

Ida Matero  
Ethical Hacking: Research and Course  
Compilation

---

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

22 November 2016

Author(s) Title	Ida Matero Ethical Hacking
Number of Pages Date	37 pages + 1 appendix 22 November 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networking
Instructor(s)	Marko Uusitalo, Senior Lecturer
<p>The constant leaps forward in all technological areas have begun to cause increasing amounts of concern to both business owners and private individuals. Security is one of the areas where constant education and improvement is required in order to keep a system inaccessible for unauthorized personnel.</p> <p>Ethical hacking is a form of penetration testing where the tester takes the role of a legitimate attacker and attempts to access the system through unauthorized means. This attack shows the vulnerabilities in the system and network and points out the components which must be hardened in case of a true attack.</p> <p>The objective of this project was to gather and compile information into a course on Ethical Hacking. The course consists of ten chapters made of PowerPoint lectures and is planned to be complemented by the Netlab+ practical exercise labs on penetration testing.</p> <p>The target audience for the course is students with intermediate knowledge on internet technology and networking, but no prior knowledge on penetration testing is required.</p>	
Keywords	Ethical hacking, Security, Penetration testing, Vulnerability scanning

## Contents

### List of Abbreviations

1	Introduction	1
2	The Hacking Process	2
2.1	The CIA Trinity	3
2.2	The Information Security Management System	4
3	The Phases of Penetration Testing	5
3.1	The Hacking Cycle	5
3.2	Reconnaissance	6
3.2.1	Google Hacking	6
3.2.2	Shodan	7
3.3	Scanning	8
3.3.1	Locating Open Ports	8
3.3.2	Network mapping	9
3.3.3	OS Fingerprinting	10
3.4	Gaining and Maintaining Access	10
3.4.1	Passwords	10
3.4.2	Password Cracking Methods	12
3.4.3	Password Cracking Software	12
3.4.4	Man-in-the-Middle	13
3.4.5	Backdoors	15
3.4.6	Denial of Service	15
3.5	Covering tracks	16
3.5.1	Intrusion Detection System	16
3.5.2	Intrusion Prevention System	17
3.5.3	Anti-Virus	17
3.6	Malware	18
3.6.1	Viruses	18

3.6.2	Worms	20
3.6.3	Trojans and Spyware	20
3.7	Social Engineering	21
3.7.1	Phishing	21
3.7.2	Vishing	21
3.7.3	Tailgating	22
3.7.4	Social Media	23
3.7.5	Counteracting Social Engineering	23
3.8	Mobile Security	23
3.8.1	Mobile Devices	24
3.8.2	Cloud Services	24
3.8.3	Bluetooth	25
3.9	SQL Injections	26
3.10	Physical Security	27
3.10.1	Access Restrictions	27
3.10.2	Server Room Security and Maintenance	27
4	Ethical Hacking Course Compilation	29
5	Netlab+ Learning Environment	31
5.1	Requirements	32
5.2	Course Content	34
5.3	Software in Practicals	35
5.3.1	Operating Systems	35
5.3.2	Software	35
5.4	Learning Material	36
5.5	Improvements	36
6	Conclusion	38

Image Sources

References

## List of Abbreviations

AV	Anti-Virus. A software or hardware –based program used to detect and remove malicious software.
CEHv9	Certified Ethical Hacking version 9. A certification exam to show one meets or exceeds the minimum standards of the ethical hacking credentials.
CIA	CIA triad. Short for Confidentiality, Integrity and Availability.
DNS	Domain Name System. A protocol used for translating IP-addresses into domain names and vice versa.
DoS	Denial-of-Service. An attack where the goal is to make a system or a service unavailable, typically by flooding it with redundant requests.
DDoS	Distributed Denial-of-Service. A Denial of Service attack where more than one IP-address is used in the attack.
FTP	File Transfer Protocol. A protocol used for computer file transfer between a client and a server.
ICMP	Internet Control Message Protocol. A protocol used by network devices to send error messages. ICMP echo requests, also known as ping requests, are used to check whether a service available at a given time.
IDS	Intrusion Detection System. A software used for monitoring a network for malicious activity. Upon finding anything harmful it will inform a system administrator.
IoT	Internet of Things. All physical devices connected to the internet including cars, buildings and house appliances.
IPS	Intrusion Prevention System. A software used for monitoring a network for malicious activity. Upon finding anything harmful it will inform the system administrator and also quarantine or terminate the harmful process.

MITM	Man-in-the-Middle. An attack where the attacker captures and potentially alters the content relayed between two hosts.
SQL	Structured Query Language. A programming language used to create and control databases.
SSID	Service Set Identifier. A wireless network identifier. In practice SSID stands for the name of a wireless network.
TCP	Transmission Control Protocol. One of the main protocols used in TCP/IP networks.
TTL	Time to live. A limiting mechanism for data lifetime in a computer or in a network.
UDP	User Datagram Protocol. One of the main protocols used for online telecommunications.

## 1 Introduction

The current climate in computer security is fickle and volatile. New programs and exploits are constantly found with new ways to access secured systems, making computer security a quickly evolving and changing area. It is difficult to keep a whole network hardened when any new update could have a security issue leaving the system open for exploitation.

Ethical hacking is a form of penetration testing where the tester assumes the role of a legitimate attacker with permission of the target system owner. The tester is a network and security expert who will attempt to find vulnerabilities in the system and network in order to inform the owner about their existence. Once the security risks are known the process of hardening the network can take place.

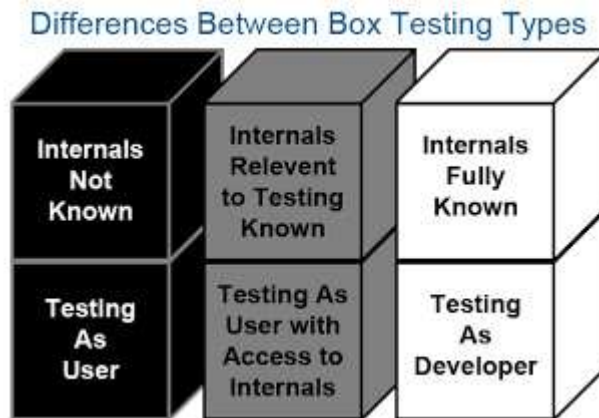
This form of penetration testing is becoming more common, as keeping a system exploit-free during its development becomes extensively more difficult the more complex said system is. The extreme time pressure with development increases the probability of error, making it easier to test for vulnerabilities at a later date.

The objective of this project was to research the topic of ethical hacking and penetration testing, and compile a course on the subject based on this research. Resources for information are readily available in the forms of online sources, research papers and published books. The security community and professionals linked to it generally take the path of total transparency, making it easier for both ethical hackers and legitimate attackers to find information on security risks and threats.

Both the compiled course and this thesis go through the hacking process from the point of view of an ethical hacker.

## 2 The Hacking Process

The different approaches to a hacking process can be simplified into three different categories: white box, grey box and black box, as shown in the Picture 1 below.



Picture 1: Box Testing Types

As shown in Picture 1, in a white box test the penetration tester has all the important information on the network and the credentials necessary to access it. This test examines the development and internal workings of the system. In a grey box test the tester has partial knowledge of the system, usually only knowledge necessary to complete the test. This analyses the way an insider attack would work – for example how well the security would hold up if one of the employees would attempt to extract secure information. A black box test is one where the attacker has no prior knowledge of the system or the network and tries to behave exactly like a legitimate assailant. The goal in this test is to find the so called soft spots of a network in order to secure them against future attacks.

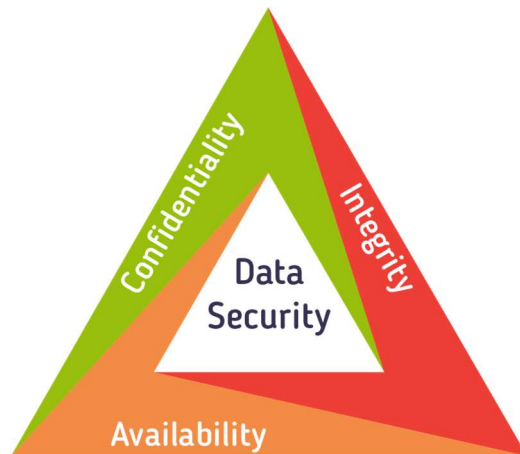
Black box testing is the most common of the three main approaches. The reason to this is the difficulty, and proportionally the price, of the two others. White box testing is the most extensive and delves as deep as going through the code written for the system to find any errors and security issues. (Software Testing Fundamentals, 2016)

This thesis concentrates mainly on the black box approach on accessing the system from the outside and appearing as a malicious hacker to find the vulnerabilities of the system.



## 2.1 CIA Trinity

CIA trinity consists of confidentiality, integrity and availability and it is used to describe data security, as shown in Picture 2.



**Picture 2: CIA Trinity**

In Picture 2, confidentiality stands for the privacy of the data. Ensuring confidentiality comes down to designing a system where only those who have the authorization to see certain information are able to access it. Integrity stands for consistency and accuracy of the information: it cannot be altered in transit or otherwise without the necessary credentials. In practice this comes down to file and user permissions, and assuring the integrity of data with encryption checksums. The third side of the triangle is availability, which assures the accessibility of the data. It is guaranteed by maintaining hardware, being ready for immediate repairs and keeping the systems up to date.

All three of these are important, especially with respect to one another. The best way to assure complete confidentiality and integrity is to lock a machine in a safe room with no Internet access, but this provides absolutely no availability. There must be a balance between the three and leaning towards a single aspect should be kept to a reasonable and explicable level

## 2.2 The Information Security Management System

The Information Security Management System, also known as ISMS, is the company policy when it comes to IT-related matters. Not all companies have an ISMS, but it is recommended especially for larger companies. An ISMS is a long-term plan for security situations. It includes company policy for preventive security and the protocol to follow in the case of an attack.

