



INFORMATICS
INSTITUTE OF
TECHNOLOGY

UNIVERSITY OF
WESTMINSTER 

INFORMATICS INSTITUTE OF TECHNOLOGY

in collaboration with

the University of Westminster, UK

BEng (Hons) in Software Engineering

Security and Forensics Coursework Report

By

Nawanage Don Hasith Sasanka Nawana

16266670 / 2016110

Module Leader: Mr. Saman Hettiarachchi

Date of Submission: 29th April 2020

Contents

List of Tables	2
List of Figures	2
Assigned Scenario	2
A - Information gathering – Social engineering and nmap	3
1) Threats to open ports.....	3
2) Two services running on the server machine that should be priority to protect	5
3) Research three internet vulnerabilities related to those services	6
4) Pick the four least secure services running on the server machine and explain the danger posed by each of them	7
B - Finding and exploiting vulnerabilities	8
(1) Identify if the application is vulnerable to data tampering and exploit it if possible	8
(2) Identify if the application is vulnerable to SQL injection and exploit it if possible	9
(3) Identify if the application is vulnerable to XSS vulnerability and exploit it if possible	10
(4) Can you identify any other vulnerability?	10
C – Man in the Middle attacks and Social Engineering	11
1) If a client is connected to the server while you are testing the environment, identify what are the information that can be obtained from a packet capture of their communication.....	11
2) Identify a method that lure a normal user of the server to your computer instead of the server machine	14
3) If the server is protected, what can you do to penetrate the system from the client side.....	15
D – Protecting the Server	16
1) Port Knocking	16
2) False Positives and False Negatives in relation to a Network Intrusion Detection System.....	16
3) Difference between Intrusion Detection System IDS and Intrusion Prevention System IPS	17
4) Firewall, Snort and Iptables	18
5) Other security recommendations	19
References	20

List of Tables

Table 1 False Positive vs False Negative.....	17
---	----

List of Figures

Figure 1 IP address of the server machine with 'ifconfig' command.	3
Figure 2 Getting the open ports on server machine with 'nmap' command.	4
Figure 3 Data Tampering	8
Figure 4 SQL Injection	9
Figure 5 Client login	11
Figure 6 Ettercap intercepting login information.....	11
Figure 7 Client giving login credential on sqlmap page.....	12
Figure 8 Wireshark intercepts information	13
Figure 9 Phishing example.....	14
Figure 10 Phishing Cycle.....	15

Assigned Scenario

You are hired as a penetration tester for a new start-up company with a niche idea for rooms rentals. Their web application allows their customers to post information about rooms in their properties and for potential renters to hire them online. The application holds financial details for their customers and for properties owners. It also stores personal information for both customers and properties owners. Users credentials are stored on the database. Not all users have the same privilege.

