Module Title: Network forensics

Type: Practical and Reports

Title: CA2 – Security Testing and Report

Student: Thiago CavalcantePetcov

Student ID: 2016206

Lecturer: Greg South

College of Computing Training

(CCT)

2020

Introduction

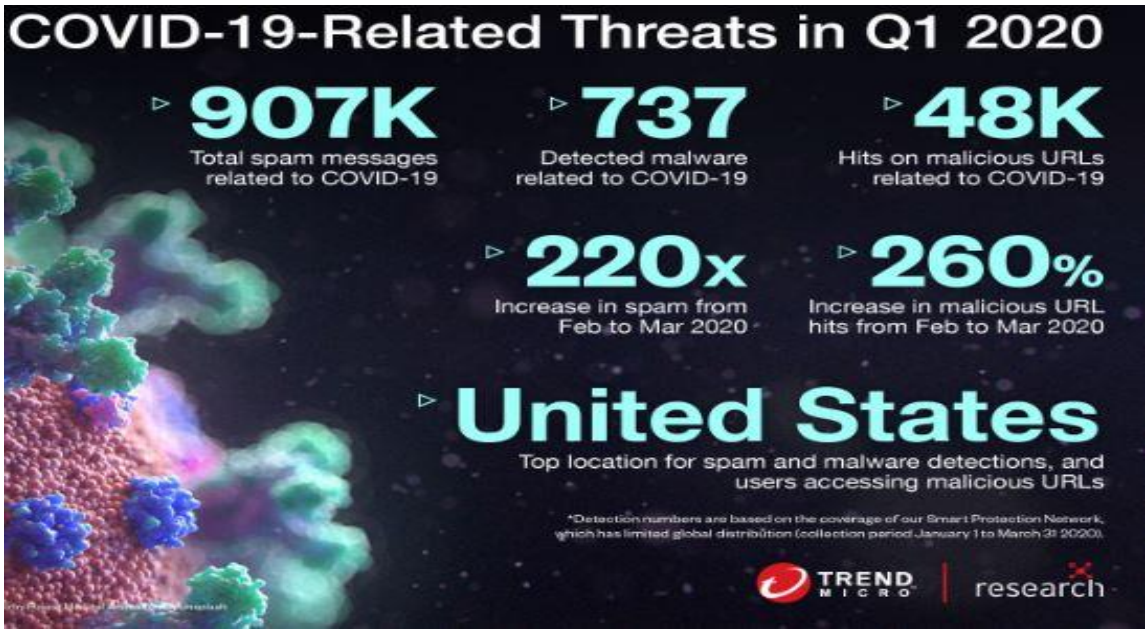
The purpose of this assignment was to build and set three virtual machines using Kali Linux to communicate with another virtual machine and to attack it. This virtual machine was using Metasploitable2 and Windows 10 Enterprise.

OWASP stands for Open Web Application Security Project and it is useful for checking a networks vulnerabilities.

The target of this assignment was to learn in a realistic way how to identify threats in the internet over the network set.

