




## ASSIGNMENT 1

<b>Qualification</b>	<b>BTEC Level 5 HND Diploma in Computing</b>		
<b>Unit number and title</b>	Unit 5: Security		
<b>Submission date</b>	November 26, 2021	<b>Date Received 1st submission</b>	
<b>Re-submission Date</b>		<b>Date Received 2nd submission</b>	
<b>Student Name</b>	Quach Cong Tuan	<b>Student ID</b>	BHAF200014
<b>Class</b>	PBIT17101	<b>Assessor name</b>	Le Van Thuan
<b>Student declaration</b> I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		<b>Student's signature</b>	

### Grading grid

P1	P2	P3	P4	M1	M2	D1

☐ Summative Feedback:

☐ Resubmission Feedback:

Grade:

Assessor Signature:

Date:

Signature & Date:

## TABLE OF CONTENTS

INTRODUCTION .....	8
P1. IDENTIFY TYPES OF SECURITY RISKS TO ORGANIZATIONS. ....	9
THREATS .....	9
VULNERABILITY .....	9
RISKS .....	9
1. MALWARE .....	10
1.1. Virus .....	11
1.2. Worm .....	12
1.3. Spyware .....	13
1.4. Trojans .....	14
1.5. Ransomware .....	15
2. SOCIAL ENGINEERING ATTACKS .....	16
2.1. Baiting .....	17
2.2. Scareware .....	17
2.3. Pretexting .....	18
2.4. Phishing .....	19
2.5. Spear Phishing .....	20
3. WEB APPLICATION ATTACKS .....	21
3.1. XSS .....	21
3.2. SQL Injection .....	22
3.3. DoS .....	23
4. NETWORKING BASED ATTACKS .....	24
4.1. Sniffing .....	24
4.2. Spoofing .....	25
4.3. DDoS .....	26
Prevention Risk Organizations .....	30
Example of a business that has been attacked .....	31
P2. DESCRIBE ORGANIZATIONAL SECURITY PROCEDURES FOR NORTHSTAR. ....	33
1. Authentication .....	34
2. Anti-Virus .....	35
3. Cloudflare (Cloud Firewalls) .....	36
4. Ads Blocked and Pop-up Blocked .....	37
5. Employee training .....	38

<b>P3. IDENTIFY THE POTENTIAL IMPACT TO IT SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND IDS.....</b>	<b>39</b>
1. Firewall.....	39
1.1. The Benefit of the firewalls:.....	40
1.2. Firewall solution providers: .....	41
2. IDS.....	44
1. Function .....	44
2. There are two types of IDS in use: <i>NIDS</i> and <i>HIDS</i> :.....	44
3. Benefit of IDSs .....	44
4. Legal System .....	45
5. IDS implementation models .....	46
<b>P4. SHOW, USING AN EXAMPLE FOR EACH, HOW IMPLEMENTING A DMZ, STATIC IP AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY.....</b>	<b>49</b>
1. DMZ .....	49
2. IP .....	51
2.1. IP Address .....	51
2.2. Static IP Address .....	51
2.3. Dynamic IP Address .....	51
2.4. Static IP Address can improve network security.....	52
3. NAT .....	53
3.1. Static NAT (Post-Forwarding).....	54
3.2. Dynamic NAT (One-to-one).....	55
3.3. NAT Overload (PAT) .....	56
<b>M1. PROPOSE A METHOD TO ASSESS AND TREAT IT SECURITY RISKS.....</b>	<b>57</b>
Establish a risk management framework.....	57
Identify risks.....	58
Analyze risk .....	58
Evaluate risk .....	58
Select risk treatment option.....	58
<b>M2. DISCUSS THREE BENEFITS TO IMPLEMENT NETWORK MONITORING SYSTEMS WITH SUPPORTING REASONS. ....</b>	<b>59</b>
1. Benchmarking standard performance.....	60
2. Effectively allocating resources .....	60
3. Managing a changing IT environment .....	60
4. Identifying security threats.....	60