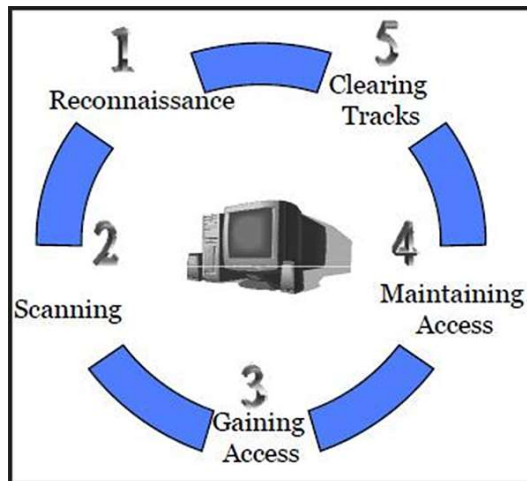
Crafting an ISMS can be divided into four stages of a cycle. These stages are sometimes referred to as the “Plan-Do-Check-Act” cycle. The first stage is to plan an appropriate and inclusive security plan for the specified needs of the company. Once that is completed, the next step is to follow this policy while simultaneously evaluating the policy, placing improvements as necessary. The last stage is the act stage where the improvements are implemented. This is also the stage under which reaction to an attack falls.

An Information Security Management System is presumed to be constantly up-to-date as technological security is ever changing with constant new threats which must be planned for.

### 3 The Phases of Penetration Testing

#### 3.1 The Hacking Cycle

The hacking process can be simplified into 5 parts, shown in Picture 3.



Picture 3: Hacking process

These five parts of the cycle contain the whole penetration testing process. The sequence isn't clear-cut and often the order changes depending on the target system – for example in a case of preventing security logs from happening by avoiding detection programs, an attacker is technically conducting the fifth step while simultaneously executing the third one.

The methods for hacking a system are as many and varied as are the attackers, but certain programs are more common or more successful than others.

Kali Linux has gathered together many of these programs under a single operating system, causing it to be one of the most common distributions to be used for penetration testing. Some of the programs, such as Wireshark which is used to capture and list packets sent and received on a certain interface, can be used as a utility tool to achieve different results on separate steps of the process. Others, like Jack the Ripper which is a password cracker, have a very specific set of functions and are used on a very specific part of the cycle to achieve a set goal.

## 3.2 Reconnaissance

Reconnaissance is the first step any hacker should take regardless of intentions. It is the process of finding information about the target in different ways such as search engines, social media, the target's own website and anything they may have posted on the Internet. This process is time-consuming and is considered most important to complete thoroughly, as all the information uncovered in this step will be used later on in the process to minimize unnecessary actions which might leave tracks on the security logs of the target system.

The methods for information gathering range from social media searches to specified Google operators. Looking the company location up in Google Maps can let the attacker navigate to the area to use a packet analyzer. A Whois lookup lets anyone find the domain names, registration and expiry dates, name servers and holder information, along with similar domains which are still unused. People tend to mistype website information often, which is why Google has also purchased domains such as [www.gogle.com](http://www.gogle.com), [www.google.com](http://www.google.com) and [www.googel.com](http://www.googel.com). In the case of someone else owning [gogle.com](http://gogle.com), for example, and setting a page looking exactly like Google's homepage people might attempt to sign in to Gmail and the malicious owner would then have their login information.

Another way to find information on system information is to go through job postings. A company may be looking for an IT administrator who has experience with certain programs or operating systems, which immediately tells the attacker these systems are in use within the company.

### 3.2.1 Google Hacking

Google Hacking is a fairly anonymous way of finding information on any online target. In addition to its basic search system, Google also has other ways to refine searches which are called advanced operators. Most of these operators can be combined together to narrow the result further.

## Advanced Operators at a Glance

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Picture 4: Google Advanced Operators

Picture 4 shows a list containing most of the Google advanced operators. Combining this search method with other information found from different scanning methods can reveal information which is not supposed to be visible for the general public.

### 3.2.2 Shodan

Shodan is an Internet search engine for all devices connected to the Internet. It shows not only routers and servers but also IP-cameras, webcams and even baby monitors. Shodan searches the Internet for IP-addresses with open ports and lists them on the website. The website has a one-time user fee with which anyone can see all results – free use of the website only shows first ten results of any search.

Shodan has had negative news coverage for the way it forages through devices connected to the Internet without censure. It lists out appliances belonging to the Internet of Things which can be used to cause harm to their owner. Tools such as heart monitors, biochip transponders or car sensors can all be accessed if they are connected to the Internet and not adequately protected against attacks.

### 3.3 Scanning

Scanning is the second step of the hacking process. The information gathered previously during the reconnaissance phase is important as it helps fine-tune the search. Specific searches not only decrease the time required to find information but also lower the chances of an anti-virus or an intrusion detection system logging the scans or alerting the system administrator.

#### 3.3.1 Locating Open Ports

Network mapping is done via software such as Nmap, OpenVAS and network sniffers like Wireshark or tcpdump. Nmap is a terminal based program used for finding out whether a port is open, closed or listening. It can also be used to find hosts, detect the operating system and determining application names and version numbers. Pictured below is a search mapping open ports for the IP-address of 192.168.68.12.

```
root@Kali2:~# nmap 192.168.68.12

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-12-15
mass_dns: warning: Unable to determine any DNS servers. Rev
Try using --system-dns or specify valid servers with --dns
Nmap scan report for 192.168.68.12
Host is up (0.0043s latency).
Not shown: 991 closed 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 1.20 seconds
```

Picture 5: Nmap port scan

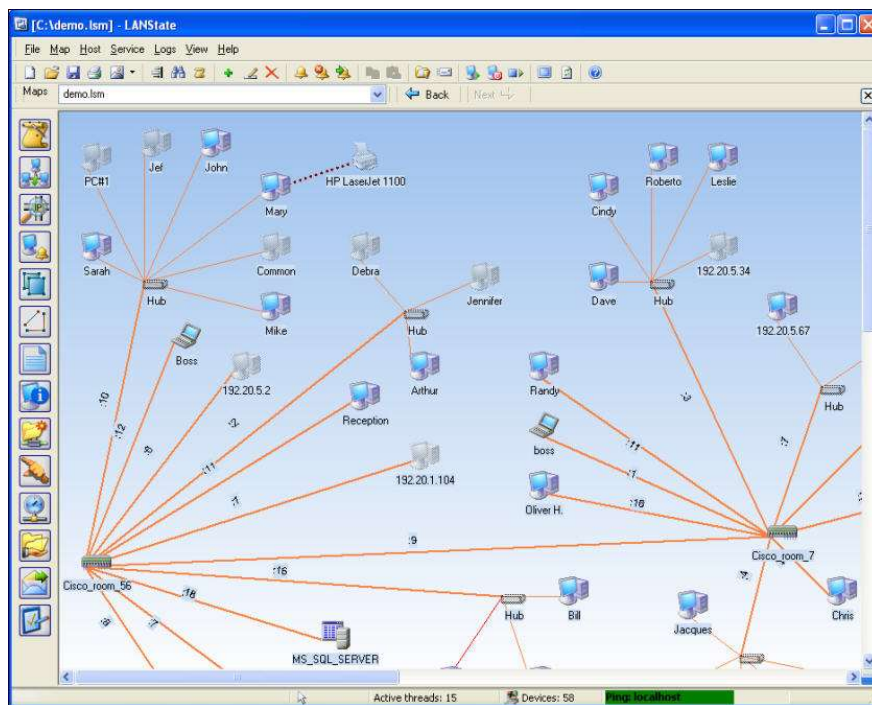
Finding out which ports are open, which are closed and which service runs on each port helps to decide the next step of the process. In the case shown in picture 5, for example, running tests on port 20 for HTTP-traffic related vulnerabilities should be perceived as a waste of time as port 20 is not open nor would it be likely to accept HTTP-related traffic in any case, considering port 20 is usually used for FTP – the file transfer protocol.

Wireshark and tcpdump are both packet analyzers. This means they see and listen to the traffic on a certain interface on a network listing it out simultaneously. The main difference between the two programs is that Wireshark has a graphical user interface while tcpdump is terminal-based.

### 3.3.2 Network mapping

Network mapping is usually done with dedicated network mapping software. It is also possible to do manually but a manual mapping is a long and slow process if the network size is medium or large.

Having a mapped network topology makes visualizing the network communicational and security aspects simpler. Picture 6 shows the result of a LANState network mapper.



Picture 6: LANState network mapping

Looking at Picture 6 it is immediately visible which computers are connected to which hubs, routers or switches.

### 3.3.3 OS Fingerprinting

Operating system fingerprinting can begin at the reconnaissance step if the attacker can find relevant work position advertisements. In the case of looking for a new employee and listing the requirements a job posting may hold information on the systems used within the company or service provider.

The process of fingerprinting itself can be divided into two categories: active and passive. The difference between the two is that active fingerprinting introduces traffic into the target network, increasing the risk of leaving logs and thus also increasing the possibility of getting caught. Passive fingerprinting concentrates on using packet analyzers to listen to and investigate network traffic. In both cases the network responses to packets are analyzed in order to narrow down the possible operating system used.

## 3.4 Gaining and Maintaining Access

Attempting to gain access to a system is the point of the cycle where having a written and signed contract including permission to conduct the penetration testing is imperative. Methodically scanning a system is frowned upon and many intrusion detection systems can log it happening, but the malicious gain of access is the first point upon which legality truly comes into play. Attempting to crack the passwords to a system or support a denial-of-service attack can lead to fines or even imprisonment.

Once the permissions of system entry and legality are no longer an issue it is possible to move to the methods of hostile entry.

### 3.4.1 Passwords

The most common attempted entry is through passwords. Many individuals and companies bluntly neglect their security by not changing the default passwords on their hardware and software. The Internet has multiple lists of default passwords for routers,



switches, antivirus-software and other security software. Attempting to gain access by finding out the default password only demands a minimal amount of the attacker's time and yields a surprising amount of success.