Source: https://community.sitecore.net/developers/f/5/t/3335

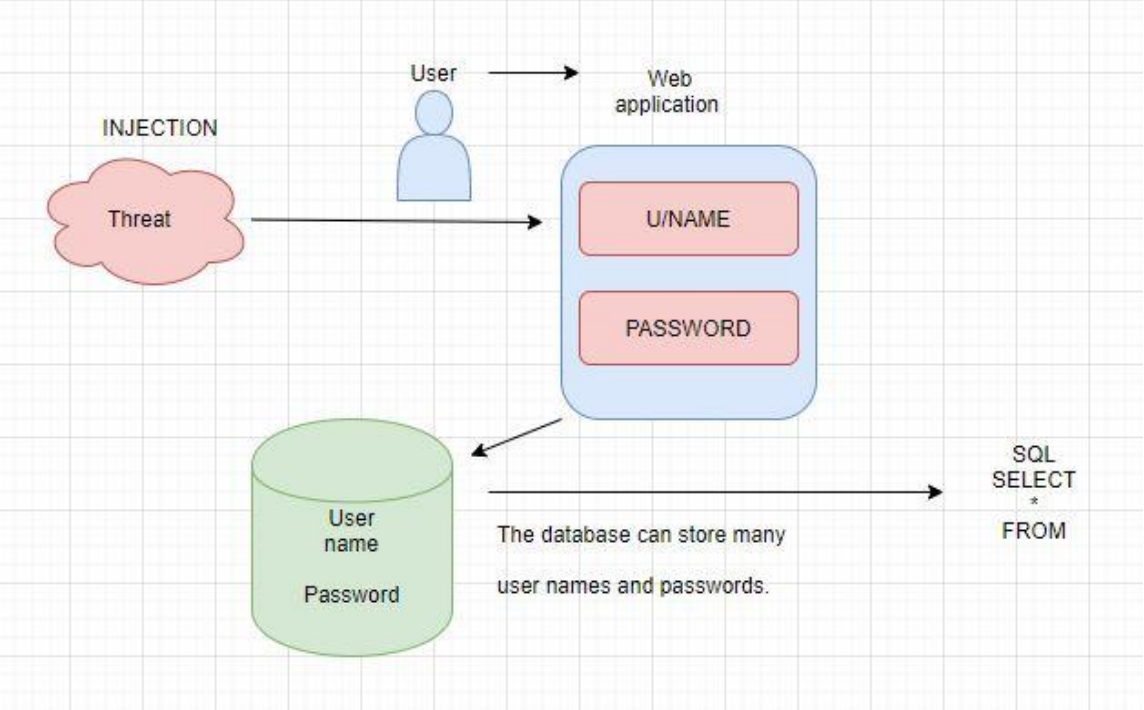
Published on March 06, 2020



Source: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Unfortunately COVID - 19 hascreated a lot of new ways for hackers to attack users as the virus has become a trend over the internet.

Below is a simple example of how the inputs of a user can get hacked.



Discussion

I chose Injection attack because I was more familiar with it and I did research that showed how injection attacksare stilla very common form of attack. Banks are very vulnerable to hack attacks as is any website that deals and manage big amounts of money. According to New York Times on July 30 2019,banks were the major focus of hacking attacks (Cowley and Perlroth, 2019).MasterCardis an example of a company that combats 460,000 intrusion attempts a day in a typical day. Usually hackers takeadvantage of weak passwords. Another method is fishing with fake emails. The user opens the email thinking it is from someone in the company which helps to get the hackers into the network and enables them to access bank accounts and etc. Cybersecurity is the way companies and people prevent or protect themselves from attacks and/or threats.

A1 Injection Threat/Attack Vectors

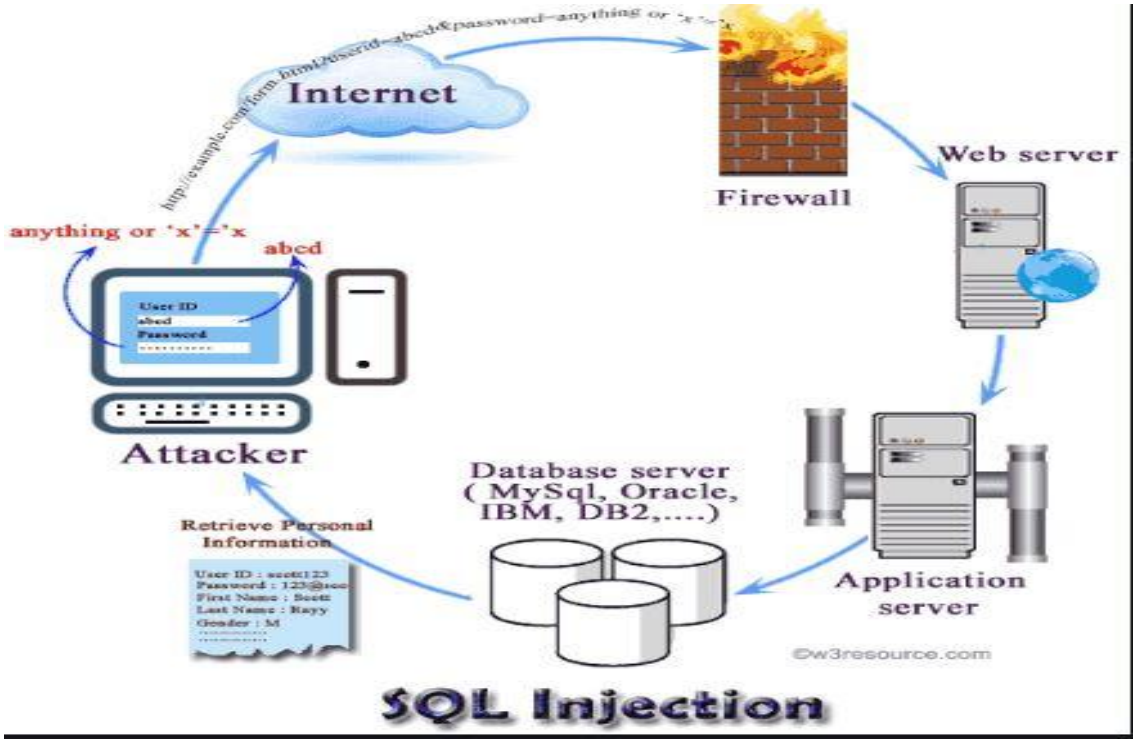
An injection can be any type of data infiltration into a network from a black hat from outside or inside.