5. Deploying new technology and system upgrades successfully .....	60
SLIDE FOR TRAINING .....	63
CONCLUSIONS .....	82
REFERENCES .....	83

## TABLE OF FIGURES

Figure 1 Malware .....	10
Figure 2 Virus .....	11
Figure 3 Worm .....	12
Figure 4 Spyware.....	13
Figure 5 Trojans Horse .....	14
Figure 6 Ransomware .....	15
Figure 7 Scareware.....	17
Figure 8 Pretexting.....	18
Figure 9 Phishing.....	19
Figure 10 Report Phishing .....	19
Figure 11 Spear Phishing.....	20
Figure 12 XSS - Cross Site Scripting.....	21
Figure 13 Report XSS.....	21
Figure 14 SQL Injection .....	22
Figure 15 Report SQL Injection.....	22
Figure 16 DoS.....	23
Figure 17 Sniffing .....	24
Figure 18 Spoofing .....	25
Figure 19 HTTP Flood .....	27
Figure 20 SYN Flood .....	28
Figure 21 DNS Amplification.....	29
Figure 22 ChongLuaDao .....	30
Figure 23 BKAExample 1 .....	31
Figure 24 BKAExample 2 .....	32
Figure 25 BKAExample 3 .....	32
Figure 26 Authentication.....	34
Figure 27 Antivirus .....	35
Figure 28 Cloud Firewall.....	36
Figure 29 Ads Block .....	37
Figure 30 Training .....	38
Figure 31 Cyberoam .....	41
Figure 32 Cisco.....	42
Figure 33 Cloudflare.....	43
Figure 34 IDS-Model-1 .....	46
Figure 35 IDS-Model-2 .....	47
Figure 36 IDS-Model-3 .....	48
Figure 37 DMZ.....	49
Figure 38 DMZ Network Architecture .....	50
Figure 39 Static IP and DHCP .....	52
Figure 40 NAT-1 .....	54
Figure 41 NAT-2 .....	54
Figure 42 NAT-3 .....	55

Figure 43 NAT-4 .....	56
Figure 44 M1.....	57
Figure 45 Tool Network Monitoring .....	61
Figure 46 Wireshark.....	62
Figure 47 Slide.....	63
Figure 48 Slide 2.....	63
Figure 49 Slide 3.....	64
Figure 50 Slide P1.....	64
Figure 51 Slide P1.....	65
Figure 52 Slide P1 .....	65
Figure 53 Slide P1 Malware.....	66
Figure 54 Slide P1 Malware .....	66
Figure 55 Slide P1 SEA .....	67
Figure 56 Slide P1 SEA .....	67
Figure 57 Slide P1 WAA .....	68
Figure 58 Slide P1 WAA .....	68
Figure 59 Slide P1 SQL .....	69
Figure 60 Slide P1 DOS .....	69
Figure 61 Slide P1 NBA .....	70
Figure 62 Slide P1 NBA .....	70
Figure 63 Slide P1 NBA .....	71
Figure 64 Slide P1 NBA .....	71
Figure 65 Slide P1 Prevention.....	72
Figure 66 Slide P1 Example.....	72
Figure 67 Slide P2.....	73
Figure 68 Slide P2 Definition .....	73
Figure 69 Slide P2 -1.....	74
Figure 70 Slide P2 -2.....	74
Figure 71 Slide P2 -3.....	75
Figure 72 Slide P2 -4.....	75
Figure 73 Slide P3.....	76
Figure 74 Slide P3 Firewall .....	76
Figure 75 Slide P3 IDS.....	77
Figure 76 Slide P4.....	77
Figure 77 Slide P4 DMZ .....	78
Figure 78 Slide P4 Static IP .....	78
Figure 79 Slide P4.....	79
Figure 80 Slide P4 NAT .....	79
Figure 81 Slide P4 Static NAT.....	80
Figure 82 Slide P4 Dynamic NAT.....	80
Figure 83 Slide P4 NAT Overload .....	81

## INTRODUCTION

In this assignment, I was assigned as a Trainee Security Specialist and Head of Security at NorthStar Secure Company. I will have to design a presentation so that they can train new employees in tools and techniques that support research and defense against information security threats with the organization's protection activities business-critical data and devices.

