resolution)
|       ff02::1:ff4d:7adf         (Solicited-Node
Address)
|       ff02::1:3                 (Link-local Multicast
Name Resolution)
|       ff02::1:3                 (Link-local Multicast
Name Resolution)
|       ff02::1:3                 (Link-local Multicast
Name Resolution)
|       ff02::1:3                 (Link-local Multicast
Name Resolution)
|       ff02::1:ff59:8ceb         (Solicited-Node
Address)
```

```
|       ff02::1:3                 (Link-local Multicast
Name Resolution)
|       ff02::1:ff4d:7adf         (Solicited-Node
Address)
|       ff02::fb                  (mDNSv6)
|       ff02::c                   (SSDP)
|_      ff02::1:3                 (Link-local Multicast
Name Resolution)
|_eap-info: please specify an interface with -e
| broadcast-igmp-discovery:
|   192.168.202.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.202.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution
(rfc4795)
|   192.168.202.1
|     Interface: eth0
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as
targets
| broadcast-listener:
|   ether
|       ARP Request
|         sender ip      sender mac    target ip
```

```
|         192.168.202.1  005056c00008  192.168.202.2
|         192.168.202.2  005056e3b4c7  192.168.202.130
|   udp
|       DHCP
|         srv ip           cli ip           mask
gw              dns             vendor
|         192.168.202.254  192.168.202.129  255.255.255.0
192.168.202.2  192.168.202.2  -
|         192.168.202.254  192.168.202.130  255.255.255.0
192.168.202.2  192.168.202.2  -
|         192.168.202.254  192.168.202.129  255.255.255.0
192.168.202.2  192.168.202.2  -
|       MDNS
|         Generic
|           ip             ipv6  name
|_          192.168.202.1        _teamviewer._tcp.local
| broadcast-ping:
|   IP: 192.168.202.2  MAC: 005056e3b4c7
|_  Use --script-args=newtargets to add the results as
targets
| targets-ipv6-multicast-slaac:
|   IP: fe80::4617:42c7:8459:8ceb  MAC: 005056c00008
IFACE: eth0
|   IP: fe80::d9ed:71cc:d24d:7adf  MAC: 005056c00008
IFACE: eth0
|_  Use --script-args=newtargets to add the results as
targets
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.202.1 fe80::922c:adf3:509:4b65
| targets-ipv6-multicast-mld:
```

```
|   IP: fe80::922c:adf3:509:4b65  MAC: 005056c00008
IFACE: eth0
|
|_  Use --script-args=newtargets to add the results as
targets
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for ironcorp.me (10.10.20.22)
Host is up, received user-set (0.27s latency).
Scanned at 2022-12-11 03:27:38 EST for 1955s
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON
53/tcp    open  domain        syn-ack ttl 125
| dns-zone-transfer:
| ironcorp.me.           SOA  win-8vmbkf3g815.
hostmaster.
| ironcorp.me.           NS   win-8vmbkf3g815.
| admin.ironcorp.me.     A    127.0.0.1
| internal.ironcorp.me.  A    127.0.0.1
|_ironcorp.me.           SOA  win-8vmbkf3g815.
hostmaster.
| dns-nsec-enum:
|_  No NSEC records found
| dns-nsec3-enum:
|_  DNSSEC NSEC3 not supported
135/tcp   open  msrpc         syn-ack ttl 125
3389/tcp  open  ms-wbt-server syn-ack ttl 125
|_ssl-date: 2022-12-11T08:34:51+00:00; 0s from scanner
time.
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
```

```
|     CredSSP with Early User Auth: SUCCESS
|_    RDSTLS: SUCCESS
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Issuer: commonName=WIN-8VMBKF3G815
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-12-10T08:17:51
| Not valid after:  2023-06-11T08:17:51
| MD5:   321f528d75b55da0832f8a29010f7ae4
| SHA-1: 34644dc62a0ee78fcf37882a8267a401c8debeb5
| -----BEGIN CERTIFICATE-----
|
MIIC4jCCAcqgAwIBAgIQUHlY20/8uLdM5V0y4DOT0zANBgkqhkiG9w0BA
QsFADAa
|
MRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwHhcNMjIxMjEwMDgxNzUxW
hcNMjMw
|
NjExMDgxNzUxWjAaMRgwFgYDVQQDEw9XSU4tOFZNQktGM0c4MTUwggEiM
A0GCSqG
|
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCc9yj83VQyJJ9gBlyh2/cS/jnkQ
TkZ3168
|
9NQdKse/H77z3zknRO1Umn322elmoaAGTQ2rmL8xsqT6wrUFH4XIczAit
tT3Chyp
|
MjXTud6EtKaP93IHpFHaALYCdgXtKq7yRhm+GiRxyklS5WVdZpmgc4kbE
0jZWCHJ
|
M4dEFJ+6+lqUwcCrQdy+XTBXdKUxeMmjczMZzp864AqFUhP2UF3YH0QJ7
```