A - Information gathering – Social engineering and nmap

1) Threats to open ports

Screen shots of port scanning on server machine

```
You can access the web apps at http://192.168.56.101/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.101, via Samba at \\192.168.56.101\\, or via phpmyadmin at
http://192.168.56.101/phpmyadmin.

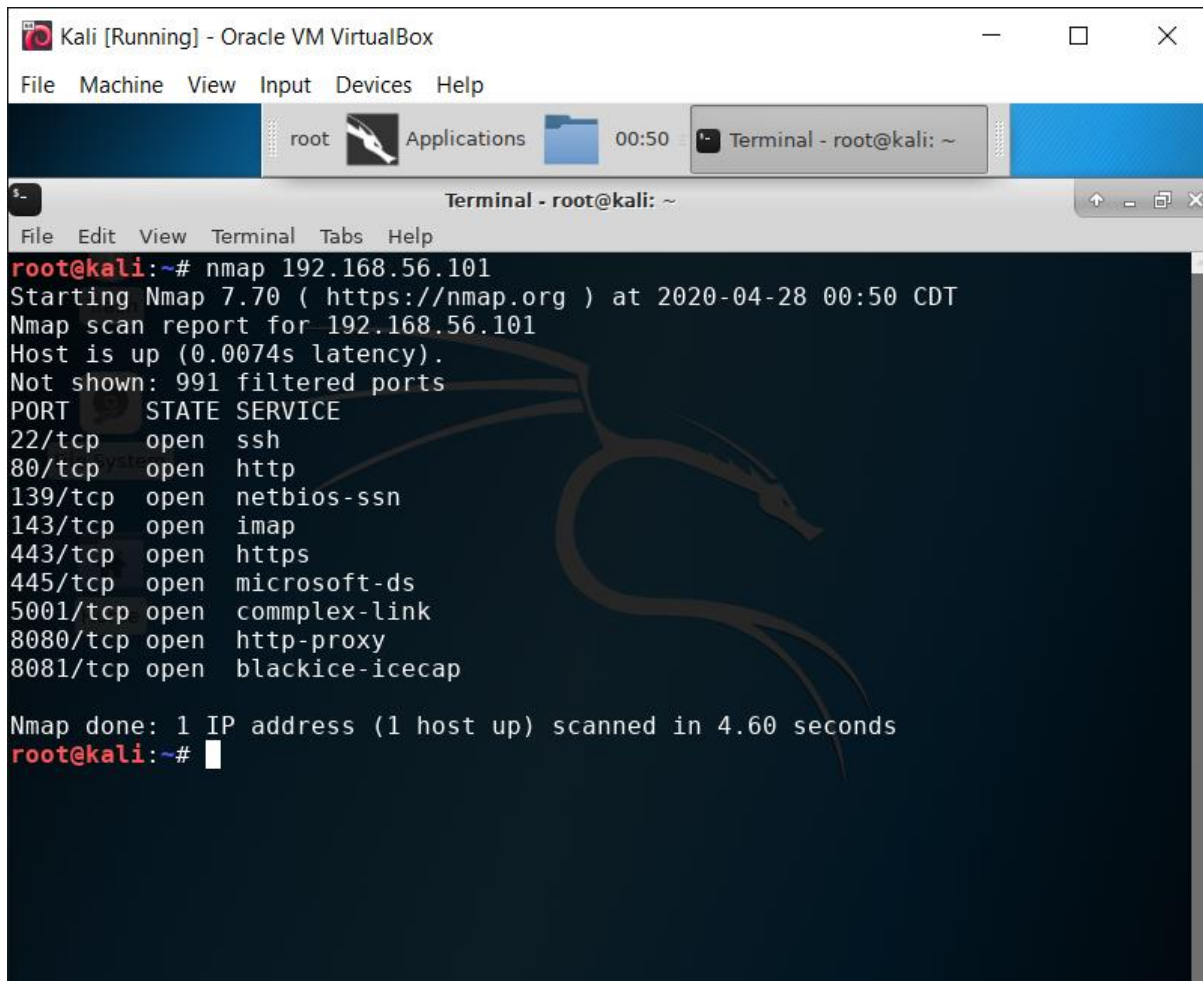
In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:17:eb:ec
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe17:ebec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1180 (1.1 KB)  TX bytes:7061 (7.0 KB)
          Interrupt:9 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14609 (14.6 KB)  TX bytes:14609 (14.6 KB)

root@owaspbwa:~#
```

Figure 1 IP address of the server machine with 'ifconfig' command.



```
root@kali:~# nmap 192.168.56.101
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-28 00:50 CDT
Nmap scan report for 192.168.56.101
Host is up (0.0074s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
5001/tcp  open  complex-link
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
root@kali:~#
```

Figure 2 Getting the open ports on server machine with 'nmap' command.

Figure 2 portrays the list of open ports in the server machine. The threats to those ports can be identified as:

- Viruses, malware and trojan horses could be spread through these ports.
- Vulnerable areas will be succumbed causing the application to be unresponsive and ultimately crash.
- IMAP (Internet Message Access Protocol) is used for sending emails through the internet. Attackers may be able to gain access to IMAP unless SSL (Secure Sockets Layer) is used.

In relation to my given scenario

Attackers may be able to penetrate the web application if HTTP (Hyper Text Transfer Protocol) is used. As the web application deals with financial data, such sensitive data might be stolen. Credit card info becomes vulnerable during a payment process. It is always recommended to use HTTPS (Hyper Text Transfer Protocol Secure) when integrating payment gateways. In order to gain HTTPS, the start-up company must purchase SSL (Secure Sockets Layer) certificate.

2) Two services running on the server machine that should be priority to protect

✓ SSH (Secure Shell)

SSH is used to log into a remote machine and execute commands more securely. Even though it's secure, attackers can gain access to the system due to similar reasons mentioned below:

- Users employing weak security keys
- Attackers gaining unauthorised SSH access

✓ HTTP

Services on HTTP have a high potential risk of being victim to attackers. Information gathering from HTTP is possible as requests sent to the server machine can be read by attackers. The reason for that is, HTTP does not possess the extra security layer unlike in SSL. It is always safe to go for HTTPS even if the application does not contain sensitive data.

3) Research three internet vulnerabilities related to those services

✓ SSH Common Vulnerabilities

- **SSH Key Tracking Troubles**

When many SSH keys are built up in an organization, overtime the organization could lose track of the keys. This occurs when development servers are moved to production environment. This could lead to an attacker gaining access to a key that was never revoked and they can have an entry point. (Walsh, 2018)

- **Embedded SSH Keys**

SSH keys are embedded within applications or scripts. Due to the lack of understanding of administrators they hesitate to change the keys. As a result, static SSH keys pave the way for backdoor attacks. (Walsh, 2018)

- **Sharing SSH keys**

For convenience SSH keys are shared among a common group of employees. Due to duplication of SSH keys, as few as five to 20 unique keys can give access to all machines in an organisation. This makes life easier of attackers. (Walsh, 2018)

✓ HTTP Common Vulnerabilities

- **HPACK Bomb**

This attack represents a “zip bomb” a malicious archive file implemented to crash a program. It can disable antivirus software. Small messages break into large sets of data eating up memory resources. (Osborne, 2016)