In this assignment, I will present and provide a detailed report with a technical assessment of the identification of risks to the NorthStar company and its policies on security breaches. Next, I will describe organizational procedures that an organization can establish to reduce the business impact of a security breach. Then I will suggest a method that NorthStar Secure can use to manage these types of risks. Finally, I'll outline 3 benefits to NorthStar when implementing the right network monitoring system and cybersecurity investigations that identify problems with firewalls and incorrect VPN configurations that expose throughput. I have identified examples of different techniques that can be deployed to improve networks and investigate network reliability through analysis of positive and negative problems. I will provide a detailed report of the implementation along with technical notes and an objective assessment.



## **P1. IDENTIFY TYPES OF SECURITY RISKS TO ORGANIZATIONS.**

Information technology now plays a critical part in people's lives. Industry 4.0 is assisting the world's development day by day, and information and data security are becoming increasingly critical concerns. Hackers are constantly evolving their attack strategies and obtaining access to organizational systems. There are several forms of security threats that might disrupt an organization's operations. As a result, there is no way to be certain that a company is totally safe from cyber threats or attacks. I'll go over 14 different types of attacks that can pose a threat to an organization in more detail below. Vulnerabilities and cyber threats are sometimes confused. The keyword, according to the definitions, is "potential." The threat does not stem from a security flaw in the implementation or organization. Instead, it is anything that has the potential to compromise security. A vulnerability, on the other hand, is a real flaw that may be exploited. Regardless of any countermeasures, the threat always exists. Countermeasures, on the other hand, can be implemented to reduce the likelihood of it occurring.

### **THREATS**

Security Threat means any threat or connected series of threats to commit an intentional attack against a Computer System for the purpose of demanding money, securities or other tangible or intangible property of value from an Insured.

The terms threat, vulnerability and weakness are often used in cybersecurity. Understanding the difference between these terms is important. It allows organizations to correctly implement, document and assess their cybersecurity activities and controls. Here, we take a closer look at security threats.

### **VULNERABILITY**

A vulnerability is a recognized weakness in an asset (resource) that one or more attackers can exploit. To put it another way, it's a well-known flaw that permits an assault to succeed.

### **RISKS**

When a danger exploits a vulnerability, risk is defined as the possibility of loss or damage. Risk can also be calculated using the formula: Risk = Threat x Vulnerability.

## 1. MALWARE

Malware includes viruses, ransomware, and spyware, among other types of malicious software. Malware, or malicious software, is a sort of code developed by cybercriminals with the intent of causing significant data and system damage or gaining unauthorized network access. Malware is typically sent as a link or a file in an email, and it requires the user to click on the link or open the file for it to be executed.

