

Introduction to Information Security

Autumn Term 2019

Practical Laboratory Assignment 1

2019 - 12 - 01

Group 21

Justas Narusas, Efstathios Psyllakis

Laboratory Assignments for Windows

Exercise 1

When analyzing both executables we found out the following differences:

1) Injected _calc.exe is bigger than calc.exe

2) Date modified for

calc.exe

->9/17/2012 12:00 pm

injected_calc.exe

-> 9/17/2012, 3:10 pm

- *What implications does this have for security?*

We compared file hashes values in order to check the integrity of the file, which shows us that they are not the same. User is exposed to viruses, trojans, worms and other kinds of malicious attacks. According to Pfleeger et al. (2015): '*A virus is a program that can replicate itself and pass on malicious code to other nonmalicious programs by modifying them.*' (pg.196)

```
/// File Checksum Integrity Verifier version 2.05.
/// e1fe13a125bdcf9d2bc8651d93e9bdf8 c:\users\cs2lab\desktop\securityp
ion\injected_calc.exe
C:\Users\cs2lab\Desktop\SecurityPrograms\fciv>fciv C:\Users\cs2lab\
ityPrograms\injection\calc.exe
/// File Checksum Integrity Verifier version 2.05.
/// 829e4805b0e12b383ee09abdc9e2dc3c c:\users\cs2lab\desktop\securityp
ion\calc.exe
```

- *In what circumstances might an attacker (or malicious software) modify an executable as part of an attack, or utilize modified executables in an attack?*

An attacker could modify an executable, if he has malicious intent to cause unanticipated or undesired effects (Pfleeeger et al., 2015). As a result, the regular user would not be able to see a difference and therefore keep the malicious file on his computer or download it not knowing it contains malicious code.

- *What could an executable be modified to do?*
 - Spread a virus.
 - Used as a virus attachment. (Pfleeeger et al., 2015)
- *How might one be exposed to such threats, and how can one protect oneself from them?*

A user could be exposed to such threats with regard to transmission errors (Pfleeeger et al., 2015). A user can be protected by them through error detecting and error correcting codes which reveal transmission errors and can perform repairs on the affected code (Pfleeeger et al., 2015). More specifically, *Pfleeeger et al.* illustrate their use on his book “*Security in Computing*” (2015): “*Error detecting codes detect when an error has occurred, and error correcting codes can actually correct errors without requiring a copy of the original data.*” (pg.138.)