Another security risk are easy passwords. The following Figure lists the worst passwords of 2015 listed originally by Teams ID.

Rank	Password	Change from 2014	13	abc123	Up 1
1	123456	Unchanged	14	111111	Up 1
2	password	Unchanged	15	1qaz2wsx	New
3	12345678	Up 1	16	dragon	Down 7
4	qwerty	Up 1	17	master	Up 2
5	12345	Down 2	18	monkey	Down 6
6	123456789	Unchanged	19	letmein	Down 6
7	football	Up 3	20	login	New
8	1234	Down 1	21	princess	New
9	1234567	Up 2	22	qwertyuiop	New
10	baseball	Down 2	23	solo	New
11	welcome	New	24	passw0rd	New
12	1234567890	New	25	starwars	New

**Picture 7: Worst Passwords 2015 listed by TeamsID**

Coincidentally, these are also the most common passwords.

A company can control unauthorized access by limiting the use of unsecure passwords. This is done through password policies, which include rules about password length, complexity, minimum and maximum password age, and consequences of wrong password input – usually the lockdown of that account after a certain number of incorrect passwords.

### 3.4.2 Password Cracking Methods

Password cracking can be done through direct input to the target system or through dedicated software which compares the hash of an account password to a list of potential passwords in hashed form, trying to find a match. Different attacks have dissimilar levels of being effective, especially when it comes to secure passwords.

A brute force attack is exactly what it's named for: an attack which pushes through by pure force. It tries every possible combination of letters, numbers and special characters depending on parameters given to it, and is extremely effective with short passwords. However, the longer and more complex a password is the more time a brute force attack requires. For example, a password consisting of six characters which are either upper- or lowercase alphabetic characters or numbers requires only 1.5 hours when done with a fast, dual processor computer. (Lucas, 2009) If the password length is increased to 8 characters, cracking it will take 253 days with the same PC.

Another common attack is the dictionary attack. It uses a premade wordlist consisting of every word in the dictionary and tries to match all of them to the account one at a time. This attack works very well not only on passwords consisting of words found in the dictionary, but also on re-used passwords.

Using the same secure password in an insecure environment causes the password to lose its security. This is why online banks and other services which contain private information demand the user to choose a unique password. If the same password is used on an unsecured website or application and that site or application has a security leak, the password may be released online and added to a hacker's dictionary wordlist and later used in an attack.