Security Weakness

In a technical way, injection can access a user's system through code and is easily found in these languages: SQL, LDPA, XPath, or no SQL queries, OS commands, XML parses, SMTP Headers, and etc. When well analysed, the threat can be easily found.

Impacts

Businesses and customers can suffer differing impacts either financially or by an unauthorized person gaining access to confidential documents and private data. Nowadays, businesses are investing massive amountsof money to keep their data servers and network safe from any cyberattack.



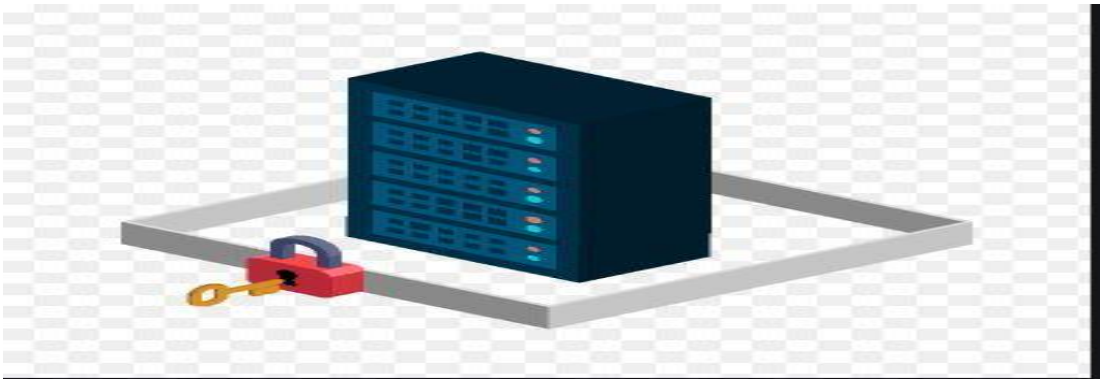
Source: https://www.w3resource.com/sql/sql-injection/sql-injection.php

Mitigation techniques

1. Make sure your work force is well educated in matters of security. Theworld of IT is always changing and employers and employees must constantly update their software as well as their skills to use the software correctly.
2. Keep management application layers simple and automat all updates.
3. Staff members can cause harm. There have been cases where a staff member can pay money to a cybercriminal and they can use the staff member's credentials to access private data.
4. Keep an eye on simple changes to a website that a hacker can make. For example if someone is looking for Ferrari.it but then,without noticing, a person may access Ferrari.It. With the only change being to the capital I, it is very hard notice this.