Exercise 2

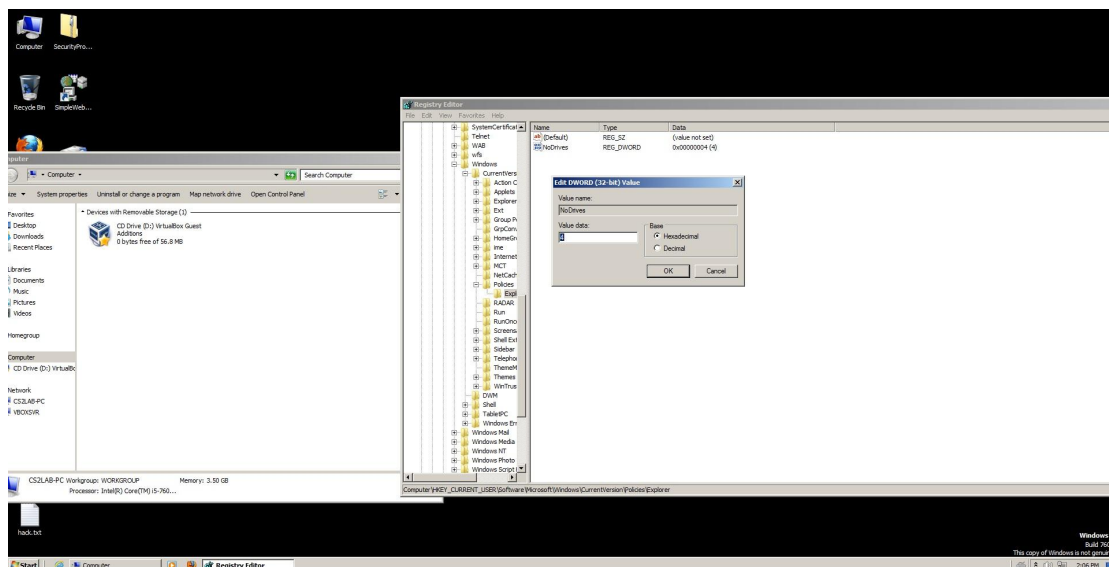
Exercise 2A

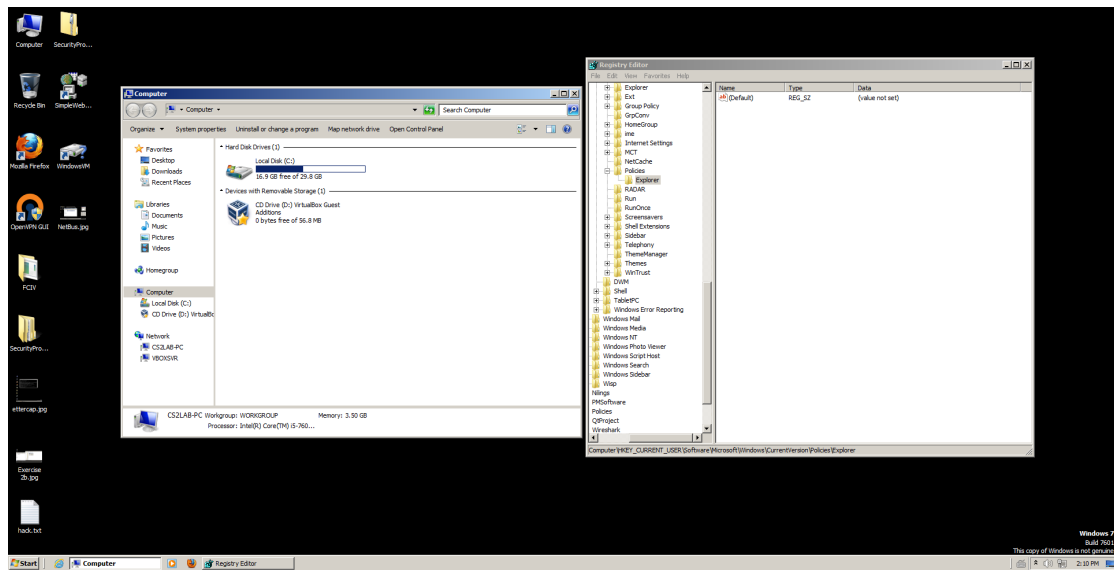
We have been through all the steps required, we modified and checked *DontDisplayLastUsername* in Registry editor, logged off to see if the last user was displayed and it was not. Then we deleted from the registry as stated in the assignment sheet and the previous user appeared as shown in the screenshots below.



Exercise 2B

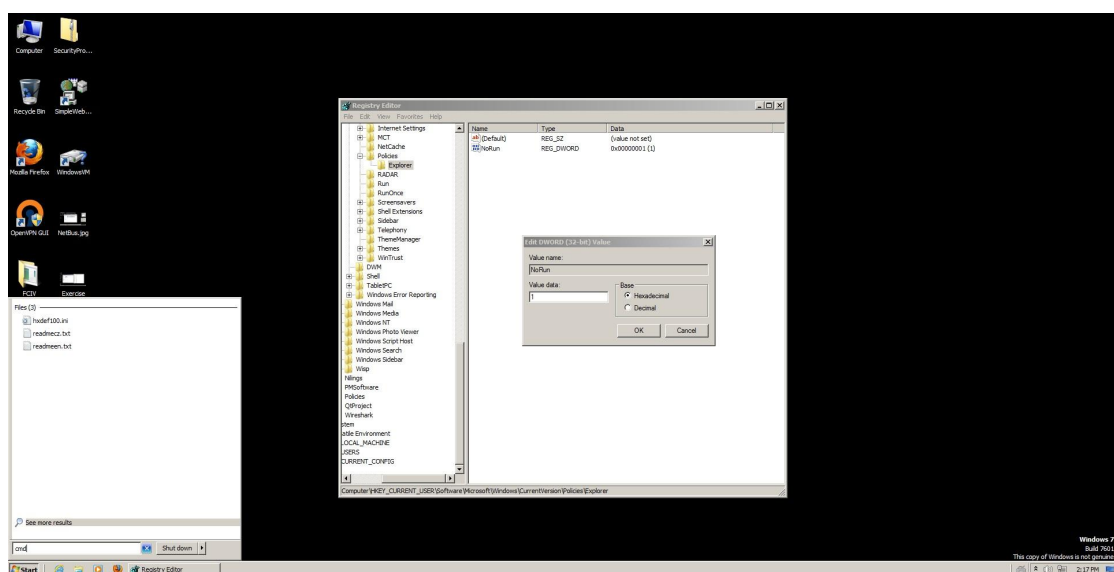
We have been through all the steps explained in Exercise 2B, we created a key named Explorer in the folder *Policies*. In the folder Explorer, we have added a value C=4. We logged off and on, and the drives were not actually there as it was expected. Afterwards, we deleted *NoDrives* from the registry and Drive:C appeared again.





Exercise 2C

We have been through all the steps required and registry could not execute any programs. After we removed the value *NoRun*, registry run as usual.



Exercise 3

- *What would you be able to perform in a situation where you had access to a command shell with administrator privileges?*

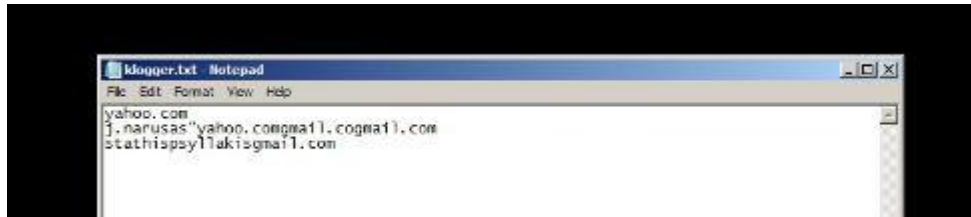
“Limited privilege is the act of restraining users and processes so that any harm they can do is not catastrophic. A system that prohibits all accesses to anything by anyone certainly achieves both confidentiality and integrity, but it completely fails availability and usefulness.” (Pfleeger et al., 2015, pg.103)

As a result, a user with administrative privileges can make changes to the system that could be harmful.