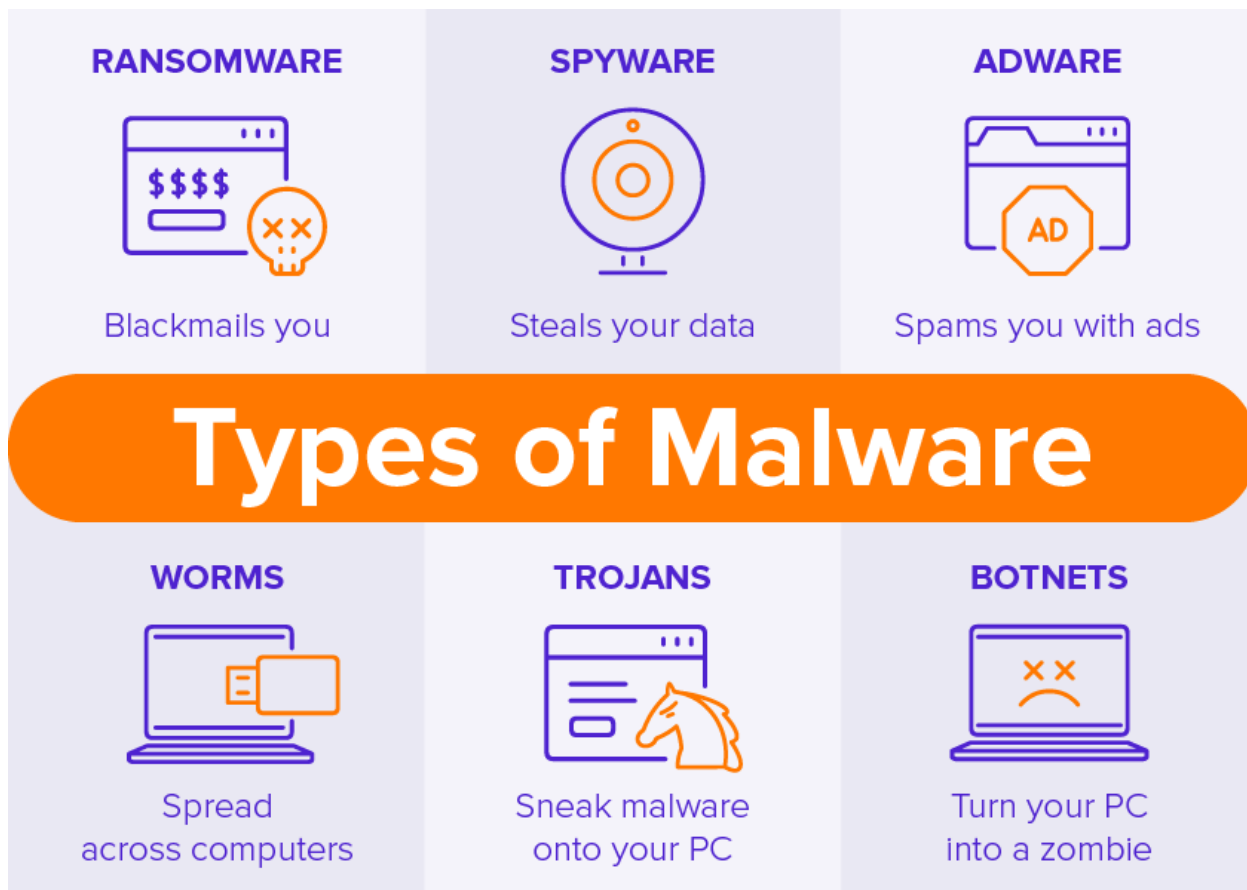


Figure 1 Malware

### 1.1. Virus

Viruses attach malicious code to clean code and wait for it to be executed by an unwary person or an automated process. They can spread quickly and rapidly, similar to a biological virus, disrupting system processes, corrupting files, and locking people out of their computers.



*Figure 2 Virus*

**Protection:** In order to protect our devices from Malware attacks, for viruses, we always update to the latest software versions, turn on manufacturer's security functions such as Windows Defense, or use programs Anti-Virus program by trusted organizations like McAfee, Avast, or at BKAV (A security company in Vietnam)

## 1.2. Worm

Worms get their moniker from how they infect computers. They work their way across the network, starting with one infected machine and connecting to other machines to spread the infection. This type of virus is capable of infecting large networks of devices with ease.