- Dependency Cycle attack

A new flow control mechanism was introduced by HTTP to optimise networks. Although this can be exploited when a request is done by an attacker which creates a dependency circle. It happens after an infinite loop is established which cannot be escaped when the flow control system attempts to process the requests. (Osborne, 2016)

- Stream Multiplexing Abuse

This problem erupts when attackers use security flaws present in how servers implement stream multiplexing functionality. These bugs can crash servers, resulting in a denial of service to legitimate users. (Osborne, 2016)

4) Pick the four least secure services running on the server machine and explain the danger posed by each of them

- HTTP

In HTTP data is exchanged using plain texts. These data can be easily exploited even by inexperienced attackers. Examples are sniffing attacks, DOS attack etc.

- IMAP

IMAP could be possible victim of DOS attacks and password spraying attacks. The main security issue is that IMAP was designed to accept plaintext login credentials.

- NetBIOS SSN

Enabling NetBIOS open to the outside gives the attackers an opportunity to reach shared directories and files. Sensitive information such as computer name, domain and workgroup maybe captured by them. (Anon., n.d.)

- SMTP

Similarly, to HTTP, in SMTP emails are exchanged in plain texts through the network. The attackers can easily penetrate and gain access to these emails.

B - Finding and exploiting vulnerabilities

- (1) Identify if the application is vulnerable to data tampering and exploit it if possible

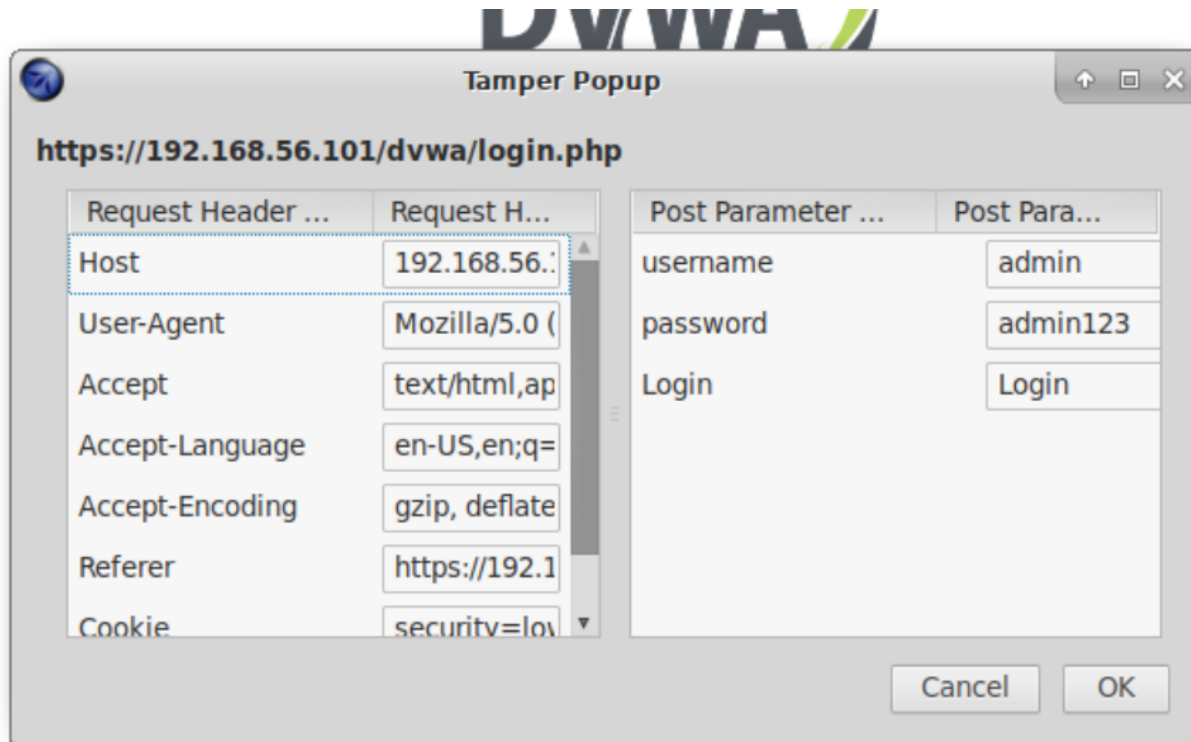
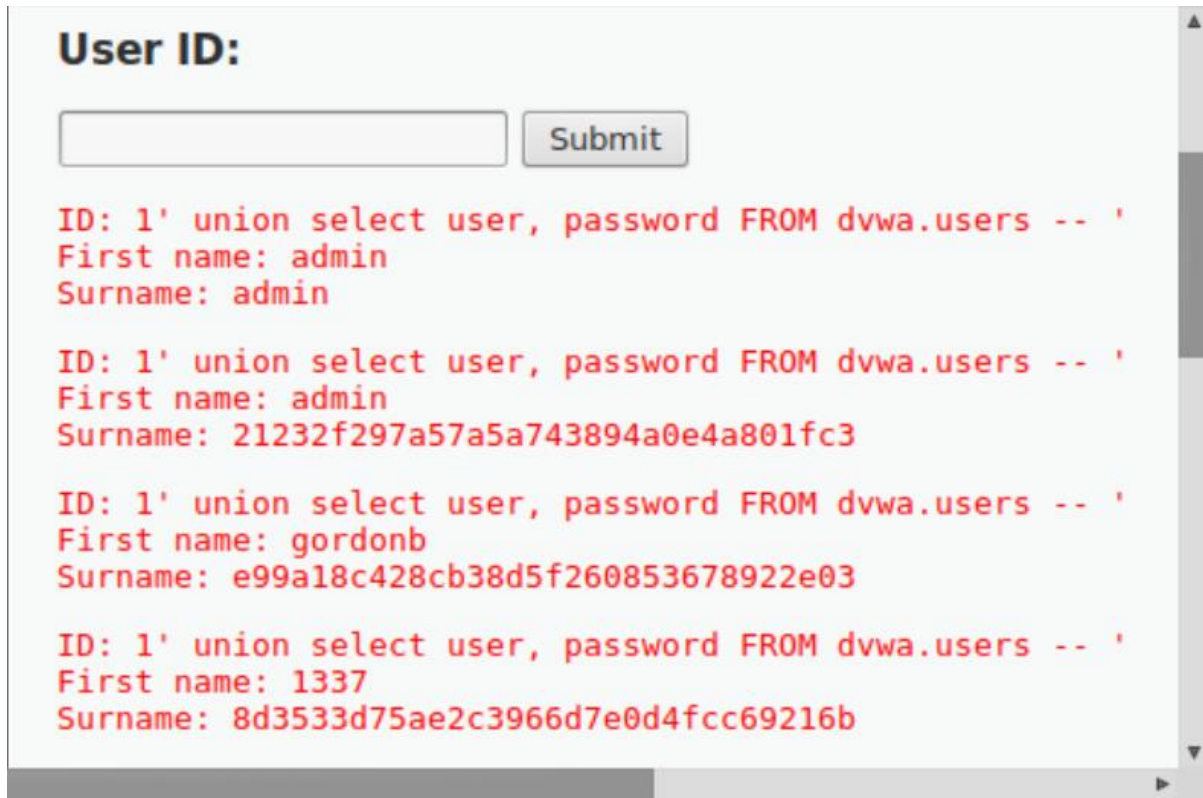