Server hardening

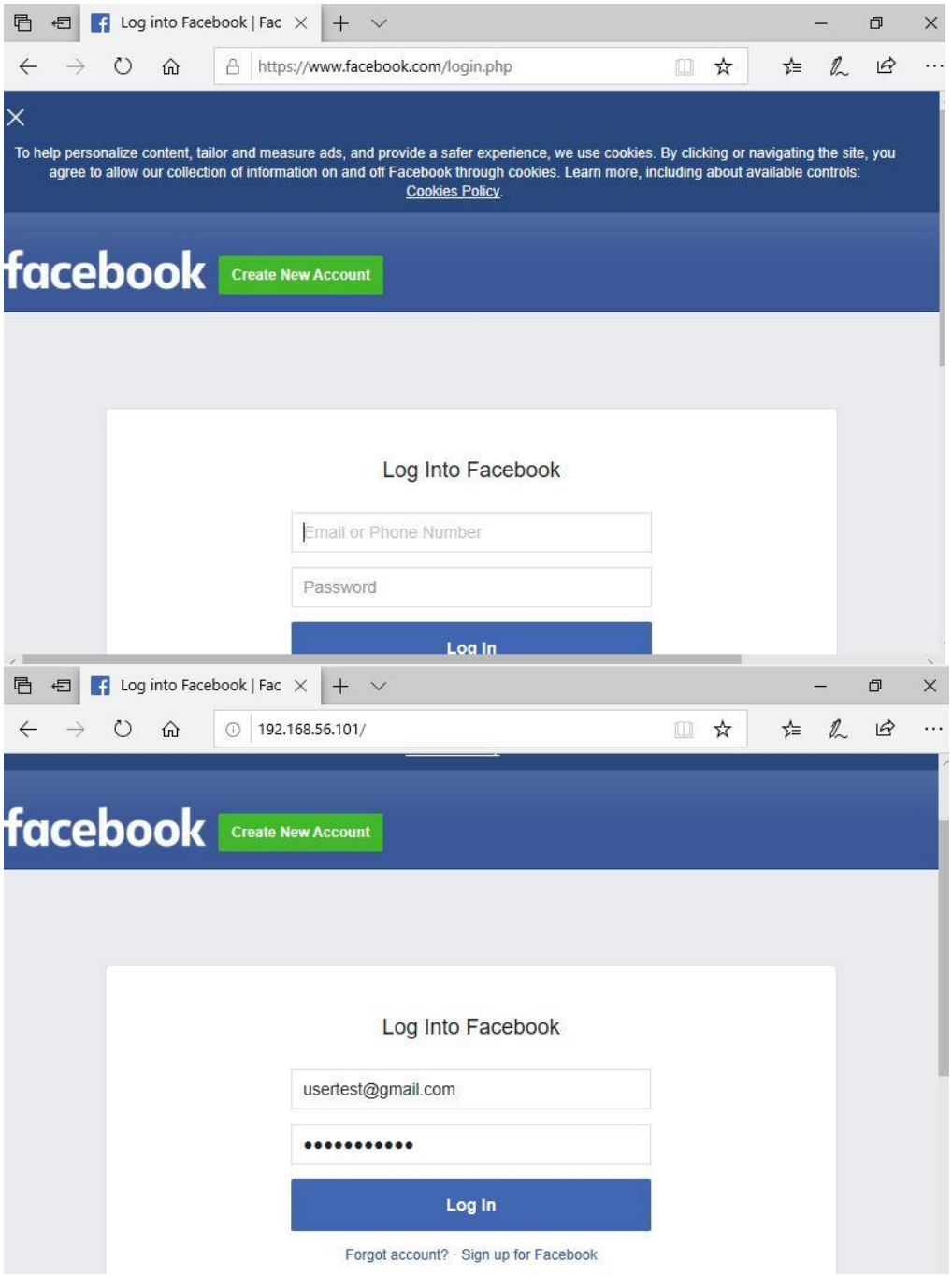
1. Physical security server protection
2. Update the software
3. Credit Banks can be vulnerable when the user is inputting their password
4. The storage where they store personal information can be a source of an attack



Server security is important for any business. Theserver must be backed up regularly. Any server that stores information that is important to thebusiness, such as customer information,should be backed up often.

Access list limits access to certain layers on the network. Staff cannot have full access over the network. One example wouldbe HR not being able to access financial data and vice versa.