```
jSwUlHv
|
U+ysiG18R/ENk8m+b3y1Z32YDqnW8knMVYkEuyeRxVj1Y0KO9HYJEz6we
8ukgi5b
|
oHckY07ic71A/6UmjxIW6PTk5A3ZptAD/ZMul94AGRX7sdC9WoDnAgMBA
AGjJDAi
|
MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9
w0BAQsF
|
AAOCAQEACGQ2VWNak+5PL9lM672Th++KIr3ppXk3ipGdgYarxS55QVxRm
b/TYWVx
|
+F2nzymwJd83hdbzQEtEBIC8mScbk9m7/OyBvWR9Z0MmBzLUlKdCsyf7x
1mG2cTg
|
lTdjDRiVoJ8nnPUIo0822kNQglM3Nxu5VxfA+xrjzI6qVftBzs1j7gedH
xTa+CV0
|
DgYfAwpL3y5bmIuiRKaarRXyR7h74fiLW5vnyDOCEBqV06/wNAZma3/T6
STjVG7/
|
Km6o2DHxc7HwBBKSwphinj6E/GnpcDAdb07W9qjP8ZWDXF+PrpupDiyg5
1cndoKm
| P7Fq/yyX3g+TmnmGl/rrZ5R31i/XQw==
|_-----END CERTIFICATE-----
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519)
- A
```

```
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 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
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 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
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
```

```
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
(ecdh_x25519) - 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
(ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
(ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519)
- A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519)
- A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - 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
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
```

```
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|_  least strength: C
| rdp-ntlm-info:
|   Target_Name: WIN-8VMBKF3G815
|   NetBIOS_Domain_Name: WIN-8VMBKF3G815
|   NetBIOS_Computer_Name: WIN-8VMBKF3G815
|   DNS_Domain_Name: WIN-8VMBKF3G815
|   DNS_Computer_Name: WIN-8VMBKF3G815
|   Product_Version: 10.0.14393
|_  System_Time: 2022-12-11T08:35:06+00:00
8080/tcp  open  http-proxy    syn-ack ttl 125
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
| http-vhosts:
|_128 names had status 200
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-fetch: Please enter the complete path of the
directory to save data in.
|_http-litespeed-sourcecode-download: Request with null
```

```
byte did not work. This web server might not be
vulnerable
|_http-date: Sun, 11 Dec 2022 08:35:03 GMT; -1s from
local time.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the
target web server open and hold
|       them open as long as possible.  It accomplishes
this by opening connections to
|       the target web server and sending a partial
request. By doing so, it starves
|       the http server's resources causing Denial Of
Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2007-6750
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=ironcorp.me
|   url                                 method
|_  http://ironcorp.me:8080/login.html  FORM
|_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-malware-host: Host appears to be clean
| http-enum:
|_  /login.html: Possible admin folder
| http-php-version: Logo query returned unknown hash
f5f97997227a3aa4fcc08f4788018883
|_Credits query returned unknown hash
f5f97997227a3aa4fcc08f4788018883
|_http-chrono: Request times for /; avg: 756.69ms; min:
654.25ms; max: 929.96ms
| http-headers:
|   Content-Length: 20040
|   Content-Type: text/html
|   Last-Modified: Sun, 23 Feb 2020 11:30:30 GMT
|   Accept-Ranges: bytes
|   ETag: "0f1ea73cead51:0"
|   Server: Microsoft-IIS/10.0
|   Date: Sun, 11 Dec 2022 08:35:08 GMT
|   Connection: close
|
|_  (Request type: HEAD)
|_http-title: Bad Request
| http-grep:
|   (1) http://ironcorp.me:8080/:
|     (1) email:
|       + mccoy@example.com
|   (1)
http://ironcorp.me:8080/assets/plugins/Chart.js/Chart.min
.js:
|     (1) email:
|_      + emn178@gmail.com
11025/tcp open  unknown       syn-ack ttl 125
```