Figure 3 Data Tampering

In relation to my given scenario

It was observed that the web application of the server machine succumbed to data tampering. The data tampering service successfully intercepted the HTTP request. User credentials of property owners and customers could be leaked if successfully intercepted and data is tampered.

(2) Identify if the application is vulnerable to SQL injection and exploit it if possible



User ID:

ID: 1' union select user, password FROM dvwa.users -- '
First name: admin
Surname: admin

ID: 1' union select user, password FROM dvwa.users -- '
First name: admin
Surname: 21232f297a57a5a743894a0e4a801fc3

ID: 1' union select user, password FROM dvwa.users -- '
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' union select user, password FROM dvwa.users -- '
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

Figure 4 SQL Injection

In relation to my given scenario

During the penetration testing it was observed that the application is vulnerable to SQL injection attacks. SQL union queries can show user credentials. The attacker can reveal the username and password. The information of property owners and customers stored in the database can be accessed and manipulated after logging in with the username and password.

(3) Identify if the application is vulnerable to XSS vulnerability and exploit it if possible

In relation to my given scenario

The application succumbed to cross site scripting attacks (XSS attacks). The search and find functionality of the web application might get affected. Hence the search for room rentals might show false information and mislead customers and property owners. Although this won't be affecting sensitive data, yet it is a negative impact on the company.

(4) Can you identify any other vulnerability?

- Brute Force Login

Brute force login can be depicted as the simplest way to get access to a website or a server. The technique is to try various combinations of usernames and passwords persistently until it succeeds. The hacker's motive is getting illegal access to steal data or to shut a website down. The hacker might inject the website with malicious scripts leaving no digital footprints behind. Therefore, it is recommended to follow best password practices in order to secure servers and web applications. (Rehman, 2018)

C – Man in the Middle attacks and Social Engineering

1) If a client is connected to the server while you are testing the environment, identify what are the information that can be obtained from a packet capture of their communication