- *How can the OS trust its own applications and what measures can it take to protect against such modifications?*

A two-way authentication based on *fingerprint* and *administrator password use* would be a great way to secure a system from executing any commands that could harm a computer.

Exercise 4



As it is displayed above, it contains the keystrokes we typed and some of them got logged more than once as we have taken two steps:

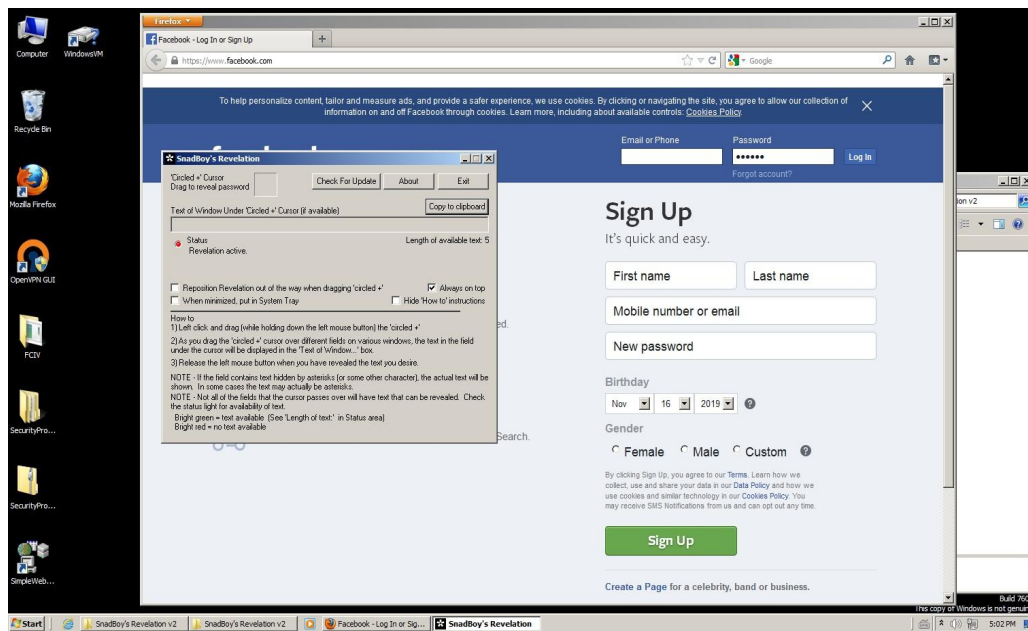
- 1) Visit URL yahoo.com and type in a username: j.narusas@yahoo.com
- 2) Visit URL gmail.com and type in a username: stathispsyllakis@gmail.com

This tool can be used in order to acquire useful information through keystrokes like usernames, passwords, links that have been visited, etc.

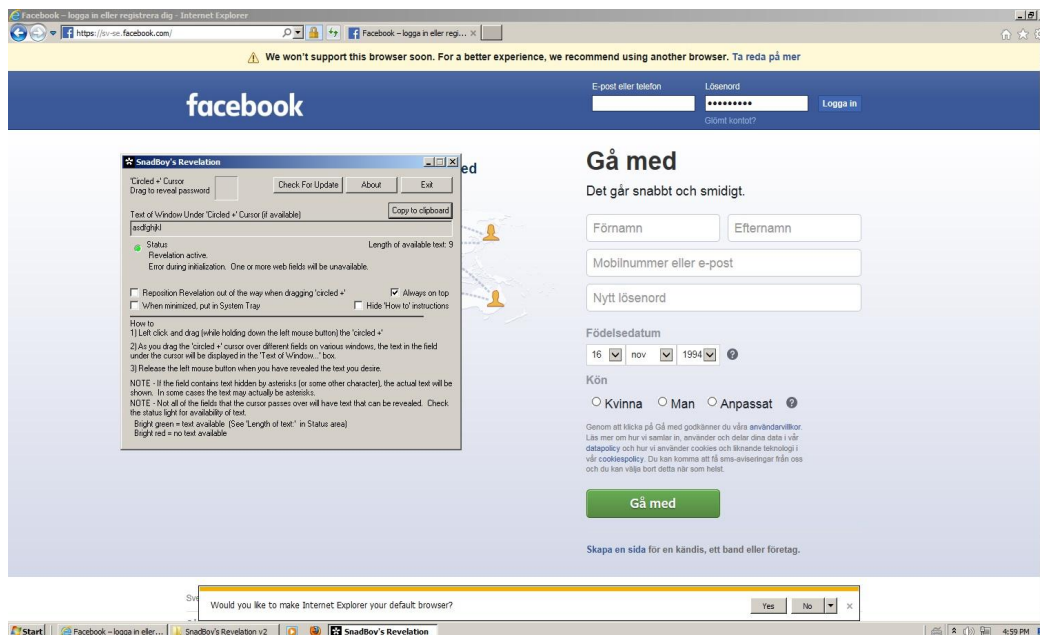
Exercise 5

With a simple tool SnadBoy's Revelation v2 we were able to see hidden passwords by dragging a cursor to reveal the password from the field we entered it in.