### 3.4.3 Password Cracking Software

There are multiple options for password cracking applications, some with their own user interface and some used from the command line terminal. John the Ripper, shown in Picture 8, is one of these applications. It is run from the command line and is primarily used for its dictionary attack.

```

root@kali2:~# john -wordlist=/usr/share/john/password.lst hashes.txt
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypto" file managing data? List, sort, group, tag and search your pentest data
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128-SSE2 2x])
Remaining 3 password hashes with 3 different salts
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
password Interrupt (mreedy)
123456 > (jsmith)
2g 0:00:00:10 DONE (2016-11-19 06:24) 0.1881g/s 333.5p/s 429.9c/s 429.9C/s modem
..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

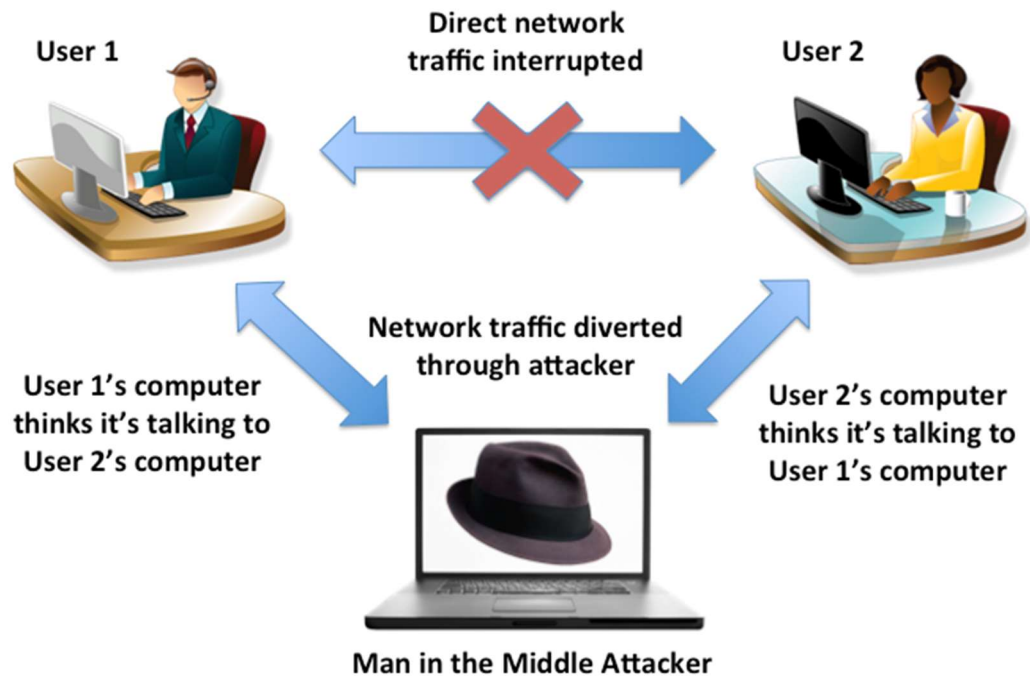
**Picture 8: John the Ripper**

Picture 8 above is output from a command which tells the system to run John the Ripper's default wordlist through the file hashes.txt, into which the account password hashes were previously copied to from /etc/passwd and /etc/shadow, the default password directories for Linux. John the Ripper compares the default dictionary hashes to the ones stored in hashes.txt and finds two matches: users mreedy and jsmith. The passwords of these users are "password" and "123456" respectively.

This shows how easy and fast it is to find unsafe passwords – this particular attack took only ten seconds to find and list these two passwords.

#### 3.4.4 Man-in-the-Middle

A man-in-the-middle attack is successful when an attacker manages to intercept traffic between two hosts and decrypt it. As shown in the following picture, the traffic is then diverted to go through the attacker.



**Picture 9: Man-in-the-Middle**

Most commonly MITM attacks occur on free Wi-Fi hotspots where an attacker sets up a malicious Wi-Fi without password requirements and tracks all traffic passing through that network. (Incapsula, 2016) If the network is suitably named for its surroundings, such as "Airport Free Wi-Fi" at an airport or "Restaurant X Wi-Fi" at restaurant x people will frequently trust the network.

When an attacker gains access to the network connection between the two communicating end appliances they can see and adjust all information flowing through the connection. This isn't an issue if all the target wants to do is browse an online forum without logging in, but in case the target decides to use this unsecured connection to connect to their online bank the attacker can find out personal information or even hijack the session for personal benefit.

### 3.4.5 Backdoors

In the terms of computer science backdoors stand for unauthorized access into a device or system. The backdoor is a method that lets a user or attacker, regardless whether they have malicious intent or not, to bypass the authentication process.

A backdoor can be its own program, a part of other software or even a hardware feature. They are commonly used during development for easier access.

Backdoors can be as simple as a remote control program installed on a computer without the system owner's knowledge or permission. This program can then be used to access the computer's screen at any time, or to spy on the system user.

### 3.4.6 Denial of Service

The denial of service attack is one where the goal is to temporarily or permanently impede a service. Any device connected to the internet without appropriate protection in the form of firewalls or intrusion detection systems can be affected by a DoS attack. Typically, a denial of service attack is conducted by flooding the victim system or network with illegitimate requests such as ICMP echo requests or ACK-requests. These requests cause the system to overload and prevent the legitimate requests from getting through.

Successfully overloading a system usually causes it to either shut down or become incapable of processing genuine requests. If this happens the attack is successful.

A distributed denial of service is similar to a DoS attack in its purpose, but differs by its methods. A DDoS uses more than one unique IP-address to conduct the attack – the number of IP-addresses in these attacks can be thousands.

A DDoS attack truly begins with an attacker spreading a program or malware in order to gain some level of control of bystander machines. These machines, usually computers, are then added to the attacker's botnet to be used simultaneously in a specified attack.

### 3.5 Covering tracks

Covering or clearing tracks is listed as the last step of the hacking cycle as it commonly includes wiping the security or auditing logs that are generated by the unauthorized access. This must always be done last, otherwise new actions may create more logs which the security administrator will be able to see upon checking the system.

Other approaches include the prevention of security logging and avoidance of detection systems during the attack. Preventing security logging from happening usually requires taking down the system in charge of logging certain security events, for example by conducting a denial-of-service attack.

#### 3.5.1 Intrusion Detection System

The purpose of an Intrusion Detection System, commonly known as IDS, is the monitoring and analyzing of security events in the system or network. (Oriyano, 2016) The IDS scans the network for security threats and violations and upon finding one it logs the information and sends an alert to the system owner, if configured to do so.

Intrusion detection systems can be divided into four subcategories. The first type is NIDS, which stands for Network Intrusion Detection System. These are the most common, and are designed to inspect all packets on the network. Upon finding malicious activity the NIDS sends out an alarm. HIDS is the second type, standing for Host-based Intrusion Detection System which, akin to its name, is concentrated on detecting activity on a single host or server. This type of IDS is very adept at detecting insider abuse. The third type are Log File Monitors or LFM's which probe through created log files and find malicious instances through pattern matching. Lastly there are file integrity-checking mechanisms, which search through files on a host or server and look for files which have been modified. (Oriyano, 2016)

A company must decide on an IDS which matches their need for observation and logging for the system. Different Intrusion Detection Systems offer different tools and methods for detecting and recording the attacks.

### 3.5.2 Intrusion Prevention System

The Intrusion Prevention System or IPS scans and analyses the network in a way similar to an IDS. The main difference between the two is the reaction to a found threat: IPS takes a more active stance and instead of only reporting it to the system owner it also reacts to the threat. Possible reactions include dropping the packets causing the alarm, blocking incoming traffic from the address sending threatening packets, and resetting the connection. (Networks, 2016)

### 3.5.3 Anti-Virus

Anti-Virus is a software used for detecting, preventing and removing malicious software. It is a common misconception that an anti-virus prevents all malicious activity, leading to vulnerabilities caused by a false sense of security. Instead of prevention this software usually warns the system owner about the presence of a potentially malicious file.

There are four main identification methods antivirus programs use: signature-based detection, heuristics, rootkit detection and real-time protection. The best defense an antivirus offers is a combination of these features.

Signature-based detection is a defense mechanism which relies on the research of the antivirus provider. In practice, all antivirus programs have signature libraries stored by the provider. The provider has researchers who analyze new files and suspected malware. Once the researchers have deemed a certain file or program as malware they extract a reasonably unique part of the algorithm or hash and add that to the provider's signature library. It is important to keep an antivirus software up to date in order for the program to update its signature library with the new research done.

From time to time new malicious programs emerge which have similar code patterns as other preexisting malware. This type of detection is referred to as heuristics, and it essentially comes down to pattern recognition. If the code pattern of a new suspect file or program is the same or similar enough to an existing signature in the signature library, it will be flagged as potentially dangerous. This is a supremely useful way of detection as many viruses mutate or are added to by other attackers, causing variants to appear. Having a more generic pattern to which potentially harmful programs are compared to speeds up the detection process of malicious programs.

The third main identification method is rootkit scanning. Many antivirus programs offer storage scanning which can find malicious activity including rootkits. Rootkits are programs which are designed to gain access to an area which it shouldn't have access to. Much of the time rootkits are made to gain administrator access and modify the system and settings without being detected. They are notoriously difficult to find and remove, often requiring extreme measures like a complete reinstallation. (Pfleeger, Lawrence, & Marguiles, 2015)

Real-time protection is the last main identification type provided by most antivirus software. It is a monitoring system which is constantly active in the background, checking all new input to the computer memory. This includes online browsing activity, opening e-mail attachments, connecting a hard drive or inserting a CD into the computer.

### 3.6 Malware

Malware, short for malicious software, includes all programs created with malicious intent. The target of malware can be to cause temporary or permanent harm, disrupt services, gain private information, gain access to accounts or systems, or spread unwanted advertisements. Depending on the target of the malware it can be anything from mildly annoying to supremely dangerous. Antivirus programs are used to protect users and systems from malicious software but it is important to remember that the software does not and cannot catch all malicious activity and the best defense is to be careful about which websites or people to trust.

#### 3.6.1 Viruses

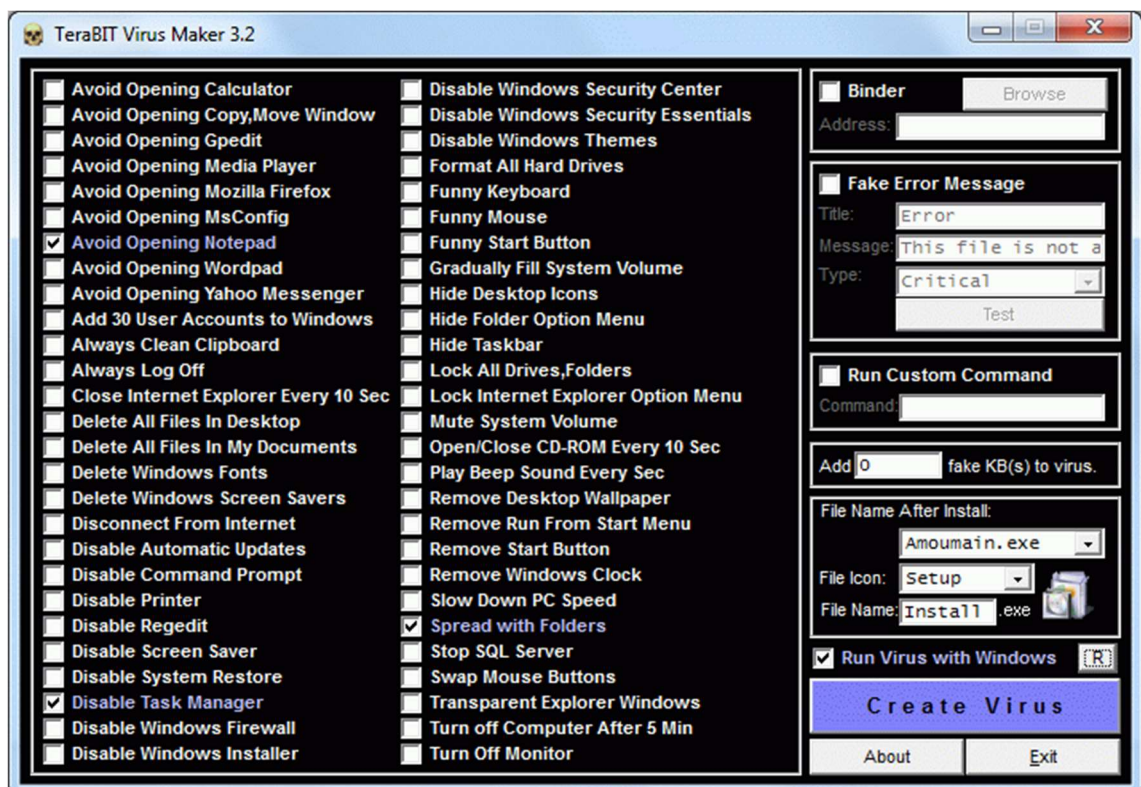
Viruses are made and spread by malicious individuals, are considered to be self-replicating and generally are attached to other programs. A virus has many possible actions listed by Oriyano (2016, Malware) as: altering data, infecting other programs, replicating, encrypting itself, transforming itself into another form, altering configuration settings, destroying data and corrupting or destroying hardware.

Viruses are the most commonly known malware and perhaps the most common type of it. They spread through means such as e-mail attachments and other downloadable files, unauthorized self-replication being the definitive part of the process. However, viruses



require some social engineering to be successful as they will not spread without user input. Chain e-mails with malicious attachments or URLs are the most common way of spreading a virus.

The objective of a virus can be to waste time, to spread misinformation, to gather private information or to cause disruption. Making a virus can be as easy as writing down a few lines of code or using a virus maker software. Pictured below is the TeraBIT Virus Maker 3.2 interface.



Picture 10: TeraBIT Virus Maker 3.2

In this virus maker, an attacker can simply tick the boxes of the effects wanted with the virus, name it and change the shown file icon. The malicious file will be created as soon as the attacker clicks on the “create virus” button. Software such as this has been causing an increase in younger, less knowledgeable hackers known as “Script Kiddies”, who use readymade programs created by others to cause harm.

### 3.6.2 Worms

Worms are computer programs which do not need user input in order to spread. They usually use the network to replicate itself on other machines.

Worms tend to not have a malicious executable payload within them. Their main objective is to spread as fast and as far as possible, and while this is not inherently malicious it does cause large issues with the consumption of bandwidth and resources.

Sometimes worms are constructed to have a malicious payload, for example a separate virus, within them. Once they have infected a new host they will release the payload and the virus begins to wreak havoc. This method is used if the attacker wants to spread a virus very fast and has enough resources to create both a worm and a virus.

### 3.6.3 Trojans and spyware

Trojans, also known as Trojan horses, are a phenomenon named after the myth where the Greeks built a large wooden horse and filled it with soldiers in order to infiltrate the city of Troy. Similarly, the way Trojan software works is: a malicious program takes the appearance of something harmless in order to mislead a user into saving or executing it on an end device. In the case of a user believing in the harmless appearance and giving access to the piece of malware, it can cause anything from security- or data loss to destruction, identity theft and spying.

Trojans are often used as a way to create a backdoor into a system, but each Trojan is different and can be programmed to do practically anything the attacker wants it to do. Once a backdoor is created the attacker has free access to the infected system and can continue gathering information or destroying content.

Spyware is a subset of malware often included in a Trojan or a virus. It stays on the infected computer and sends information, such as keystrokes, back to the attacker. Many antivirus programs offer scans or real-time scanning to decrease the likelihood of a computer having any type of malware, but they are not always successful and the best way to protect a computer from infection is to study basic social engineering and be careful with executable files.

## 3.7 Social Engineering

Social engineering consists of non-technical attacks used to abuse human gullibility and desire to be helpful. It is often overlooked as an attack in technical surroundings, but no amount of hardened network or written code will hold back an attacker who can trick a personnel member to give them the system password or otherwise pass through the security measures.

Social engineering is adaptable and can be used as an umbrella term to include everything where a human being is the weakest link granting the attacker access to the system. There are many subsections to it, the most common ones being phishing, vishing, tailgating and baiting.