```
49667/tcp open  unknown       syn-ack ttl 125
49670/tcp open  unknown       syn-ack ttl 125

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| qscan:
| PORT   FAMILY  MEAN (us)  STDDEV    LOSS (%)
| 53     0       245518.60  93507.24  0.0%
| 135    0       257728.50  78327.81  0.0%
| 3389   0       234205.80  65312.21  0.0%
| 8080   0       240624.00  77326.54  0.0%
| 11025  0       276576.11  80371.41  10.0%
| 49667  0       218970.78  43474.63  10.0%
|_49670  0       262611.00  79955.62  10.0%
|_ipidseq: Unknown
| dns-brute:
|   DNS Brute-force hostnames:
|     mx.ironcorp.me - 23.202.231.169
|     stats.ironcorp.me - 23.202.231.169
|     mx0.ironcorp.me - 23.202.231.169
|     svn.ironcorp.me - 23.221.222.250
|     syslog.ironcorp.me - 23.202.231.169
|     mx1.ironcorp.me - 23.202.231.169
|     test.ironcorp.me - 23.221.222.250
|     test1.ironcorp.me - 23.202.231.169
|     test2.ironcorp.me - 23.202.231.169
|     mysql.ironcorp.me - 23.221.222.250
|     testing.ironcorp.me - 23.221.222.250
|     news.ironcorp.me - 23.221.222.250
|     upload.ironcorp.me - 23.221.222.250
|     noc.ironcorp.me - 23.202.231.169
|     vm.ironcorp.me - 23.221.222.250
```

```
|     ns.ironcorp.me - 23.202.231.169
|     vnc.ironcorp.me - 23.221.222.250
|     ns0.ironcorp.me - 23.221.222.250
|     ns1.ironcorp.me - 23.202.231.169
|     ns2.ironcorp.me - 23.202.231.169
|     vpn.ironcorp.me - 23.202.231.169
|     web.ironcorp.me - 23.221.222.250
|     web2test.ironcorp.me - 23.221.222.250
|     ns3.ironcorp.me - 23.221.222.250
|     ops.ironcorp.me - 23.202.231.169
|     webftp.ironcorp.me - 23.202.231.169
|     whois.ironcorp.me - 23.202.231.169
|     oracle.ironcorp.me - 23.221.222.250
|     wiki.ironcorp.me - 23.202.231.169
|     owa.ironcorp.me - 23.221.222.250
|     www.ironcorp.me - 23.221.222.250
|     pbx.ironcorp.me - 23.202.231.169
|     www2.ironcorp.me - 23.202.231.169
|     s3.ironcorp.me - 23.202.231.169
|     xml.ironcorp.me - 23.221.222.250
|     secure.ironcorp.me - 23.221.222.250
|     server.ironcorp.me - 23.221.222.250
|     shop.ironcorp.me - 23.202.231.169
|     sip.ironcorp.me - 23.221.222.250
|     sql.ironcorp.me - 23.202.231.169
|     squid.ironcorp.me - 23.202.231.169
|     host.ironcorp.me - 23.221.222.250
|     ssh.ironcorp.me - 23.202.231.169
|     http.ironcorp.me - 23.202.231.169
|     admin.ironcorp.me - 23.202.231.169
|     ssl.ironcorp.me - 23.202.231.169
|     id.ironcorp.me - 23.221.222.250
```