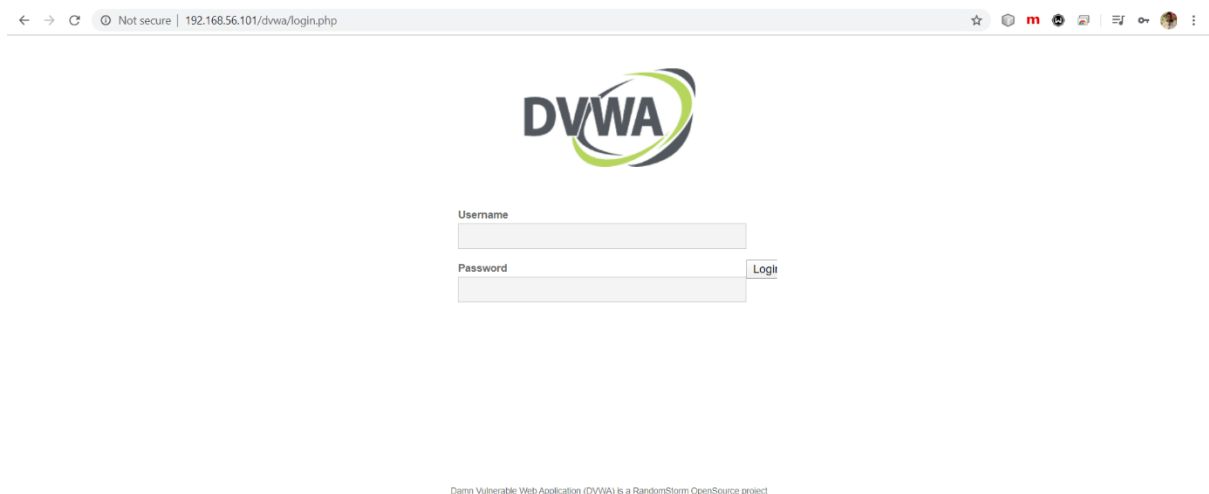


Figure 5 Client login



Figure 6 Ettercap intercepting login information

As the above screenshots portray, Figure 5 shows the client machine on the login page.

Figure 6 shows Ettercap intercepting login information between the server and the client machines. Tools such as Ettercap can be utilized to monitor login information exchanged between the client and server machines.