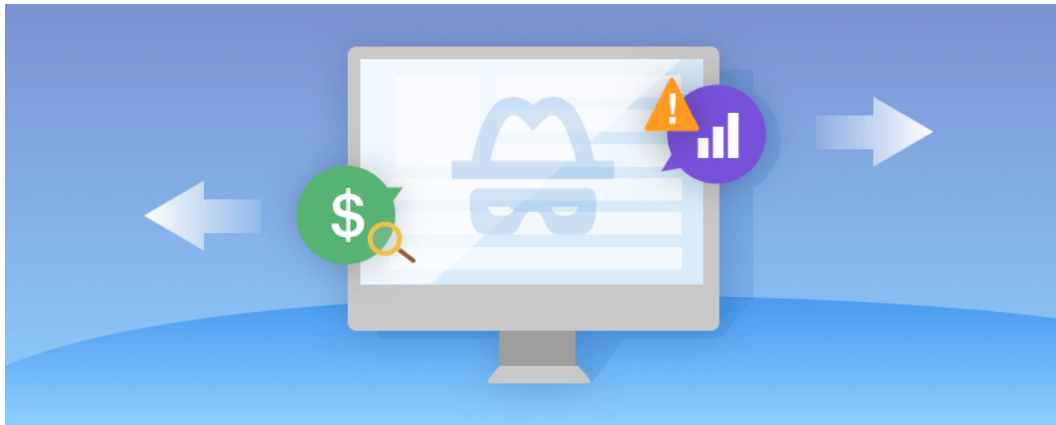


*Figure 3 Worm*

**Protection:** In order to protect our devices from Malware attacks, for worms, we do not click on attachments or links in emails or messages. If you download the file, please tick the Virus Total section to be checked, download more anti-virus software to block malware.

### 1.3. Spyware

Spyware is software that monitors a user's activity, as the term implies. This sort of malware operates in the background on a computer, gathering sensitive data such as credit card numbers, passwords, and other personal information without the user's knowledge.



*Figure 4 Spyware*

**Protection:** In order to protect our devices from Malware attacks, for Spyware we need to install anti-virus or Anti-Spyware applications. We need to regularly update the software in our device to the latest version. Use copyrighted programs. Do not use cracked versions.

## 1.4. Trojans

This type of malware hides within or disguises itself as legitimate software, much like Greek troops did when they attacked on a large horse. It will breach security discreetly by installing backdoors that provide simple access to other malware types.



*Figure 5 Trojans Horse*

**Protection:** In order to protect our devices from Malware attacks, for Trojan Horse effective way to avoid trojans is to never open any unknown files, links or software, or even emails from an address you know. The Trojan only spreads when you directly click on content containing spyware. It is best to check first with virus scanning programs or use **Virustotal** to check. Always use antivirus or firewall software to protect your computer. Fully update the vulnerability patches regularly with Windows computers, to prevent hackers from taking advantage of those vulnerabilities to infiltrate the computer.

### 1.5. Ransomware

The cost of ransomware, sometimes known as scareware, is enormous. Ransomware, which can shut down networks and lock people out unless a ransom is paid, has wreaked havoc on some of the world's most prominent organizations.



*Figure 6 Ransomware*

**Protection:** In order to protect our devices from Malware attacks, with Ransomware. Back up and continuously update your information to a file in the cloud or some database. Use security software and keep it open at all times. Do not use software, files with crack files. Please set the folder security mode on the device.

## 2. SOCIAL ENGINEERING ATTACKS

The term "Social Engineering" describes a range of nefarious activities carried out through human interactions. It manipulates users' brains in order to cause them to commit security errors or divulge sensitive information.

### **Protection:**

To ensure that we are not attacked by "Social Engineering" attack groups, we should take precautions and protect our personal information. Update necessary information about network security. Always confirm contact with relatives, avoid exchanging information/property with strangers. Avoid using multiple accounts with the same password. Limit posting personal information/identifications/schedules on social networking sites. It is recommended to use separate personal and work accounts. Do not provide information for emails/messages asking for financial/identity verification or providing personal information or passwords.