Question 2.A


Log into Facebook | Fac
https://www.facebook.com/login.php
To help personalize content, tailor and measure ads, and provide a safer experience, we use cookies. By clicking or navigating the site, you agree to allow our collection of information on and off Facebook through cookies. Learn more, including about available controls: Cookies Policy.
facebook
Create New Account
Log Into Facebook
Email or Phone Number
Password
Log In
Log into Facebook | Fac
192.168.56.101/
facebook
Create New Account
Log Into Facebook
usertest@gmail.com
Log In
Forgot account? · Sign up for Facebook

```
File  Actions  Edit  View  Help

"compression":""}]
----------------------------7e4c01b101a2--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ----------------------------7e413d1b101a2
Content-Disposition: form-data; name="ts"

1588277307329
----------------------------7e413d1b101a2
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"gQWQW1siY2F0ZWdvcml6ZWRfb2RzIix7IjI5NzkiOnsiYmFuemFpIgEK8D5s
dWVfdG90YWxfbWVzc2FnZXNfcmVjZWl2ZWQiOls2NV19fX0sMTU4ODI3NzMwNzMyMi4zMDYxLDAsNTddLFvmZgAMc2VudF5
iAAg3MDYBYWAzXSxbInRpbWVfc3BlbnRfYml0X2FycmF5AcxcdG9zX2lkIjoic2Vzams0Iiwic3RhcnRfATAEIjoVsgQyLA
UqCTcUOls1LDBdCRIUbGVuIjo2CQwIc2VxFQyAY3VtIjo2NCwic2lkX3JhdyI6ImV1d3UzbDplZ3M5aHg6DXA2FgEIMy41B
bQIMTMxAbVEc2NyaXB0X3BhdGhfY2hhbmdlAbMUc291cmNlBRYwIjoiL2xvZ2luLnBocAG8CRsIdG9rAZc4ImFkOTc2NDIw
IiwiZGVzCUkUIjpudWxsDRENKQkSNGNhdXNlIjoidW5sb2FkAU52uwAALBGKGGVmX3BhZ2URWg2FdHVyaSI6Imh0dHBzOi8
vd3d3LmZhY2Vib29rLmNvbR23NgMBNDUuNjA2MiwwLDIxMV1d","user":"0","webSessionId":"euwu3l:egs9hx:ses
jk4","send_method":"beacon","compression":"snappy_base64","snappy_ms":1},{"webSessionId":"euwu3
l:egs9hx:sesjk4","posts":[["categorized_ods",{"2979":{"banzai":{"blue_messages_received":[4]}}}
,1588277307326.506,0,50]],"user":"0","app_id":"256281040558","compression":""},{"webSessionId":
"euwu3l:egs9hx:sesjk4","posts":[["categorized_ods",{"2979":{"banzai":{"blue_messages_sent":[6]}
}},1588277307326.6062,0,46]],"user":"0","app_id":"256281040558","compression":""}]
----------------------------7e413d1b101a2--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.56.103 - - [30/Apr/2020 16:07:38] "GET /favicon.ico HTTP/1.1" 404 -
```

```
File  Actions  Edit  View  Help

"compression":""}]
----------------------------7e4c01b101a2--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ----------------------------7e413d1b101a2
Content-Disposition: form-data; name="ts"

1588277307329
----------------------------7e413d1b101a2
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"gQWQW1siY2F0ZWdvcml6ZWRfb2RzIix7IjI5NzkiOnsiYmFuemFpIgEK8D5s
dWVfdG90YWxfbWVzc2FnZXNfcmVjZWl2ZWQiOls2NV19fX0sMTU4ODI3NzMwNzMyMi4zMDYxLDAsNTddLFvmZgAMc2VudF5
iAAg3MDYBYWAzXSxbInRpbWVfc3BlbnRfYml0X2FycmF5AcxcdG9zX2lkIjoic2Vzams0Iiwic3RhcnRfATAEIjoVsgQyLA
UqCTcUOls1LDBdCRIUbGVuIjo2CQwIc2VxFQyAY3VtIjo2NCwic2lkX3JhdyI6ImV1d3UzbDplZ3M5aHg6DXA2FgEIMy41B
bQIMTMxAbVEc2NyaXB0X3BhdGhfY2hhbmdlAbMUc291cmNlBRYwIjoiL2xvZ2luLnBocAG8CRsIdG9rAZc4ImFkOTc2NDIw
IiwiZGVzCUkUIjpudWxsDRENKQkSNGNhdXNlIjoidW5sb2FkAU52uwAALBGKGGVmX3BhZ2URWg2FdHVyaSI6Imh0dHBzOi8
vd3d3LmZhY2Vib29rLmNvbR23NgMBNDUuNjA2MiwwLDIxMV1d","user":"0","webSessionId":"euwu3l:egs9hx:ses
jk4","send_method":"beacon","compression":"snappy_base64","snappy_ms":1},{"webSessionId":"euwu3
l:egs9hx:sesjk4","posts":[["categorized_ods",{"2979":{"banzai":{"blue_messages_received":[4]}}}
,1588277307326.506,0,50]],"user":"0","app_id":"256281040558","compression":""},{"webSessionId":
"euwu3l:egs9hx:sesjk4","posts":[["categorized_ods",{"2979":{"banzai":{"blue_messages_sent":[6]}
}},1588277307326.6062,0,46]],"user":"0","app_id":"256281040558","compression":""}]
----------------------------7e413d1b101a2--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.56.103 - - [30/Apr/2020 16:07:38] "GET /favicon.ico HTTP/1.1" 404 -
^C[*] File in XML format exported to /root/.set/reports/2020-04-30 16:09:53.887817.xml for your reading pleasure...

     Press <return> to continue
```

```
File   Actions   Edit   View   Help

      <param>legacy_return=0</param>
      <param>profile_selector_ids=</param>
      <param>return_session=</param>
      <param>skip_api_login=</param>
      <param>signed_next=</param>
      <param>trynum=1</param>
      <param>timezone=-75</param>
      <param>lgndim=eyJ3Ijo4MDAsImgiOjYwMCwiYXciOjgwMCwiYWgiOjU2MCwiYyI6MjR9</param>
      <param>lgnrnd=125000_0veY</param>
      <param>lgnjs=1588276980</param>
      <param>email=usertest@gmail.com</param>
      <param>pass=pwd12345678</param>
      <param>prefill_contact_point=</param>
      <param>prefill_source=</param>
      <param>prefill_type=</param>
      <param>first_prefill_source=</param>
      <param>first_prefill_type=</param>
      <param>had_cp_prefilled=false</param>
      <param>had_password_prefilled=false</param>
      <param>ab_test_data=AAAPPfAPPPf/PPPPAAAAPAPPAAAPAAAAAPAAAPAAi/ttLFFFAAMEAF</param>
   </url>
   <url>      <param>----------------------------7e4c01b101a2</param>
   </url>
   <url>      <param>----------------------------7e413d1b101a2</param>
   </url>
</harvester>
root@kali:~/.set/reports#
```