- As it is shown, on Mozilla Firefox the tool did not work.

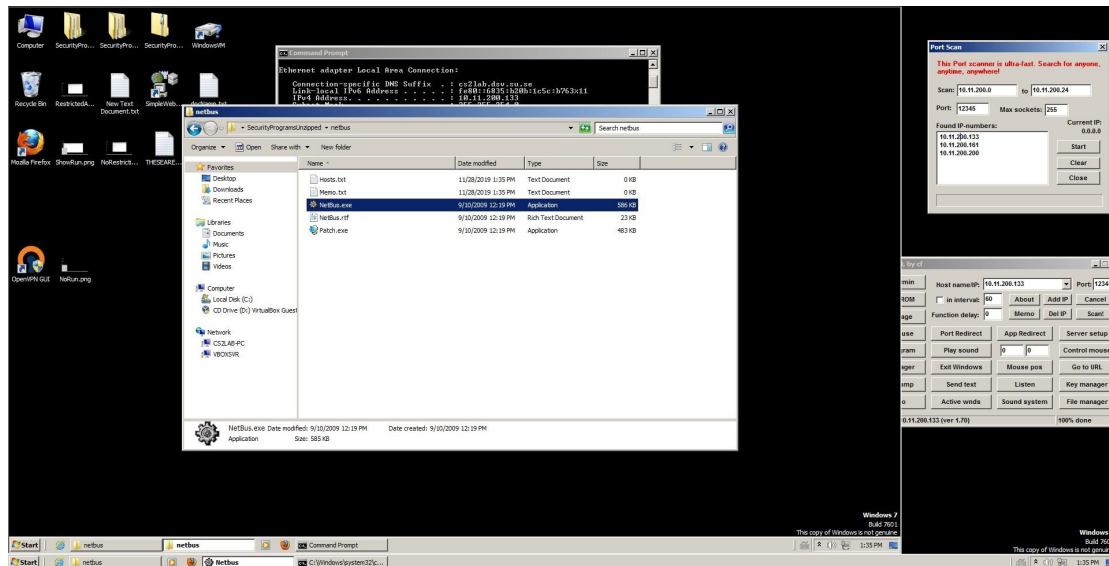


- It worked properly and the password was shown on Internet Explorer.



Exercise 6

We connected to our victim's computer successfully and performed a screen dump.



Laboratory Assignments for Kali Linux

Exercise 1 (Nmap)

- Which ports are open?

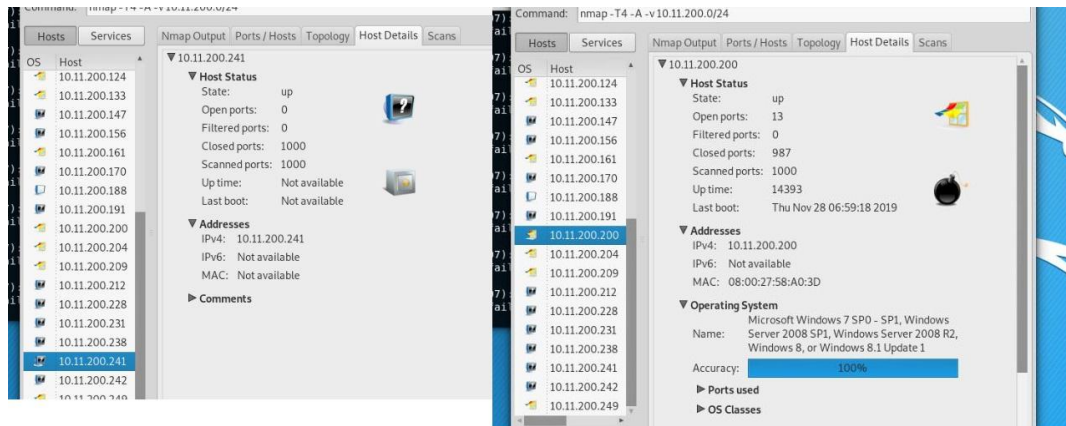
135, 139, 445, 49152-7, 5357

There were other ports open on some of the machines: 80, 100, 12345, 2869, 10243.

- Is there any difference in scanning Windows or Linux computers?

Zenmap does not display open ports on Kali OS.

Zenmap does not display the Operating system on Kali machines.



Exercise 1 (OpenVas)

On Windows only IP addresses were shown compared to Linux and Nmap where IP addresses were shown alongside (generally more detailed info about Users etc.)

Pfleeger et al. (2015) illustrate the use of tools such as Nmap and OpenVas in their book “Security in Computing” (2015):

“Port scanning tells an attacker three things: which standard ports or services are running and responding on the target system, what operating system is installed on the target system, and what applications and versions of applications are present. This information is readily available for the asking from a networked system; it can be obtained quietly, anonymously, without identification or authentication, drawing little or no attention to the scan.” (pg.396)

After scanning for vulnerabilities, we found the following information about different systems:

Windows:

Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host.