### 2.1. Baiting

Baiting attacks, as the term suggests, rely on a false promise to pique a victim's interest. They lure customers into a trap in which their personal information is stolen or their systems are infected with malware. Baiting schemes don't have to take place in real life all of the time. Baiting occurs online in the form of tempting advertisements that lure visitors to malicious websites or tempt them to download a malware-infected application.

### 2.2. Scareware

Scareware victims are bombarded with false warnings and threats. Users are led to believe their system is afflicted with malware, prompting them to download and install software that has no purpose (other than to benefit the offender) or is malware. Scareware is also known as deception software, rogue scanner software, and fraud. Scareware is also disseminated via spam email, which issues bogus warnings or urges consumers to purchase unnecessary or harmful services.



Figure 7 Scareware

### 2.3. Pretexting

A scam artist may begin the con by claiming that he or she requires sensitive information from a victim in order to fulfill a critical task. To acquire trust from their target, the attacker typically impersonates coworkers, police, bank and tax officials, or other people with right-to-know authority. The pretext asks inquiries that appear to be needed to verify the victim's identity, but are actually designed to gather sensitive personal data.



Figure 8 Pretexting

## 2.4. Phishing

One of the most prevalent social engineering attack types is phishing scams, which are email and text message campaigns aimed at building a sense of urgency, curiosity, or dread in victims. People are then pressured into providing personal information, visiting phishing websites, or opening malware-infected attachments.