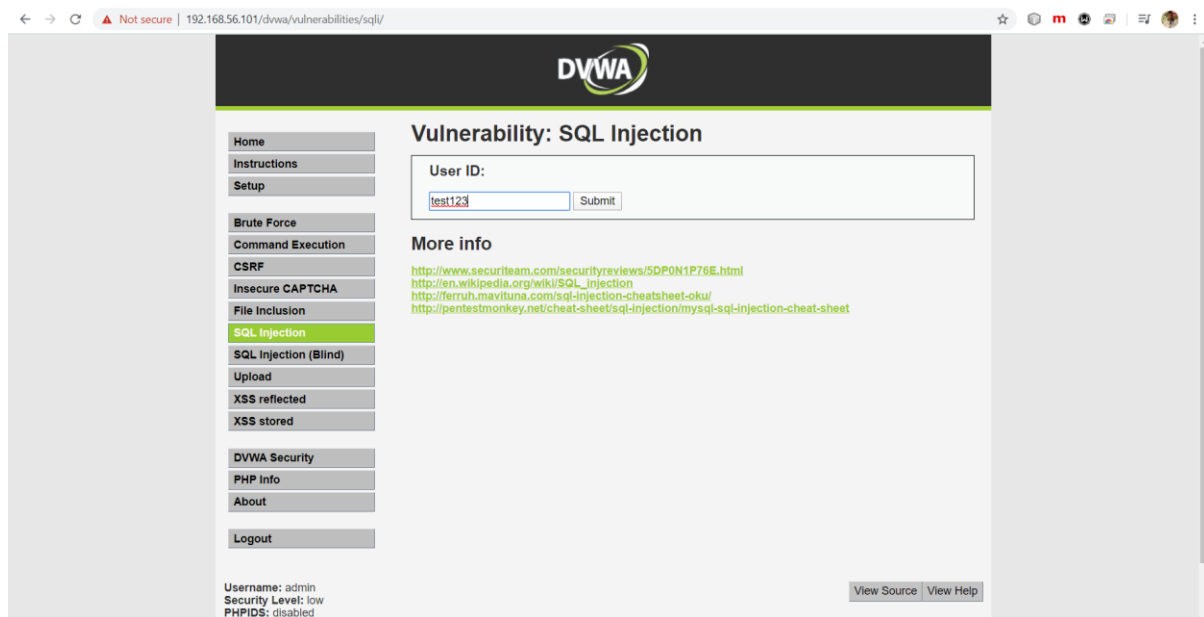


Figure 7 Client giving login credential on sqli page

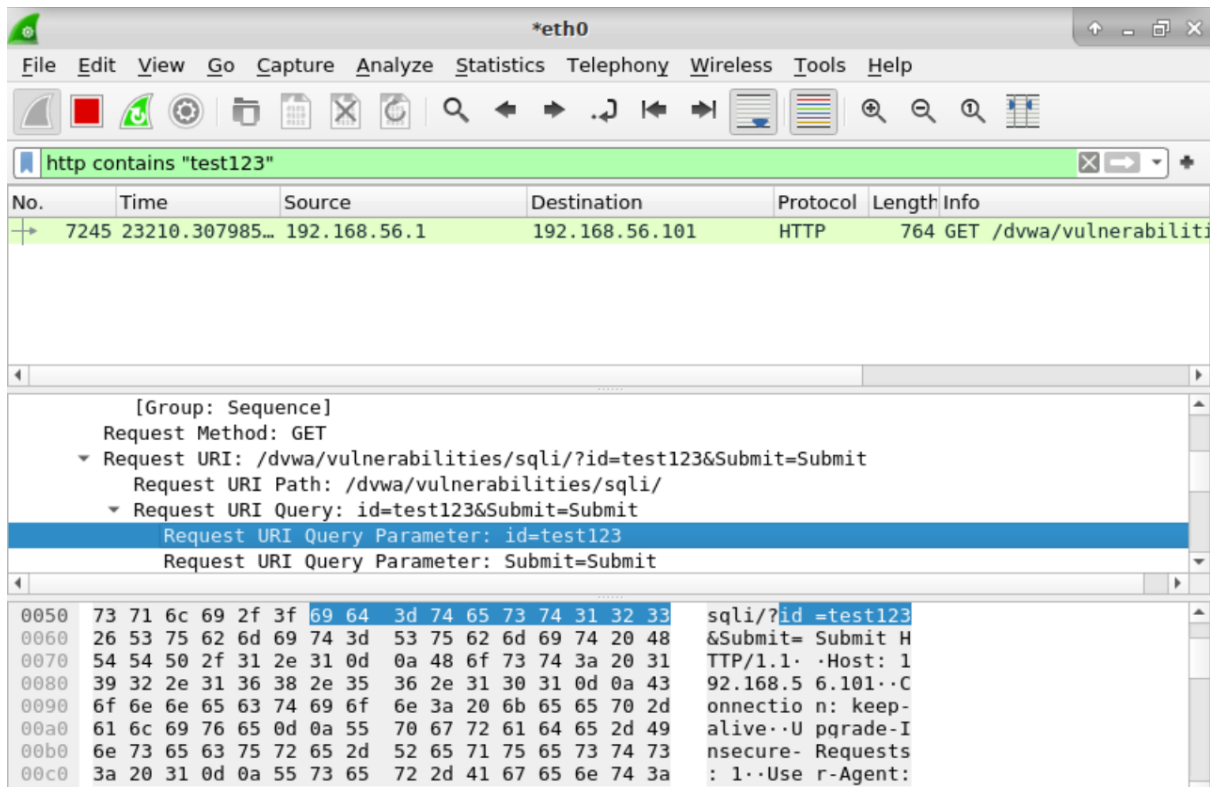


Figure 8 Wireshark intercepts information

Wireshark is a tool used to intercept all network traffic exchanged between the client and server machines. Figure 8 shows Wireshark capturing login information entered in the sqli page by the client machine. The technique used here to intercept data is ARP poisoning.

In relation to my given scenario

The Ettercap tool can be used to alter intercepted data in Ettercap filter files. Attackers can program to intercept data on ports. Sensitive data such as financial information and personal information of property owners could be intercepted and modified.

2) Identify a method that lure a normal user of the server to your computer instead of the server machine

A common method to lure a normal user to your machine is to launch a phishing attack. Phishing uses disguised email as its weapon to launch an attack. The objective is to trick the email recipient into believing that the email is significant and from someone they trust. It lures the recipient to click a link or download content. Phishing is distinguished from the form the message takes. It may be a trusted person or some organisation the victim deals with. Phishing is one of the oldest yet widespread modes of cyberattacks. (Fruhlinger, 2020)