Kali:

No vulnerabilities found.

Metasploitable:

PostgreSQL vulnerabilities:

- denial-of-service issue
- privilege-escalation issue
- authentication-bypass issue
- 'bitsubstr' Buffer Overflow Vulnerability
- PL/Perl and PL/Tcl Local Privilege Escalation Vulnerability
- 'RESET ALL' Unauthorized Access Vulnerability
- Conversion Encoding Remote Denial of Service Vulnerability
- Hash Table Integer Overflow Vulnerability
- Low Cost Function Information Disclosure Vulnerability

vsftpd Compromised Source Packages Backdoor Vulnerability

OpenSSL CCS Man in the Middle Security Bypass Vulnerability

http TRACE CSS attack

/doc directory browsable

awiki Multiple Local File Include Vulnerability

phpMyAdmin

- Unspecified SQL Injection and Cross Site Scripting Vulnerabilities
- Multiple Cross Site Scripting Vulnerabilities
- Debug Backtrace Cross Site Scripting Vulnerability
- SQL bookmark XSS Vulnerability
- Setup Script Request Cross Site Scripting Vulnerability
- 'error.php' Cross Site Scripting Vulnerability
- pmd_pdf.php Cross Site Scripting Vulnerability

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability

Check: Mailserver answer VRFY and EXPN requestis, SSL Weak Ciphers, rexecd Service

TCP timestamps

Samba 'client/mount.cifs.c' Remote Denial of Service Vulnerability

Exercise 2

Webspy is part of dSniff tools, which intercepts URLs from a specific IP address and directs them to your browser and connects to the same URL on your machine (it did not exactly work for us, because every time it caught a URL from the machine we were sniffing on, the browser crashed trying to open the same URL and we could not figure out exactly why). ("DSniff," 2018)

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# webspy -i eth0 10.0.2.5
webspy: listening on eth0
openURL(http://104.102.50.14/fwlink/?LinkId=69157)
webspy: window 0x1e0001b was destroyed.
openURL(http://204.79.197.203/?ocid=iehp)
webspy: not running on display :1
root@kali:~# webspy -i eth0 10.0.2.5
webspy: listening on eth0
openURL(http://23.32.98.200/fwlink/?LinkId=69157)

```

Urlsnarf is part of the dSniff tools used for network monitoring. Below is the answer we got while monitoring our own network.

root@kali:~# urlsnarf

```

urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://go.microsoft.com/fwlink/?LinkId=69157 HTTP/1.1" - - "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://www.msn.com/?ocid=iehp HTTP/1.1" - - "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://www.msn.com/sv-se/?ocid=iehp HTTP/1.1" - - "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://static-global-s-msn-com.akamaized.net/hp-neu/sv-se/homepage/_sc/css/3bf20fde-b3eba4bd/direction=ltr,locales=sv-se,themes=start.dpi=resolution1x/d2-442eb3-26acb587/b6-8917b2-41546a27/31-c31fb0-68ddb2ab/49-481f80-677c872a/14-6fb3bf-2b29dea6/2a-c5209a-d0f2a40b/69-8f5e1d-d8da69e2/25-dd7b49-d55835e5/55-2e75c6-9336e448/18-56aa26-dbc6220a/b5-77bbe0-e1d32d27/7e-9493f9-5fe1842f/b8-cbc6ea-793099c5/67-f5a030-95aa7dda/1e-ed96c4-6163f058/d0-c37c5e-c329ca6a/b0-c5de1a-23a6edb1/c8-2a23e7-160c7f00/ae-0f4566-a484bc65/23-5d0d80-cb31fb5/8a-19583d-17636285?ver=20191116_19676952&fdhead=gholdout,muidflt10cf,muidflt49cf,muidflt50cf,adflt-gal4p5sec,muidflt58cf,muidflt300cf,startedge3cf,bingcollabedge1cf,platagyhp2cf,audexhp1cf,samrtbareb-nc,article2cf,article3cf,gallery2cf,onetrustpoplive,jsltlelemetry,ntpdisplaye&ocid=iehp&csopd=20191120223745&csopdb=20191125235020 HTTP/1.1" - - "http://www.msn.com/sv-se/?ocid=iehp" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://static-global-s-msn-com.akamaized.net/hp-neu/sv-se/homepage/_sc/js/3bf20fde-9ae9d78b/direction=ltr,locales=sv-se,themes=start.dpi=resolution1x/97-9a8c47-68ddb2ab/50-16a2f2-3671893c/6b-96b2ae-ab822b88/e4-0588d3-68ddb2ab/d9-222405-11d52793/9e-a7a255-68ddb2ab/a9-ac9b58-68ddb2ab/f1-d0c6aa-cae48929/c7-47822a-426a0a13/30-ea66ac-bc3833fd/5d-eb3fde-68ddb2ab/fe-718b87-

```