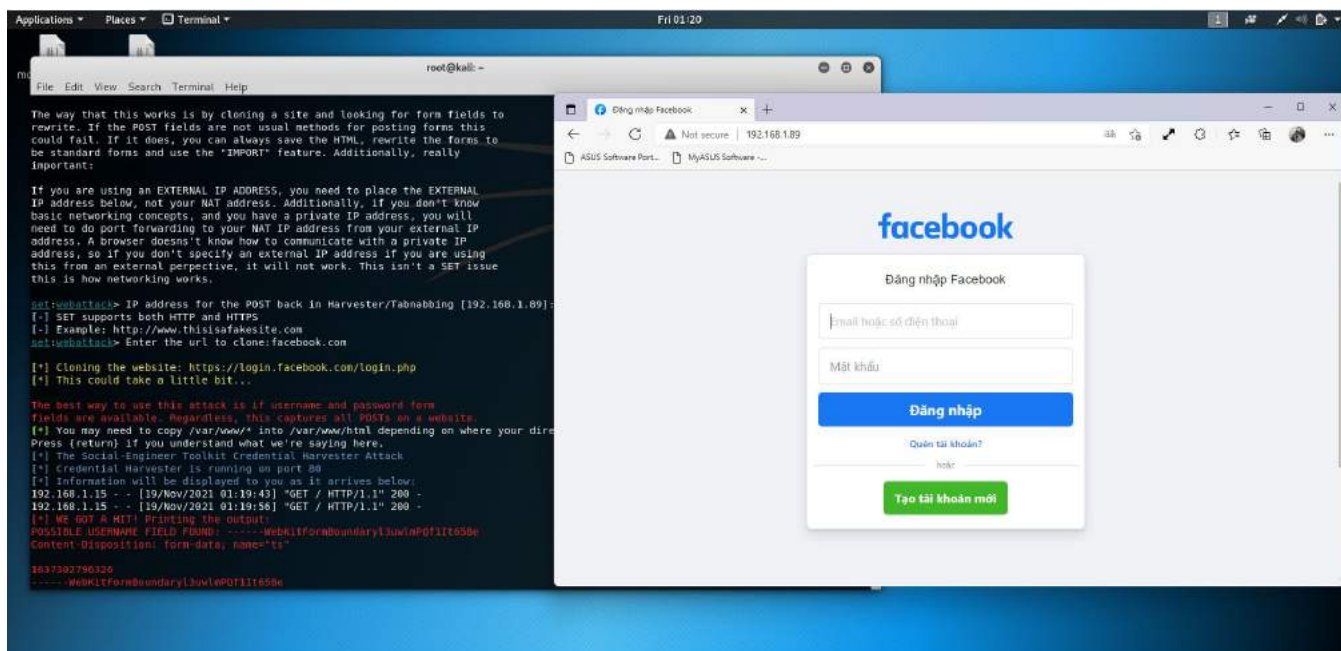


Figure 9 Phishing

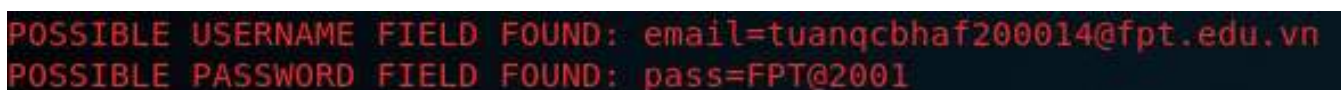


Figure 10 Report Phishing

## 2.5. Spear Phishing

This is a highly focused phishing scam in which the offender focuses on a specific person or company. They tailor their emails depending on the traits, employment titles, and contacts of their victims to make their attack less noticeable. Spear phishing requires much more effort on the part of the perpetrator and can take weeks or months to execute. They're much more difficult to detect, and if done correctly, they have a much greater success rate.

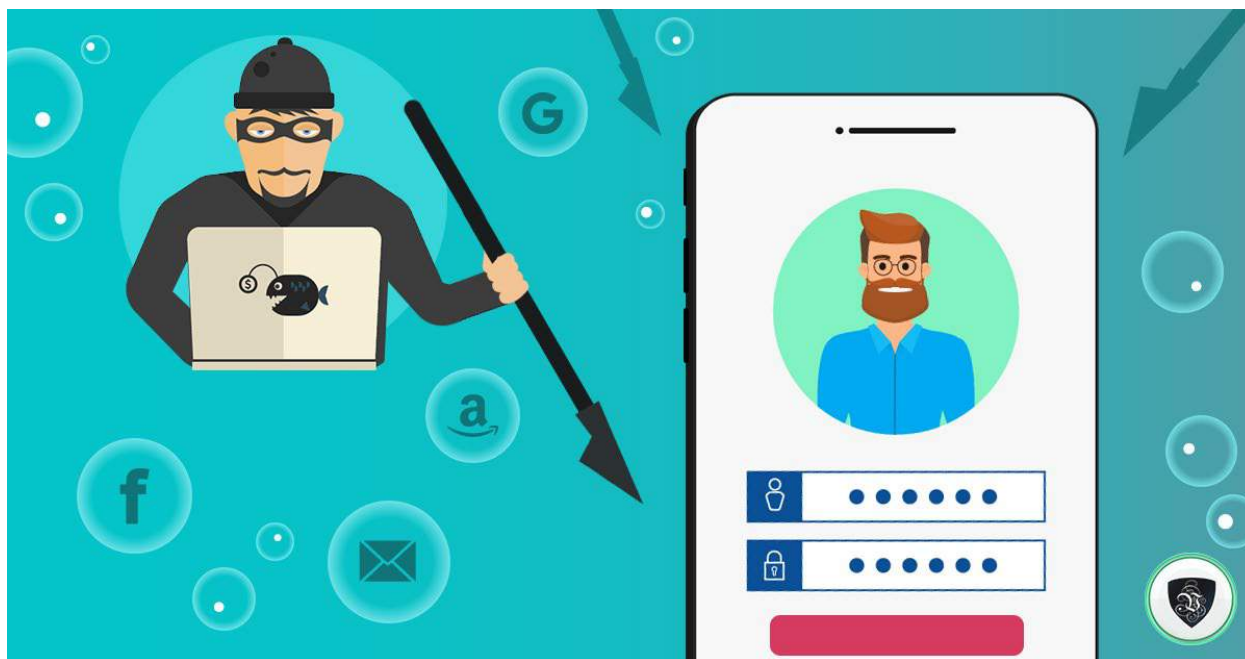


Figure 11 Spear Phishing

### 3. WEB APPLICATION ATTACKS

A Web application attack is any attempt by a malicious actor to compromise the security of a Web-based application. Web application assaults can either target the application directly to obtain access to sensitive data or utilize it as a staging place for attacks on the program's users.