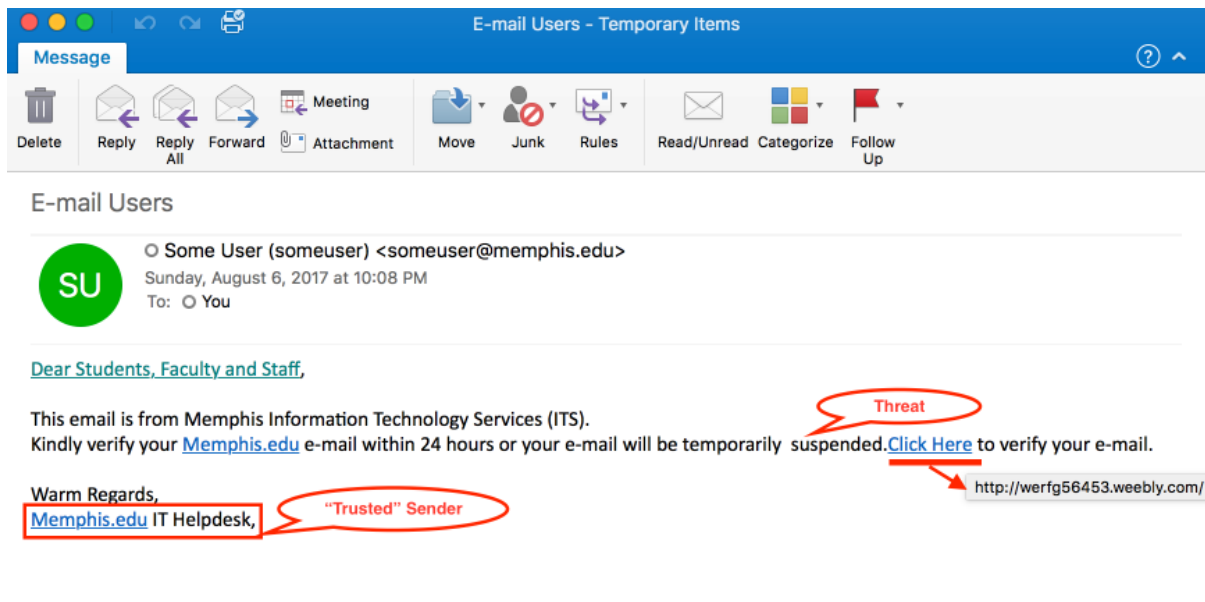


Figure 9 Phishing example

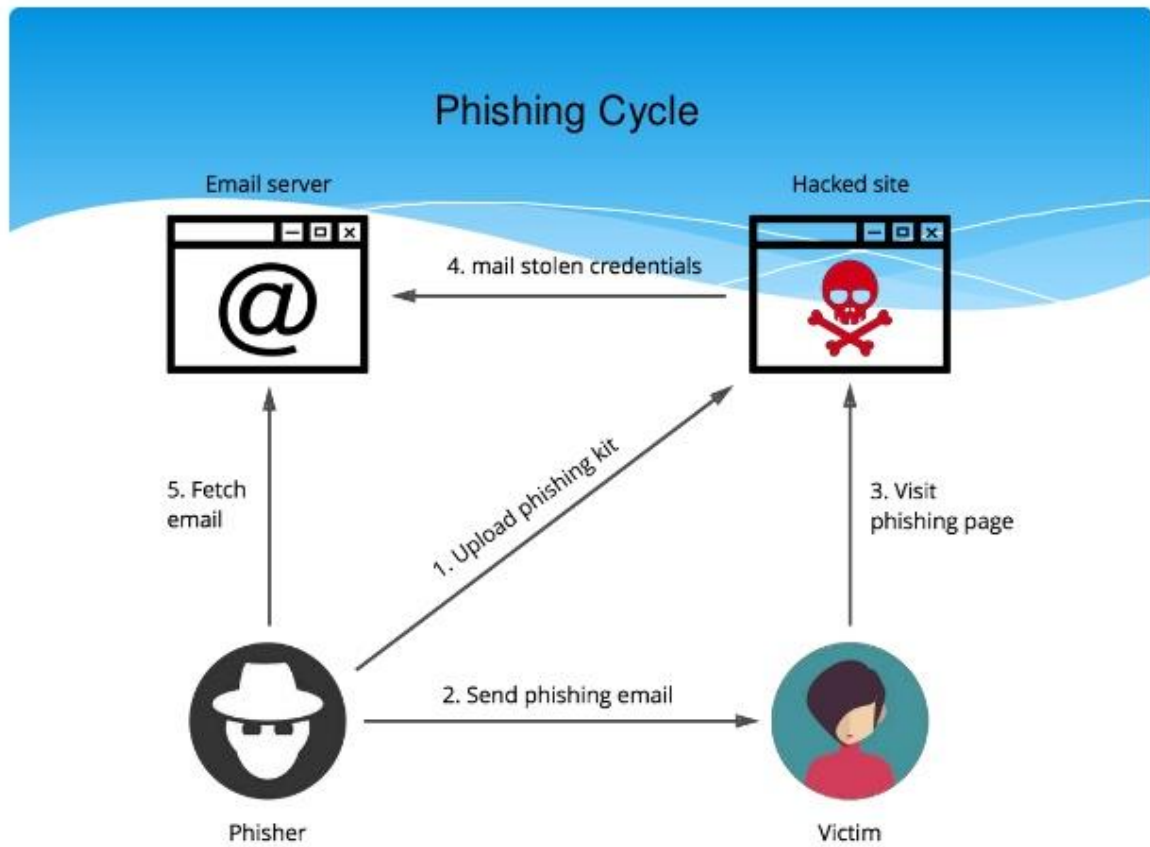


Figure 10 Phishing Cycle

3) If the server is protected, what can you do to penetrate the system from the client side

- Honeypot attacking

With the development of technology wireless networks also have evolved drastically. They are growing in terms of bandwidth and range. A hacker can easily lure users to a malicious network without users getting suspicious. A wireless honeypot is a device with the configuration to be an access point with the same SSID as to another access point in the vicinity. The honeypot is configured with a proxy to the attacker's computer. If a user connects to the honeypot all their network traffic will be filtered or monitored by the attacker. (Anon., n.d.)