```

243aa040/a9-d6e5f0-a1e90492/9c-639daf-68ddb2ab/85-0f8009-68ddb2ab?ver=20191116_19676952&fdhead=gholdout,muidflt10cf,muidflt49cf,muidflt50cf,adflt-
gal4p5sec,muidflt58cf,muidflt300cf,startedge3cf,bingcollabedge1cf,platagyp2cf,audexhp1cf,samrtbareb-
nc,article2cf,article3cf,gallery2cf,onestrustpoplive,jsltlemetry,ntpdisplaye&ocid=iehp&csopd=20191120223745&csopdb=20191125235020 HTTP/1.1" --
"http://www.msn.com/sv-se/?ocid=iehp" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXlnr0.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=2128&y=840 HTTP/1.1" -- "http://www.msn.com/sv-
se/?ocid=iehp" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:49 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXlpB3.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp"
"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/hp-neu/sv-se/homepage/_sc/js/3bf20fde-
2923b6c2/direction=ltr.locales=sv-se.themes=start.dpi=resolution1x/41-0bee62-
68ddb2ab?ver=20191116_19676952&fdhead=gholdout,muidflt10cf,muidflt49cf,muidflt50cf,adflt-
gal4p5sec,muidflt58cf,muidflt300cf,startedge3cf,bingcollabedge1cf,platagyp2cf,audexhp1cf,samrtbareb-
nc,article2cf,article3cf,gallery2cf,onestrustpoplive,jsltlemetry,ntpdisplaye&ocid=iehp&csopd=20191120223745&csopdb=20191125235020 HTTP/1.1" --
"http://www.msn.com/sv-se/?ocid=iehp" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBWKkp0.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=333&y=317 HTTP/1.1" -- "http://www.msn.com/sv-
se/?ocid=iehp" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXl5k8.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg&x=471&y=484 HTTP/1.1" -- "http://www.msn.com/sv-
se/?ocid=iehp" "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXltga.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp" "Mozilla/5.0
(Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBWDaSh.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp" "Mozilla/5.0
(Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXl5BF.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&x=513&y=138 HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp"
"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXizGG.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp" "Mozilla/5.0
(Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/AAJZFqg.img?h=194&w=300&m=6&q=60&u=t&o=t&l=f&x=1805&y=775 HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp"
"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"
10.0.2.5 - - [26/Nov/2019:13:37:50 +0100] "GET http://static-global-s-msn-com.akamaized.net/img-
resizer/tenant/amp/entityid/BBXihWe.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&x=214&y=201 HTTP/1.1" -- "http://www.msn.com/sv-se/?ocid=iehp"
"Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko"

```

dSniff is a sniffing network tool which can capture usernames and passwords, web pages visited, contents of email etc. In addition, dSniff “*can also be used to disrupt the normal behavior of switched networks and cause network traffic from other hosts on the same network segment to be visible, not just traffic involving the host dsniff is running on.*” (“DSniff,” 2018)

```

root@kali:~# dsniff
dsniff: listening on eth0
-----
11/26/19 10:18:23 tcp kali.47028 -> 10.11.9.39.21 (ftp)
USER msfadmin
PASS msfadmin

root@kali:~# dsniff -m
dsniff: listening on eth0
-----
11/24/19 16:04:56 tcp kali.54268 -> 10.11.9.39.23 (telnet)
msfadmin
msfadmin
ls
cd vulnetrrable
ls
cd samba

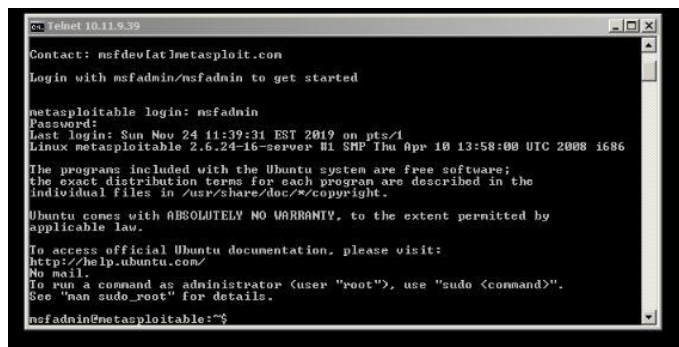
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun Nov 24 10:01:36 EST 2019 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

```

Ettercap

First of all, we have used the IP-based mode of operation as long as packets were filtered on IP source and destination. We have used the password collector feature for Telnet successfully and TCP OS fingerprinting feature in order to determine the OS of the victim host and its network adapter (“Ettercap (software),” 2019).



```

telnet 10.11.9.39

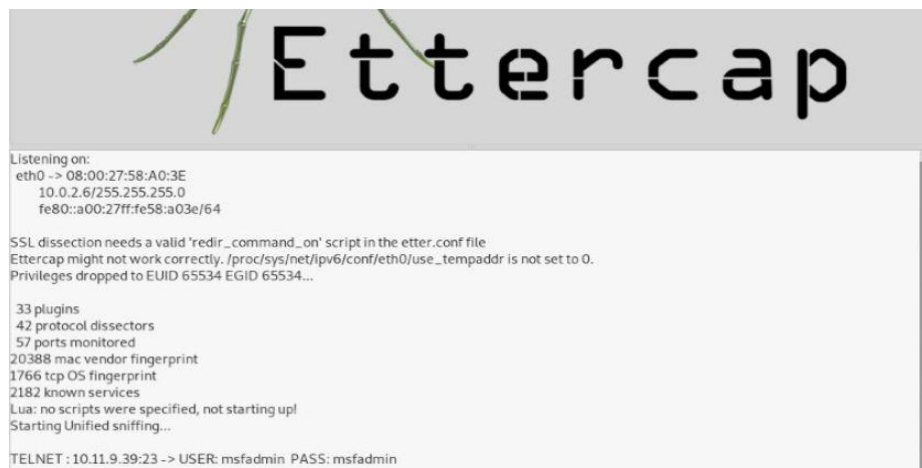
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun Nov 24 11:39:31 EST 2019 on pts/1
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.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
msfadmin@metasploitable:~$
  
```