### 3.7.1 Phishing

Phishing divides into basic phishing and a more concentrated form called spear-phishing. Phishing is the act of conducting an unspecified attack, typically an e-mail, sent to a large audience of people hoping for a few of the recipients to react to it so the scam may continue. Spear-phishing is a more concentrated effort where the attack is tailored to seem legitimate to a single victim or a specific group of people, for example the CEO or a certain department of a company.

Phishing e-mails attempt to find out the authentication details or private information of a user by presenting misinformation or masquerading as a legitimate preexisting service. E-mails phishing for authentication details can provide a link to a false site the user has a high chance of using, such as Facebook, PayPal, Amazon or a banking company. The message will usually also pressure the user to act quickly claiming the account will be closed unless the password is changed within 48 hours of receiving the message, or other such time-sensitive consequence.

### 3.7.2 Vishing

Vishing is a scam conducted over a phone connection. It is the reason many companies now require logging in with account details before providing individualized support on the

phone. It can be used to gain more information about the victim to use in other services, or to gain access to the victims account.

An attacker can spoof their phone number so it appears to be coming from the contract owner, which lends legitimacy to the call. Pretending to be the owner or their spouse who has forgotten the account credentials and absolutely needs the matter done today puts pressure on the customer service representative or other target of the call. Combining this with the correct vocal patterns and situational embellishments can make the target very receptive and inclined to help.

Vishing depends intensely on human error and the only way to reduce its effectiveness is to educate the staff and enforce caller identification and authentication.

### 3.7.3 Tailgating

The act of tailgating, also known as piggybacking, takes advantage of basic human courtesy. Tailgating is when an unauthorized person gains access to private property through locked doors, areas requiring a PIN-code to enter, or other similar security measures.

Methods used for tailgating include three main techniques

- Following an authorized individual through a security point, attempting to appear as their companion
- Hiding in a larger crowd of authorized personnel while pretending to be a part of it
- Tricking or bribing someone with possibly questionable morals into granting access

Tailgating can be discouraged and diminished through increased security measures. Live security personnel, keycards or swipe cards and mantraps all improve physical access security.

### 3.7.4 Social Media

The basis of any targeted social engineering attack is having enough information about the target or the victim. A common way of attacking is pretending to be a legitimate user and finding out possible information about them beforehand. Social media without proper security settings is a particularly weak spot when it comes to this.

Many different social media platforms such as Facebook, Twitter, Instagram, Foursquare and LinkedIn may have important information set to public view, which can easily be misused by an attacker. Unless the security settings are correctly configured they can be a fountain of private information: anything from where a user works to what is the name of their pet can be useful. The former information can be used when trying to impersonate the victim and the latter, or details similar to it, can be used to guess security questions in other services.

### 3.7.5 Counteracting Social Engineering

The prevention of social engineering comes down to educating individuals and requiring the personnel to follow safety protocols. Most successful social engineering attacks come down to ignorance or a flippant attitude towards safety rules. Once the personnel are educated in basic strategies which might be used against them, they will find it easier to respond to said strategies appropriately and according to policy.

Many companies periodically hold conferences or presentations on newest forms of security risks. These should always include social attacks and ways in which malicious individuals may attempt to exploit the systems in place.

## 3.8 Mobile Security

The main security issues with mobile devices are their small size and their lack of encryption. Small devices are easy to steal or plant without notice, which can cause data loss, integrity issues or the spreading of malware. Placing an unsecured mobile phone, external drive or a USB drive in a pocket or a bag and walking out without anyone being aware of it is often not particularly difficult.

Encryption is a large issue that has been tackled more commonly in the recent years. A decade ago mobile phones or external drives were rarely encrypted at all, making stealing small devices an effective method of information gathering. According to a 2008 survey conducted by Robert Richardson only 53% of the companies questioned encrypted their stored data. (Richardson, 2008)

Today this number is much higher, and as security issues become more common so do the methods used to minimize them. Phone companies offer encryption possibilities and companies often encrypt devices before allowing personnel to use them. Android, for example, offers full-disk encryption for versions 5.0 and newer, and file-based description from version 7.0 onwards. (Android Encryption, 2016)

### 3.8.1 Mobile Devices

The definition of mobile devices can include all small handheld devices such as phones, tablets, cameras, memory devices like USBs and hard drives, pagers, smartwatches and calculators. Stealing or planting any of these causes a loss of confidentiality, especially in the case of improper encryption or other security measures.

Most common security risk caused by mobile devices are company owned work phones given to employees. This practise is common, the mobile phones are taken out of the workplace surroundings constantly, and they also often contain e-mail access, contact information, saved files and folders or even pictures or recordings related to the work environment.

Another large security risk are USB devices. They are used to store or move information in an easy manner, causing a threat of theft or losing the device, both of which are a risk when it comes to confidential information. To combat this, confidential files should only be moved with secure means according to the company policy and small memory devices should be discouraged.

### 3.8.2 Cloud Services

The cloud services have different offered service models: Software as a Service, Platform as a Service and Infrastructure as a Service, respectively also known as SaaS,

PaaS and IaaS. All three of these also offer different types of deployment models, making it important to understand that the cloud computing system is very varied. The main security concerns, however, remain the same. The main concern for many companies choosing cloud services is the loss of physical access to the servers storing important information. This lessens the influence the company itself has with the employees who have access to the server information and thus increases the risk of insider attacks.

The cloud service provider must screen its employees carefully in order to decrease the possibility of malicious individuals gaining access to information. It also must be able to ensure complete data isolation in order to provide integrity and confidentiality to its customers.

In addition to the security issues with data storage, cloud services also include moving data over networks. This requires a certain level of network security and file transfer encryption. The responsibility of this falls both on the service user and the service provider. The user must choose to only trust reliable and trustworthy networks and use sufficiently secure password and username credentials. The service provider must guarantee service encryption and server-end security for the stored information.

### 3.8.3 Bluetooth

Bluetooth is, at best, an unsecure channel for file transfer and at worst a constant security risk. Bluetooth offers levels of security options to combat these issues, including a safe mode where only trusted devices can connect with it. Trusted devices, in this case, are ones which the device has previously connected with. This system has been perceived as adequate security by Bluetooth designers, but it has several glaring security issues. First, this pairing system leaves the Bluetooth protocols L2CAP and SDP exposed. In addition to this the four-digit passcode used for security verification is easy to break as it is very short, and some devices often have a hardcoded code of 0000. (Mäkilä; Taimisto; & Vuontisjärvi, 2011)

Common attacks through Bluetooth include Bluejacking, Bluesnarfing and Bluebugging. Bluejacking is reasonably harmless, as its main feature is automatically sending text messages to all Bluetooth connected devices within 10 meters and adding the message sender's contact information to the target address book. Bluesnarfing is an attack where the target phone's privacy is invaded. The attacker can access private information on the

phone such as text messages, the calendar, contacts and e-mail through Bluetooth. Bluebugging is the most dangerous of the three attacks. It creates a short connection over Bluetooth and creates a backdoor on to the target device. The attacker is then able to access the phone at any time without the owner's information and listen in to calls.

The basic level of Bluetooth security, however, is very easy: simply turning off the Bluetooth option when it is not in use guarantees there is little to no undetected misuse.

### 3.9 SQL Injections

SQL stands for Standard Query Language, and is used to create, view, modify and delete databases and the information stored in them. Most moderately sized companies use databases in some form, which opens them to exploits if the code and systems used are not adequately hardened.

SQL injections are a type of attack exploiting the quirks of the SQL language and its commands. Generally, SQL injections do not exploit the databases themselves, but instead find the erroneous designs of web applications or websites. Most often the reason the injection attacks are successful is absent input validation, meaning the input area has been programmed or configured so as to let through input without verifying it is in correct form.

SQL injections work in situations where a user is supposed to input information to fields from which the info is moved to an existing database, but instead of valid information the user input is one of certain commands the database will respond to. This will cause the database to release confidential information out to the user. These attacks can be used to view, change or delete information in the databases, making it a large risk. Other uses can be using SQL injections to alter database information by escalating user privileges or changing authentication information and altering transaction information, if such is found in the system.

Preventing SQL injections can be done through whitelists and blacklists: registers of characters and commands which are and are not allowed in specific fields. Another way to prevent the injections in most cases is to completely disallow scripts in input fields.



### 3.10 Physical Security

Physical security is an occasionally overlooked aspect, especially in smaller companies. Without an inclusive company policy, unauthorized employees may be able to access resources they should not have access to. Physical security starts from requiring the use of screensavers and lock screens while away from a computer and displaying proper warnings for unauthorised use and ends in properly sanitizing used devices which may still hold confidential information.

#### 3.10.1 Access Restrictions

Access restrictions can include introducing locked doors, key card use, fences, gates and mantraps to an otherwise already closed location. Depending on the safety requirements different extent of physical security is advised. A site hosting low-level employees obviously does not require a three-layer biometrics security check whenever accessed. Making security unnecessarily complicated may encourage employees to disregard company policy, leave doors open or share credentials.

Biometrics are security measures based on unique biological or physical features like fingerprints, retina scans or voice recognition.

Mantraps are used to discourage tailgating. They are a system where only one individual may enter into a closed enclosure at a time, from which the individual must move forward by showing authorization.

A common but relatively expensive access restriction possibility is employing security professionals to control access to certain areas. This, however, leaves room for human error so it is encouraged to be used in combination with other authorization methods.

#### 3.10.2 Server Room Security and Maintenance

In most situations in any moderately sized company the server room contains the largest amount of confidential information. It is absolutely imperative to keep this information

within the CIA triad including confidentiality, integrity and availability. This includes locking the doors and requiring access authorization in the form of keys, key cards or passcode knowledge.

Another form of keeping a server room available is to maintain the room and its requirements. A larger server centre especially has needs when it comes to temperature, humidity and air pressure. A server room is recommended to be kept at the temperature of 20-24 degrees Celsius, and between 45-55% humidity. (Grundy, 2005) Slight variance in both are acceptable but the more either of these stray from the optimal the less reliable the servers become. Air pressure is recommended to be kept slightly positive in order to keep dust, dirt and smoke out of the room. Cameras and cable and rack security are also recommended for additional control.

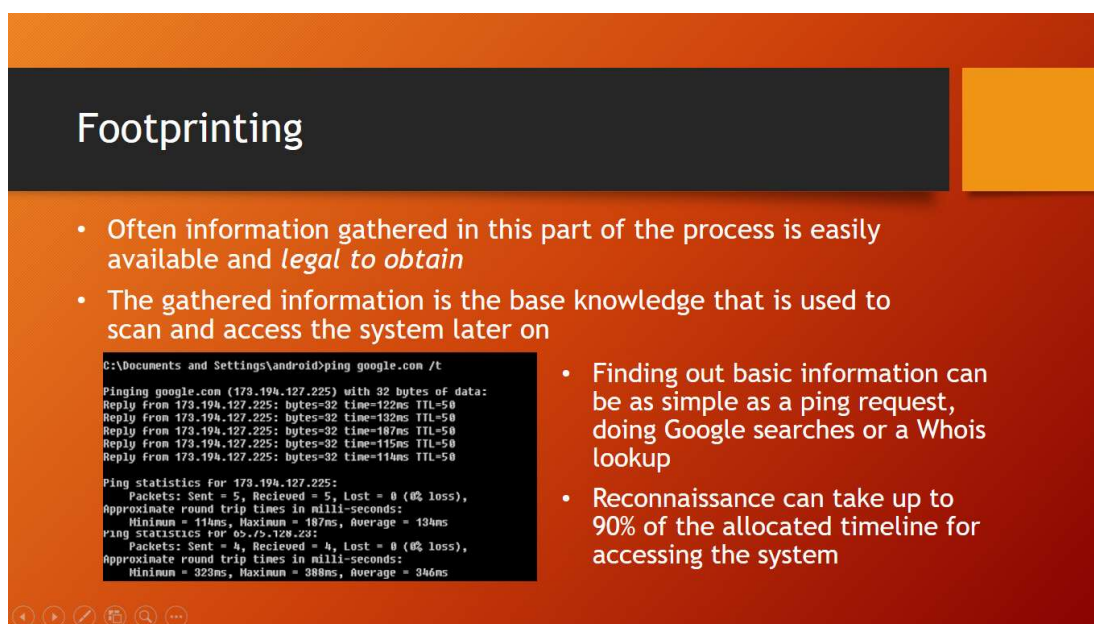
## 4 Ethical Hacking Course Compilation

The main objectives of this thesis were to research penetration testing and to create an online course based on this research. The course consists of ten PowerPoint lectures on the theory of ethical hacking, and uses the Netlab+-system to provide practical tasks supporting each chapter.

The ten chapters of the course are:

1. Introduction and Reconnaissance
2. Social Engineering
3. Scanning and Information Gathering
4. Enumeration and Security
5. Accessing the Network
6. Infecting the Network
7. Avoiding Detection and Anti-Virus
8. SQL Basics and SQL Injections
9. Mobile Device Security
10. Physical Access Security

Each of the chapters consists of 14-18 pages and has a list of relevant Netlab+ exercises and other potential information sources on the last page of the presentation. Picture 11 portrays how the PowerPoint chapters generally look like.



### Footprinting

- Often information gathered in this part of the process is easily available and *legal to obtain*
- The gathered information is the base knowledge that is used to scan and access the system later on