D – Protecting the Server

1) Port Knocking

Port Knocking can be identified as a mechanism executed with the objective of gaining access to a port which is already closed by a firewall. It can be also defined as a method to transmit data through blocked ports. Before transmitting data, it must be verified that proper authentication is done for the users who access those ports. A potential benefit of port knocking is that alleged cyber attackers cannot find the respective machine as its ports are closed. If the user intends to establish a connection to the service running the port, they must connect several predefined ports with a specific sequence. Abiding to that method will allow the authorised user to gain access to the relevant service they intended. This method is effective as it minimizes the chances of potential attacks on the ports and simultaneously the user can access the service without any restriction. Administrators can conceal vulnerable services in this manner, although authorised users will have access to the services. If a user intends to implement port knocking on their server machine, a thumb rule they should follow is to add a rule to the server's firewall. It will drop all requests. Doing so will make sure that the server machine's services do not get caught to the scanning done by potential attackers.

2) False Positives and False Negatives in relation to a Network Intrusion Detection System

Intrusion Detection System

The objective of an Intrusion Detection System (IDS) is to identify malicious intrusions. The system does that by analyzing and monitoring the network activity occurred through the network.

False Positive	False Negative
<ul style="list-style-type: none"> False positive is when the IDS detect normal network activity as a malicious intrusion. 	<ul style="list-style-type: none"> False negative is when the IDS does not detect malicious intrusions, although it is not normal network activity.

Table 1 False Positive vs False Negative

3) Difference between Intrusion Detection System IDS and Intrusion Prevention System IPS

We can observe a common feature for both IPS and IDS. It is going through network packets in comparison of its contents searching for database threats.

Intrusion Detection System

IDS is a tool to detect and monitor network traffic. It can be utilised to identify malicious network activities and intrusions. IDS cannot control any malicious activities.

Intrusion Prevention System

IPS is utilized as a tool to control and prevent network related malicious activities. IPS works according to a predefined set of rules. They are able to control the packets delivered to the network. Hence they either accept or reject packets independently. An IPS can block network related traffic if suspicious activities are detected.

Suggest a recommendation for the scenario you have in hand

My scenario is based on a start-up company for room rentals. The web application holds sensitive data such as personal information for both customers and property owners. More significantly it holds financial details for their customers and for property owners. As a result, it is extremely important in order to secure the web application from potential attackers. I recommend an IPS for the server machine as it has the ability to both detect and control an attack. As I have mentioned above, the web application deals with sensitive information. In order to stop any leakage or misuse of sensitive data, it is recommended to choose the safer option which is IPS.

4) Firewall, Snort and Iptables

Firewall

- A firewall is a network security tool used to surveillance inbound and outbound network traffic. It is programmed according to a set of rules and regulations in order to allow or block data packets. The objective of a firewall is to create a barrier between the internal network of the user and the incoming network traffic. The goal is to protect the user's machine from hackers, viruses, trojan horses etc. coming as malicious traffic from the internet.

Snort

- A user can utilize snort to analyse and detect particular types of inbound and outbound traffic.

Iptables

- We can use Iptables, when we need to block a particular type of inbound and outbound traffic.

I recommend using Iptables as the user can control the inbound and outbound network traffic according to their wish. Snort cannot be used to filter data packets. Firewall does not have functionalities as much as Iptables.

5) Other security recommendations

As I have mentioned above the given scenario to me is based on a start-up company for room rentals. The web application deals with sensitive data such as financial information and personal information of customers and property owners. In order to secure such data, I must recommend the safest systems. After analysing strength and weaknesses of my findings, I would like to mention some additional security recommendations. Although this is a start-up company the network administrators should keep track of SSH keys. Typically, the administrators lose track of these credentials when development servers are migrated into production environments. The SSH keys should be revoked and not left unaccounted for a long time. If attackers gain access to an unrevoked key, they could have a network entry point. Hence it is recommended to the network administrators of the start-up company to keep track of the SSH keys. (Walsh, 2018)

Word count of content - 2418

References

Anon., n.d. *Beyond Security*. [Online]

Available at: <https://beyondsecurity.com/scan-pentest-network-vulnerabilities-netbios-information-retrieval.html>

[Accessed 26 4 2020].

Anon., n.d. *packt*. [Online]

Available at:

https://subscription.packtpub.com/book/networking_and_servers/9781782163183/7/ch07lv11sec44/ho-neypot-attacking

[Accessed 26 4 2020].

Fruhlinger, J., 2020. *CSO Online*. [Online]

Available at: <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

[Accessed 27 4 2020].

Osborne, C., 2016. *ZDNet*. [Online]

Available at: <https://www.zdnet.com/article/severe-vulnerabilities-discovered-in-http2-protocol/>

[Accessed 25 4 2020].

Rehman, I. U., 2018. *CLOUDWAYS*. [Online]

Available at: <https://www.cloudways.com/blog/what-is-brute-force-attack/>

[Accessed 26 4 2020].

Walsh, J., 2018. *CYBERARK*. [Online]

Available at: <https://www.cyberark.com/blog/four-ssh-vulnerabilities-you-should-not-ignore/>

[Accessed 25 4 2020].