```
|     administration.ironcorp.me - 23.202.231.169
|     stage.ironcorp.me - 23.202.231.169
|     images.ironcorp.me - 23.202.231.169
|     ads.ironcorp.me - 23.202.231.169
|     adserver.ironcorp.me - 23.202.231.169
|     alerts.ironcorp.me - 23.221.222.250
|     info.ironcorp.me - 23.221.222.250
|     alpha.ironcorp.me - 23.221.222.250
|     internal.ironcorp.me - 23.202.231.169
|     ap.ironcorp.me - 23.221.222.250
|     internet.ironcorp.me - 23.202.231.169
|     apache.ironcorp.me - 23.202.231.169
|     intra.ironcorp.me - 23.221.222.250
|     app.ironcorp.me - 23.202.231.169
|     intranet.ironcorp.me - 23.221.222.250
|     apps.ironcorp.me - 23.202.231.169
|     ipv6.ironcorp.me - 23.221.222.250
|     appserver.ironcorp.me - 23.221.222.250
|     lab.ironcorp.me - 23.202.231.169
|     aptest.ironcorp.me - 23.202.231.169
|     ldap.ironcorp.me - 23.221.222.250
|     auth.ironcorp.me - 23.202.231.169
|     linux.ironcorp.me - 23.221.222.250
|     backup.ironcorp.me - 23.221.222.250
|     local.ironcorp.me - 23.221.222.250
|     beta.ironcorp.me - 23.202.231.169
|     log.ironcorp.me - 23.202.231.169
|     blog.ironcorp.me - 23.202.231.169
|     chat.ironcorp.me - 23.221.222.250
|     citrix.ironcorp.me - 23.221.222.250
|     cms.ironcorp.me - 23.202.231.169
|     main.ironcorp.me - 23.221.222.250
```

```
|     manage.ironcorp.me - 23.202.231.169
|     mgmt.ironcorp.me - 23.221.222.250
|     corp.ironcorp.me - 23.221.222.250
|     mirror.ironcorp.me - 23.221.222.250
|     crs.ironcorp.me - 23.221.222.250
|     mobile.ironcorp.me - 23.221.222.250
|     cvs.ironcorp.me - 23.221.222.250
|     monitor.ironcorp.me - 23.202.231.169
|     mssql.ironcorp.me - 23.202.231.169
|     devel.ironcorp.me - 23.221.222.250
|     mta.ironcorp.me - 23.202.231.169
|     database.ironcorp.me - 23.202.231.169
|     development.ironcorp.me - 23.221.222.250
|     db.ironcorp.me - 23.202.231.169
|     devsql.ironcorp.me - 23.202.231.169
|     demo.ironcorp.me - 23.202.231.169
|     devtest.ironcorp.me - 23.202.231.169
|     dev.ironcorp.me - 23.202.231.169
|     dhcp.ironcorp.me - 23.221.222.250
|     direct.ironcorp.me - 23.202.231.169
|     dmz.ironcorp.me - 23.202.231.169
|     dns.ironcorp.me - 23.202.231.169
|     dns0.ironcorp.me - 23.221.222.250
|     dns1.ironcorp.me - 23.202.231.169
|     dns2.ironcorp.me - 23.221.222.250
|     download.ironcorp.me - 23.202.231.169
|     en.ironcorp.me - 23.221.222.250
|     erp.ironcorp.me - 23.221.222.250
|     eshop.ironcorp.me - 23.221.222.250
|     f5.ironcorp.me - 23.202.231.169
|     fileserver.ironcorp.me - 23.221.222.250
|     firewall.ironcorp.me - 23.202.231.169
```

```
|     forum.ironcorp.me - 23.221.222.250
|     git.ironcorp.me - 23.202.231.169
|     gw.ironcorp.me - 23.221.222.250
|     help.ironcorp.me - 23.202.231.169
|     helpdesk.ironcorp.me - 23.221.222.250
|_    home.ironcorp.me - 23.221.222.250
|_fcrdns: FAIL (No PTR record)
| port-states:
|   tcp:
|     open: 53,135,3389,8080,11025,49667,49670
|_    filtered: 1-52,54-134,136-3388,3390-8079,8081-
11024,11026-49666,49668-49669,49671-65535
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
| dns-blacklist:
|   SPAM
|     l2.apews.org - FAIL
|_    list.quorum.to - FAIL
|_path-mtu: PMTU == 1500

Post-scan script results:
| reverse-index:
|   53/tcp: 10.10.20.22
|   135/tcp: 10.10.20.22
|   3389/tcp: 10.10.20.22
|   8080/tcp: 10.10.20.22
|   11025/tcp: 10.10.20.22
|   49667/tcp: 10.10.20.22
|_  49670/tcp: 10.10.20.22
Read data files from: /usr/bin/../share/nmap
# Nmap done at Sun Dec 11 04:00:13 2022 -- 1 IP address
```

```
(1 host up) scanned in 1996.05 seconds
```

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

[redacted]

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan

[redacted]

Entire Nessus Scan

[redacted]