```

C:\Documents and Settings\android>ping google.com /t

Pinging google.com [173.194.127.225] with 32 bytes of data:
Reply from 173.194.127.225: bytes=32 time=122ms TTL=50
Reply from 173.194.127.225: bytes=32 time=132ms TTL=50
Reply from 173.194.127.225: bytes=32 time=187ms TTL=50
Reply from 173.194.127.225: bytes=32 time=115ms TTL=50
Reply from 173.194.127.225: bytes=32 time=114ms TTL=50

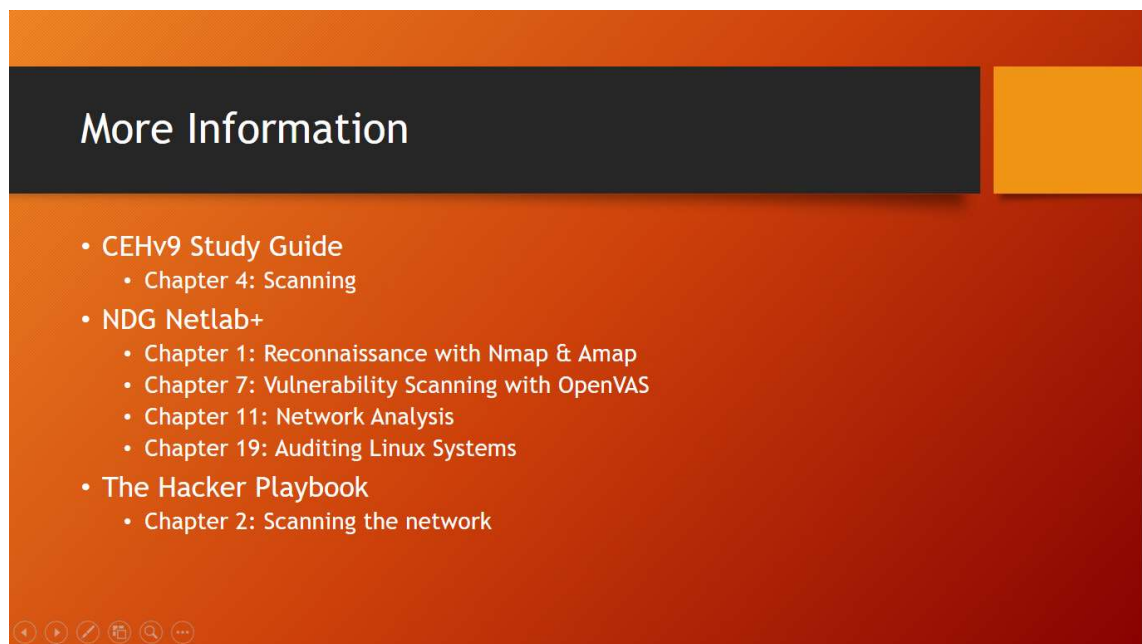
Ping statistics for 173.194.127.225:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 114ms, Maximum = 187ms, Average = 134ms
Ping statistics for 62.75.129.221:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 323ms, Maximum = 388ms, Average = 346ms
  
```

- Finding out basic information can be as simple as a ping request, doing Google searches or a Whois lookup
- Reconnaissance can take up to 90% of the allocated timeline for accessing the system

### Picture 11: Ethical Hacking Course Chapter 1

The PPT slides introduce the user to ethical hacking through a step-by-step process, where each chapter elaborates on a single step.

At the end of each chapter there is a “More Information” page which lists out the related Netlab+ chapters along with other possible resources for more information. Picture 12 shows the outlook of this last page.



Picture 12: Relevant Netlab+

The course is planned in such a manner that the best order to work through the material is to first read through the PowerPoint presentation, then see which Netlab+ chapters are relevant to the content. Before going to the actual practical labs, the user should read the two-page introductions for each practical exercise which include the following:

- Information on which step of the hacking cycle this practical falls under
- A one-sentence synopsis on what this step consists of
- Which programs are used in this practical exercise
- What are the programs generally used for


Picture 13 shows part of the first page of the introduction for chapter 1.

Introduction to the Netlab+ practical exercise. The practical contains a step-by-step instruction manual for what you must do which you can see by clicking [Show Lab Content](#) within the exercise.

Reconnaissance is the first of five steps of the hacking process.

Reconnaissance is either active, meaning you interact with the system, or passive, meaning gathering information by other means such as Google, Whois and social media. Passive recon is safer but does not always yield enough information.

Nmap and Amap are a more active take on footprinting, where you can send packets and scan the targets ports.