Social engineering

One of the top websites vulnerable to simple and straight forward attacks Facebook. Facebook is so popular you can easily set a scenario for the eventual target to steal their password and login. (Crawley, 2017)One can go to any free networking event provided by big tech companies in Ireland. They often host free network events. A hacker can get to know really important people during these events indirectly. For example, one such person could be financial manager.

As we are living in a world that is constantly busy and everything moves so fast, sometimes we do not pay attention to the smallest details on a daily basis. One can get an email on their phone from a black hat without realising.

Black hat: Hey Jon how are you doing? It was really great to meet you at the event, can we be friends on Facebook?

Under this message there will be an email “phishing” an insecure Facebook link where the target will accept the friend request without ever knowing he was being hacked.He will almost definitely have his account linked to many emails and websites. That gives the black hat the chance to collect the huge amounts of data from one person.

Protect yourself against attack

1. The first step is always to check the status of your URL. For myself I often make sure when I am banking online to pay attention to thebrowser.https//: is always a secure network.
2. Keep your operating system and firewall updated.

1. B.1

```
root@kali:~# nmap -sV -O 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 09:56 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00045s latency).
Not shown: 977 closed ports
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: 08:00:27:5F:E6:F1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Conclusion

1. **What parts of the project did you participate in?**

   For this particular assignment unfortunately I had to work on my own. I had to manage all questions and research to find solutions myself. With help from the videos provided by the lecturer on line I was able to work good solutions.

2. **What did you learn from working within a team? What would you do differently if you had to build it again?**

   Unfortunately I could not find a group to work on it. But I keep myself in touch with my classmates to trouble shoot some similar problems on our virtual machines.

3. **What did you find most difficult to implement or understand?**

   "Main in the middle" and "Honey pot"

4. What technology / area did you research? What did you find out from this research?

I had to research how to do simple penetration using Kali Linux, Concepts of cybersecurity, Social engineering and OWASP best practice. I find out that there are many vulnerabilities in any system even from the code perspective up to the whole network environment both physical and not physical.

5. What do you wish you could have implemented if you had more time? Any other thoughts on the module?

I would love to spend more time studying more about Linux and how the operating systems work from a deeper perspective. Definitely I would spend also more time on Kali Linux learning the threats and how to use them in a deep away to increase my knowledge of cybersecurity. I might like to work in this area in the future.

Resources

Cowley, S. and Perlroth, N., (2019) "*Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc" NY Times. Available online. Accessed 30/04/2020*
https://www.nytimes.com/2019/07/30/business/bank-hacks-capital-one.html

(2017) "A1: 2017 Injection" Available online. Accessed 26/04/2020

https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A1-Injection

(2016) "Is Sitecore 8.x OWASP compliant?" Available online. Accessed 28/04/2020

https://community.sitecore.net/developers/f/5/t/3335

Crawley, K. (2017) " Social Engineering on Facebook" Available online. Accessed 26/04/2020

https://threatvector.cylance.com/en_us/home/social-engineering-on-facebook.html

(2020) "Developing Story: COVID-19 Used in Malicious Campaigns" Available online. Accessed 01/05/2020

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

(2020) "SQL Injection Tutorial" Available online. Accessed 01/05/2020

https://www.w3resource.com/sql/sql-injection/sql-injection.php