```

Ettercap

Listening on:
eth0 -> 08:00:27:58:A0:3E
10.0.2.6/255.255.255.0
fe80::a00:27ff:fe58:a03e/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

TELNET: 10.11.9.39:23 -> USER: msfadmin PASS: msfadmin
  
```

Exercise 3

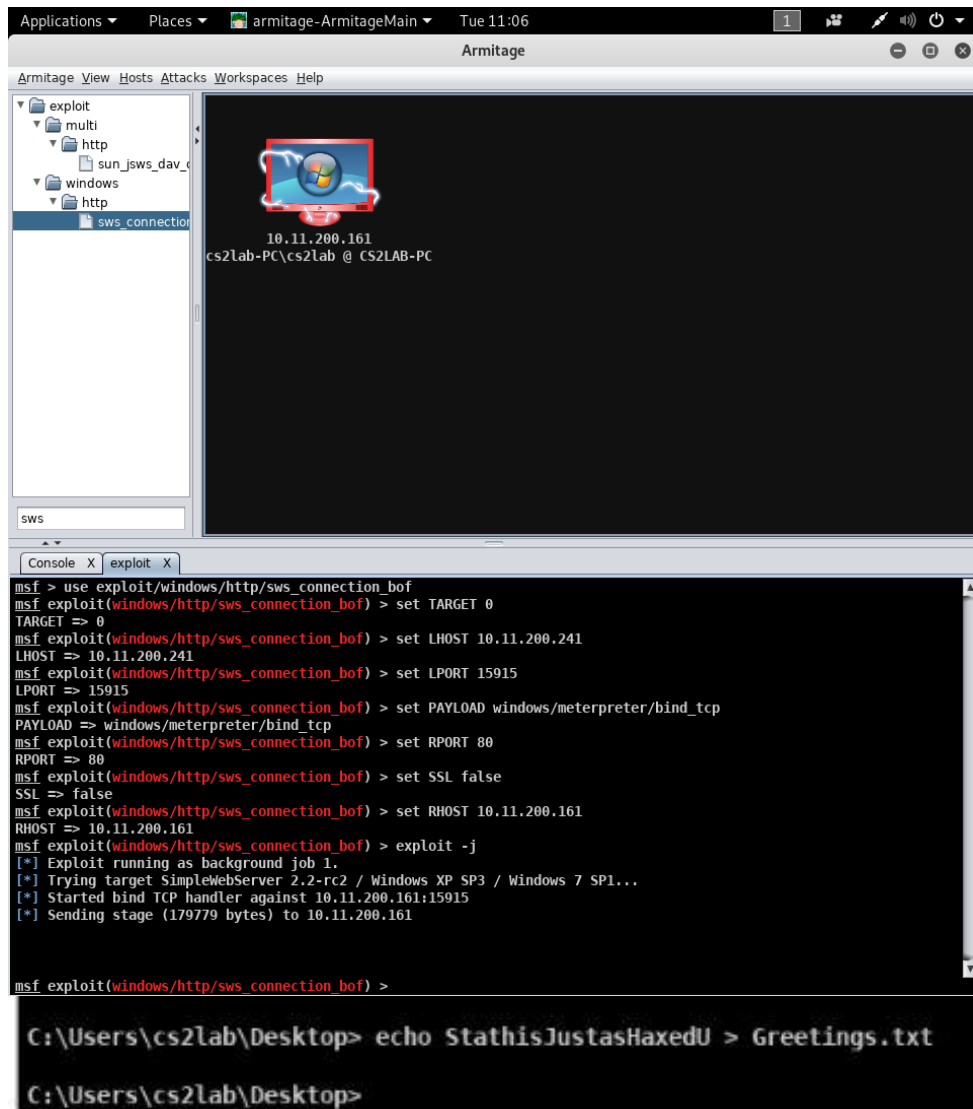
- Compare the info from tcpdump to the info from Snort. Similarities? Differences?

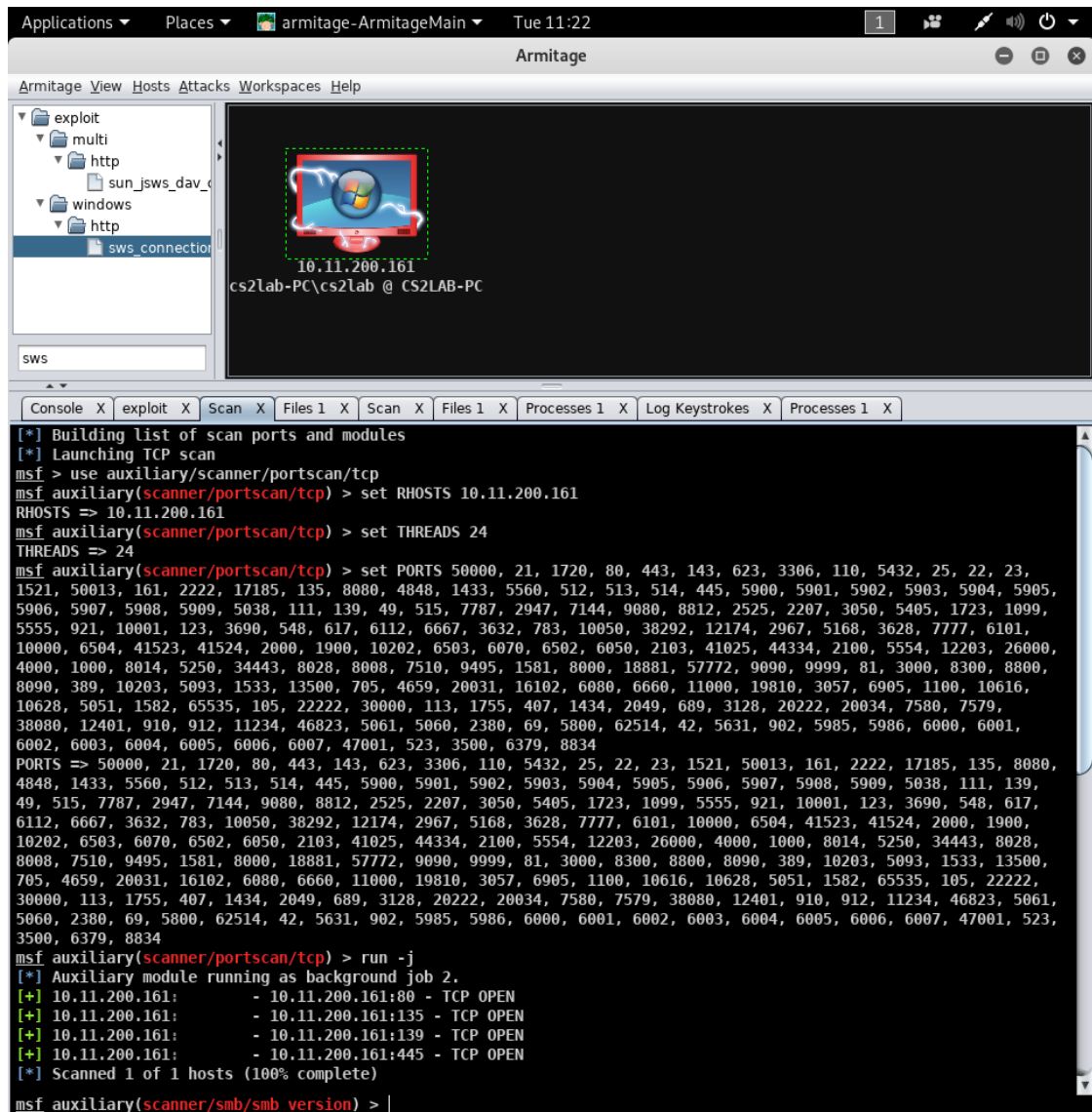
During TCPdump use, we were able to check TCP/IP data transfer and gather information about what it was sent on transmission channel. Snort also gave information about packet transfers inside transmission channel, but we were able to track transfers even outside the transmission channel.

Exercise 4

We exploited our colleagues' Windows 7 system, while following the directions in the assignment instructions. While doing a vulnerability check on exercise 2 we noticed that Simple Web Server (SWS) and PORT 135 are some of the main vulnerabilities of this Windows system. We also noticed in the pictures below that PORT 88, 139, 445 are also open. As a result, we were able to expose the system using Armitage. SWS is known to have a vulnerability: "A remote user can send a long string of data in the connection header to cause an overflow on the stack when function vsprintf is used and gain arbitrary code execution." (mr.pr0n & Juan Vasquez, 2018)

Windows Firewall could possibly help the system to not be exploited, but it was not set up. We also added a text file 'Greetings.txt' to the exploited systems Desktop and we were able to see all the files on their system.





References

DSniff. (2018). In *Wikipedia*. Retrieved from

<https://en.wikipedia.org/w/index.php?title=DSniff&oldid=875121074>

Ettercap (software). (2019). In *Wikipedia*. Retrieved from

[https://en.wikipedia.org/w/index.php?title=Ettercap_\(software\)&oldid=904380553](https://en.wikipedia.org/w/index.php?title=Ettercap_(software)&oldid=904380553)

mr.pr0n, & Juan Vasquez. (2018). Simple Web Server Connection Header Buffer

Overflow. Retrieved December 1, 2019, from Rapid7 website:

https://www.rapid7.com/db/modules/exploit/windows/http/sws_connection_bof

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (Fifth edition). Upper Saddle River, NJ: Prentice Hall.