```

graph TD
    Reconnaissance --> Scanning
    Scanning --> Gaining Access
    Gaining Access --> Maintaining Access
    Maintaining Access --> Covering Tracks
    Covering Tracks --> Reconnaissance
  
```

Picture 13: Netlab chapter 1 introduction

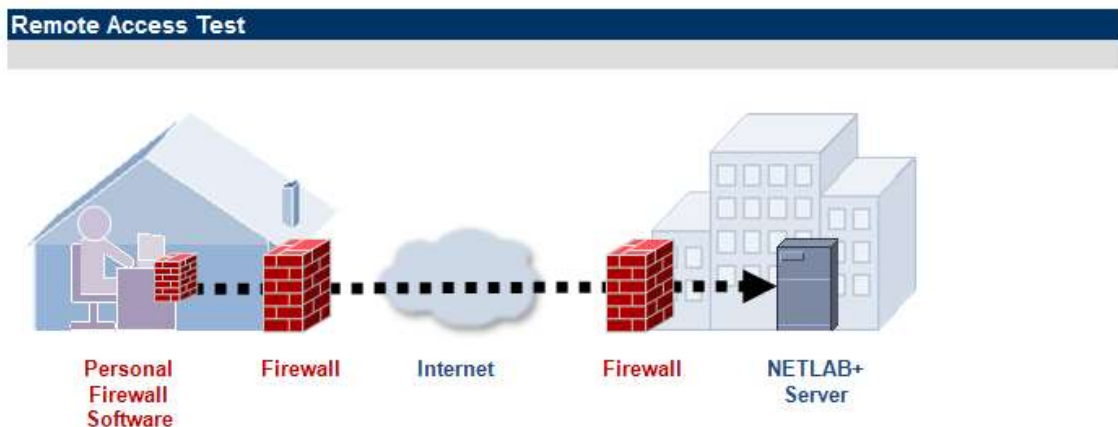
The order of reading the PowerPoint chapters first, introductions second and only doing the practical exercises after both of these is the most beneficial, as the first two give background knowledge on the ethical hacking step currently being taken and allow the user to apply this content while doing the practical exercises.

## 5 Netlab+ Learning Environment

### 5.1 Requirements

The Netlab+ practical learning environment requires access to a browser, Java, JavaScript, cookies, popup windows and IFRAMES. It supports Mozilla Firefox, Internet Explorer, Google Chrome and Apple Safari and warns that personal firewall software may interfere with the application.

In order to access the browser connection, the user must navigate to netlabpro.metropolia.fi and have an account assigned to them by an instructor or a system administrator. After a successful login, the system will prompt the user to begin a remote access test to make sure the connection to the Netlab+ server is possible.



NETLAB+ will now conduct a Remote Access Test to determine if Java is working properly and to ensure your computer can connect to the NETLAB+ server without firewall interference.

After clicking Start below, you may be prompted with security confirmation questions by your browser, by Java, and your personal firewall software.

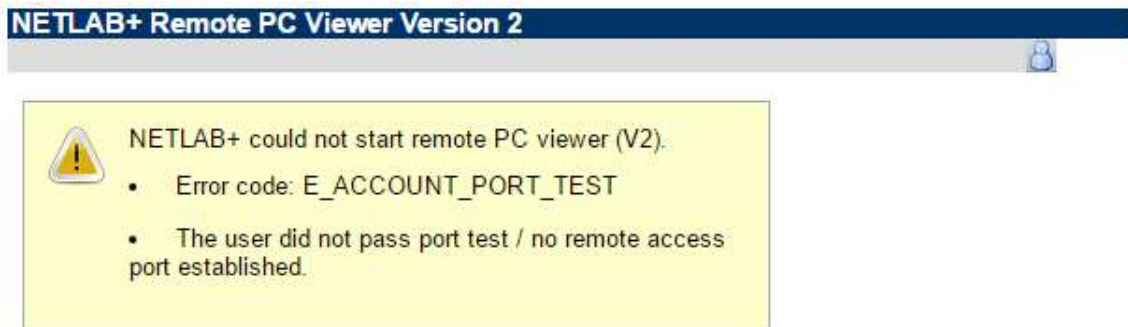
**Please allow the Remote Access Test to download, to run, and let connections proceed.**

You may be offered options to "always allow" or "always trust" for this NETLAB+ site. These options may eliminate the need to answer the same security questions each time you login into this NETLAB+ server in the future.



Picture 14: Netlab remote access test

By clicking “Start Remote Access Test”, as shown in Picture 14, the user must save a file on their computer which is used to test the connection to the Netlab server. If the test is successful, the user is able to access all the resources on the page. Skipping the test is possible but not recommended, as it usually makes it impossible to access the remote computers in the practical content giving the error shown in Picture 15.



**Picture 15: Remote PC Viewer Error**

This error can be fixed by logging out and back in to the website and completing the remote access test, which will establish a remote access port for the connection.

Once a remote connection has successfully been initiated the user must navigate to “Scheduler” seen in the Picture 16.

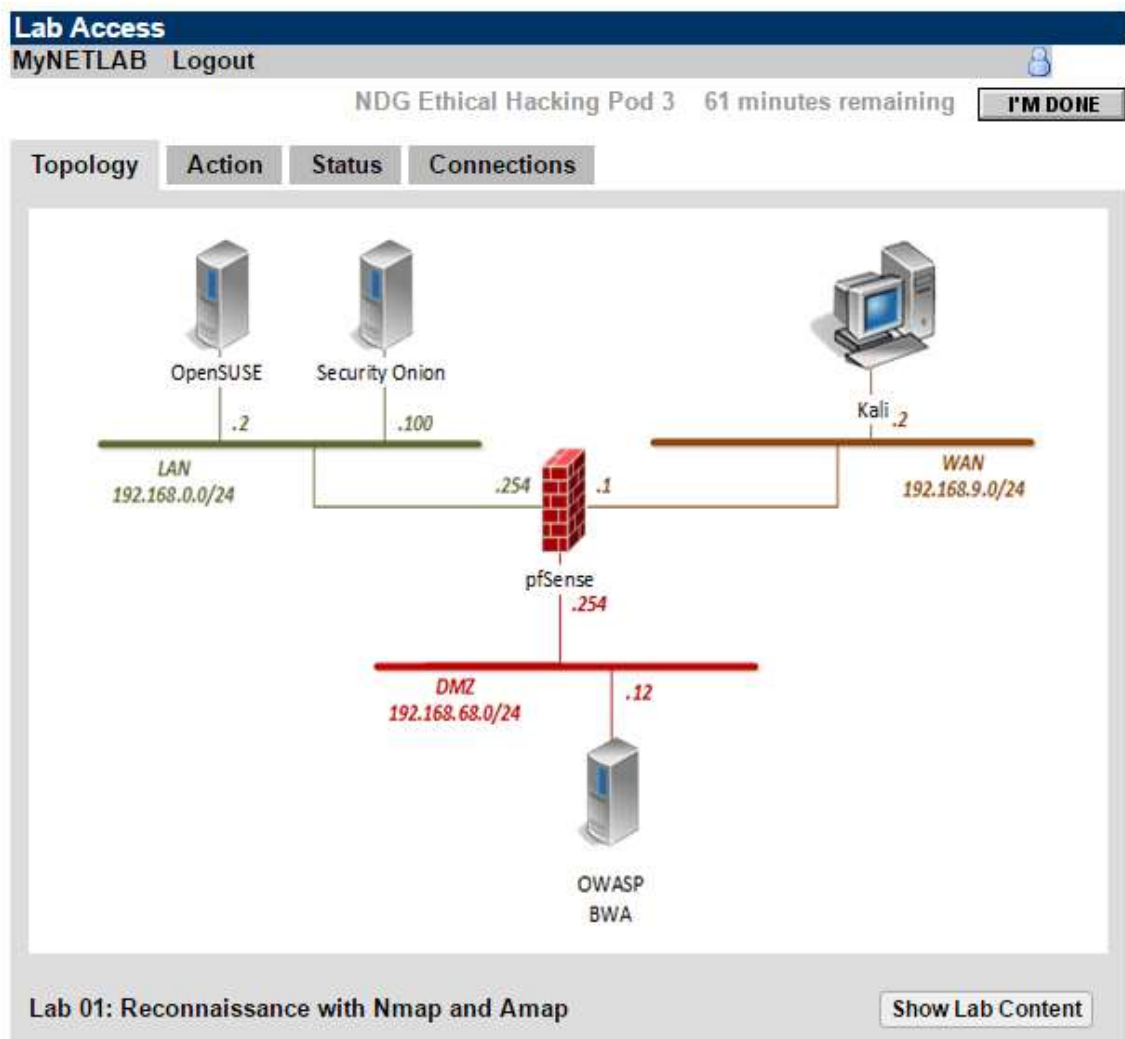


**Picture 16: Netlab options**

Within the scheduler all the courses the user has been added to by the administrator are listed. The user must choose the correct course and then reserve a timeslot for a specific lab. Only one lab can be reserved at a time and the reservation must be between thirty minutes and four hours long. It is good to note that the last 10 minutes of each lab time will be used to save the lab progress and prepare the lab for the next reserved timeslot.

## 5.2 Course content

The Netlab+ Ethical Hacking course is divided into twenty chapters. Each chapter has a content guide accessible by clicking the [Show Lab Content](#) button. This content is a step-by-step guide for the actions necessary to each practical, complete with the authorization information for the machines in the practical lab exercise. Picture 17 is the topology page of the practical labs.



Picture 17: Netlab topology page

On this page the user can access all virtual machines included in the practical exercises by double-clicking on them. This is the centerpiece and starting point of all labs and while each exercise uses different components of the system, the Kali machine is used in every practical exercise.



## 5.3 Software in Practicals

The programs used in the practical environments are varied. Different programs are necessary in different steps of the hacking process and several of the used programs have been mentioned in chapter three of this thesis – the phases of penetration testing.

### 5.3.1 Operating Systems

The operating system used in all of the exercises is Kali Linux. Kali is a Linux distribution targeted for penetration testers. It has many of the commonly used penetration testing tools installed and ready for use. Kali Linux is installed on the Kali-virtual machine on the lab environment.

Other operating systems in the practical exercises are Security Onion, OpenSUSE and a virtual machine running OWASP Broken Applications Project. All of these machines have applications or software which has intentionally been left unsecure in order to find the security issues with the software running on Kali Linux.

### 5.3.2 Software

The software used in the Netlab+ course practical exercises varies depending on the chapter. All chapter titles are included in this thesis as an appendix. In thirteen out of twenty chapters the software used in the chapter is apparent in the title or objective listed in the NDG Ethical Hacking Supported Labs list.

Much of the software used is open source resources which have been created for network security inspections and maintenance upkeep, and have a command or program component which can be misused while attempting to hack into a system. Almost every program used has a legitimate use for network defence, although a few of the programs are certainly borderline. An example of this are the password cracker programs: they can be used for legitimate issues where a user has forgotten an important password but in practice there are usually other ways to resolve such a situation.

## 5.4 Learning material

As a learning source the Netlab+ practical exercises are both diverse and concise. Each chapter takes a single approach towards a single issue and shows the user how the process of finding this exploit happens in practice.

The practical exercises cannot and should not be taken as a comprehensive list of what a penetration must or must not do. Ethical hacking is an extensive field with many possible ways of approaching vulnerabilities and while the labs give moderate insight into the practical aspect of exploiting vulnerabilities there are many angles which aren't shown.

## 5.5 Improvements

The Netlab+ practical course has many important details about penetration testing listed under its content pages. The issue with the course is that it seems to be aimed at students or other individuals who already have some experience or knowledge in the area. The course offers very little introduction to each chapter and tends to jump right in to executing certain commands to get specific output.

As a part of the content of this thesis introductory chapters were added to the Netlab+ chapters to specify which part of the hacking cycle each chapter belongs to. Other information in the written introductory chapters included an explanation of the hacking cycle step, what would conducting this step result in, which programs would be used and what those programs are generally used for. All this information was listed in order to make it clearer what the aim of each practical exercise was before typing down commands.

In my personal opinion, this helped with the course structure and made the practical exercises easier to understand, especially for someone with little to no previous experiences with the subject. Keeping this in mind, the direction of the practical exercises could still be improved by making them more interactive.

The current "lab content" files, which include very exact commands are easy to follow and well made, but all of them list out all the necessary commands and all the student

does is copy these and is then told to “observe what happens next”. This caused moderate confusion for myself in the beginning as the previous online courses with practical content I have taken all had a more generic approach: instead of “Write the following command.” the instructions would ask to “Configure the program to give the following result.” Both ways are legitimate but having the practical exercises consist only of copying down preplanned commands requires more self-study.

Picture 18 is an example of the Netlab+ instructions from chapter 2.

2. Navigate to the `/var/www/html` directory by typing the command below. Press **Enter**.

```
cd /var/www/html
```

3. List the current files in the directory.

```
ls -l
```

4. Edit the `post.php` file by typing the command below. Press **Enter**.

```
nano post.php
```

5. Using the arrow keys, move the cursor towards the end of the line. In the nano editor, change the return URL from `url=http://www.google.com` to `url=http:192.168.9.2`.

```
GNU nano 2.2.6 File: post.php  
$" content="0; url=http:192.168.9.2" />|
```

**Picture 18: Lab content for Chapter 2**

This picture shows how the chapter guides are: they are well made and easy to follow, especially with the large amount of visual aids in the form of screenshots, but there is no true student input. All steps taken in each chapter include copying a readily written command in the previously screenshotted software.

## 6 Conclusion

Cybersecurity is an increasing issue in modern technology. The transparency of information available on the subject can be seen both as a threat and an opportunity.

Penetration testing is a versatile tool for finding weaknesses in a system, as it uses the exact same methods a true attacker would. Finding these weaknesses is not enough on its own, the imperative step of the process is to harden the system appropriately. An important part of the system hardening process is having a professional and knowledgeable ethical hacker conduct the testing. The results are only as good as the researcher and being unaware of a threat leaves the system vulnerable for it.

Tools and methods used for ethical hacking are the same which malicious attackers use. There is a plethora of information and software for penetration testing, many of which were introduced in this thesis.

Penetration testing is a very all-encompassing element of information technology. A system's vulnerabilities can be anywhere: in the software, hardware, the written code or system development. Because of this it is a very educational topic when it comes to security – even someone concentrating on a very specific subsection of IT must be aware of the other components the security consists of.

Taking this into consideration I am of the opinion that studying penetration testing is, and has been, supremely educational both in terms of technological knowledge and general awareness.

## Image Sources

Picture 1: <http://www.softwaretestingstudio.com/testing-approach-method/white-box-black-box-testing>

Picture 2: <https://www.checkmarx.com/wp-content/uploads/2016/06/Data-Security.png>

Picture 3: <http://www.slideshare.net/akhileshbhura/ce-hv6-module-01-introduction-to-ethical-hacking-14896452> page 15

Picture 4: [https://www.blackhat.com/presentations/bh-europe-05/BH\\_EU\\_05-Long.pdf](https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf)

Picture 5: Screenshot of using Nmap in the Netlab+ environment

Picture 6: <http://www.bestshareware.net/download/img4/10-strike-lanstate-pro-big.jpg>

Picture 7: <https://www.teamsid.com/worst-passwords-2015/>

Picture 8: Screenshot of using John the Ripper in the Netlab+ environment.

Picture 9: <http://web.cs.ucla.edu/classes/winter13/cs111/scribe/17b/>

Picture 10: <http://vxheaven.org/vx.php?id=tt10>

Picture 11: Screenshot of chapter 1 – Footprinting, page 7.

Picture 12: Screenshot of chapter 3 – Scanning and Information Gathering page 16

Picture 13: Screenshot of Netlab+ chapter introduction for chapter 1.

Picture 14: <http://netlabpro.metropolia.fi/aptest.cgi>

Pictures 15-18: <http://netlabpro.metropolia.fi/>

## References

- Android Encryption.* (2016). Retrieved from <https://source.android.com/security/encryption/>
- Grundy, R. (2005). *Avtech.* Retrieved from <http://avtech.com/articles/3647/recommended-data-center-temperature-humidity/>
- Incapsula. (2016). *Incapsula.* Retrieved from <https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html>
- Lucas, I. (2009). *Password Recovery Speeds.* Retrieved from <http://www.lockdown.co.uk/?pg=combi&s=articles>
- Mäkilä, T., Taimisto, J., & Vuontisjärvi, M. (2011). *Fuzzing Bluetooth.* Retrieved from [http://fte.com/docs/Frontline\\_wp\\_Fuzzing\\_Bluetooth\\_20110919.pdf](http://fte.com/docs/Frontline_wp_Fuzzing_Bluetooth_20110919.pdf)
- Networks, P. A. (2016). *Intrusion Prevention and Detection Systems.* Retrieved from <https://www.paloaltonetworks.com/documentation/glossary/what-is-an-intrusion-prevention-system-ips>
- Oriyano, S.-P. (2016). *Certified Ethical Hacker Version 9 Study Guide.* Indiana: John Wiley & Sons.
- Pfleeger, C. P., Lawrence, P. S., & Marguiles, J. (2015). *Security in Computing Fifth Edition.* Massachusetts: Pearson Education Inc.
- Richardson, R. (2008). *CSI Computer Crime & Security Survey.* Retrieved from <http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>
- Software Testing Fundamentals.* (2016). Retrieved from <http://softwaretestingfundamentals.com/white-box-testing/>

## Netlab+ Ethical Hacking Supported Labs

Lab	Title	Certified Ethical Hacking (CEH) Domains	Offensive Security (PWK) Objectives	SANS GPEN Objectives
1	Reconnaissance with Nmap & Amap	<ul style="list-style-type: none"> <li>• 2: Footprinting and Reconnaissance</li> <li>• 3: Scanning Networks</li> </ul>	<ul style="list-style-type: none"> <li>• 3: The Essential Tools (netcat, ncat, wireshark, tcpdump)</li> <li>• 6: Trojans and Backdoors</li> </ul>	<ul style="list-style-type: none"> <li>• 7: Intel Target Scanning</li> <li>• 15: Scanning for Targets</li> </ul>
2	Social Engineering Attacks with Social Engineering Toolkit	<ul style="list-style-type: none"> <li>• 9: Social Engineering</li> </ul>		<ul style="list-style-type: none"> <li>• 14: Reconnaissance</li> </ul>
3	Metasploit Framework Fundamentals	<ul style="list-style-type: none"> <li>• 5: System Hacking</li> </ul>	<ul style="list-style-type: none"> <li>• 17: Metasploit Framework</li> </ul>	<ul style="list-style-type: none"> <li>• 8: Metasploit</li> </ul>
4	Web Pentesting with Nikto & OWASP Zap	<ul style="list-style-type: none"> <li>• 12: Hacking Webservers</li> <li>• 13: Hacking Web Applications</li> </ul>	<ul style="list-style-type: none"> <li>• 14: Web Application Attacks</li> </ul>	<ul style="list-style-type: none"> <li>• 6: General Web Application Probing</li> </ul>
5	Password Cracking with John the Ripper and Hashcat	<ul style="list-style-type: none"> <li>• 5: System Hacking</li> <li>• 18: Cryptography</li> </ul>	<ul style="list-style-type: none"> <li>• 15: Password Attacks</li> </ul>	<ul style="list-style-type: none"> <li>• 1: Advanced Password Attacks</li> <li>• 2: Attacking Password Hashes</li> <li>• 10: Password Attacks</li> </ul>
6	Creating and Installing SSL Certificates	<ul style="list-style-type: none"> <li>• 18: Cryptography</li> </ul>		<ul style="list-style-type: none"> <li>• 18: Wireless Crypto and Client Attacks</li> </ul>

7	Vulnerability Scanning with OpenVAS	<ul style="list-style-type: none"> <li>• 3: Scanning Networks</li> </ul>		<ul style="list-style-type: none"> <li>• 16: Vulnerability Scanning</li> </ul>
8	Enumerating SMB with enum4linux	<ul style="list-style-type: none"> <li>• 4: Enumeration</li> </ul>	<ul style="list-style-type: none"> <li>• 12: Privilege Escalation</li> </ul>	<ul style="list-style-type: none"> <li>• 4: Enumerating Users</li> </ul>
9	Backdooring with Netcat	<ul style="list-style-type: none"> <li>• 5: System Hacking</li> </ul>		<ul style="list-style-type: none"> <li>• 9: Moving Files with Exploits</li> </ul>
10	Packet Crafting with Scapy			<ul style="list-style-type: none"> <li>• 5: Exploitation Fundamentals</li> </ul>
11	Network Analysis	<ul style="list-style-type: none"> <li>• 8: Sniffers</li> </ul>	<ul style="list-style-type: none"> <li>• 3: The Essential Tools (netcat, ncat, wireshark, tcpdump)</li> </ul>	
12	Client Side Exploitations	<ul style="list-style-type: none"> <li>• 13: Hacking Web Applications</li> </ul>	<ul style="list-style-type: none"> <li>• 13: Client Side Attacks</li> </ul>	<ul style="list-style-type: none"> <li>• 6: General Web Application Probing</li> </ul>

13	Testing Firewall Rules with Firewalking	<ul style="list-style-type: none"> <li>• 16: Evading IDS, Firewalls and Honeypots</li> </ul>		
14	Understanding SQL Commands & Injections	<ul style="list-style-type: none"> <li>• 14: SQL Injection</li> </ul>		<ul style="list-style-type: none"> <li>• 14: Reconnaissance</li> </ul>
15	Understanding Buffer Overflows	<ul style="list-style-type: none"> <li>• 17: Buffer Overflow</li> </ul>	<ul style="list-style-type: none"> <li>• 7: Buffer Overflows</li> </ul>	<ul style="list-style-type: none"> <li>• 5: Exploitation Fundamentals</li> </ul>



16	Evading IDS	<ul style="list-style-type: none"><li>• 16: Evading IDS, Firewalls and Honeyd</li></ul>		
17	Packet Crafting with Hping			<ul style="list-style-type: none"><li>• 5: Exploitation Fundamentals</li></ul>
18	VNC as a Backdoor	<ul style="list-style-type: none"><li>• 5: System Hacking</li></ul>		
19	Auditing Linux Systems			<ul style="list-style-type: none"><li>• 13: Pentesting via the Command Line</li></ul>
20	Anti-Virus Evasion	<ul style="list-style-type: none"><li>• 6: Trojans and Backdoors</li></ul>		