**Protection:** To ensure that we are not attacked by "Website Application" attack groups, we should watch out for business information, secure the administrator's password. Limit the number of incorrect passwords attempts by a user. Change the login URL for the website/application management page. Always require 2FA or MFA authentication for added security. Decentralize account for reasonable. Use HTTPS website certificates.

#### 3.1. XSS

Cross-Site Scripting (XSS) assaults are injection attacks in which malicious scripts are inserted into otherwise trustworthy and innocent websites. XSS attacks occur when an attacker utilizes a web application to transmit malicious code to a separate end-user, usually in the form of a browser side script. The flaws that allow these attacks to succeed are common and can be found whenever a web application accepts user input in its output without verifying or encoding it.

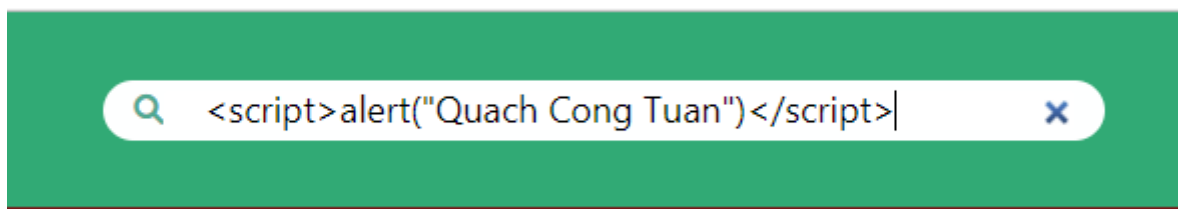


Figure 12 XSS - Cross Site Scripting



Figure 13 Report XSS

### 3.2. SQL Injection

SQL injection is a web security issue that allows an attacker to manipulate database queries in an online application. It enables an attacker to analyze data that they wouldn't normally have access to. This could include other users' data or any other information that the software has access to. An attacker can alter or remove this data on a regular basis, causing long-term modifications to the application's content or behavior.

```
[*] starting @ 01:46:27 /2021-11-19/
[01:46:28] [INFO] resuming back-end DBMS 'mysql'
[01:46:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=ACER-LAPTOP' AND 9454=9454 AND 'VxYm'='VxYm

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=ACER-LAPTOP' OR (SELECT 4450 FROM (SELECT COUNT(*), CONCAT(0x716a766271, (SELECT (ELT(4450=4450,1))), 0x716b627171, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUG
  DNS GROUP BY x)a) AND 'cyXD'='cyXD

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: id=ACER-LAPTOP' AND SLEEP(5) AND 'tZa1'='tZa1

  Type: UNION query
  Title: MySQL UNION query (random number) - 7 columns
  Payload: id=ACER-LAPTOP' UNION ALL SELECT 4786,4786,4786,CONCAT(0x716a766271,0x4b6f5763596f7a52774f6b50415a46674d4c576c4a414b4759694d59506e4f685944477677427770,0x716b6271
  71),4786,4786,4786#
---
[01:46:33] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[01:46:33] [INFO] fetched data logged to text files under '/root/.sqlmap/output/btech-qcngtuan.00@webhostapp.com'
```

Figure 14 SQL Injection



Figure 15 Report SQL Injection

### 3.3. DoS

A denial-of-service (DoS) attack is a sort of cyber-attack in which a malicious actor attempts to make a computer or other device unavailable to its intended users by disrupting its usual operation. DoS attacks work by overloading or flooding a targeted machine with requests until normal traffic cannot be processed, causing a denial-of-service to further users. A DoS attack is defined as one that is launched from a single computer.

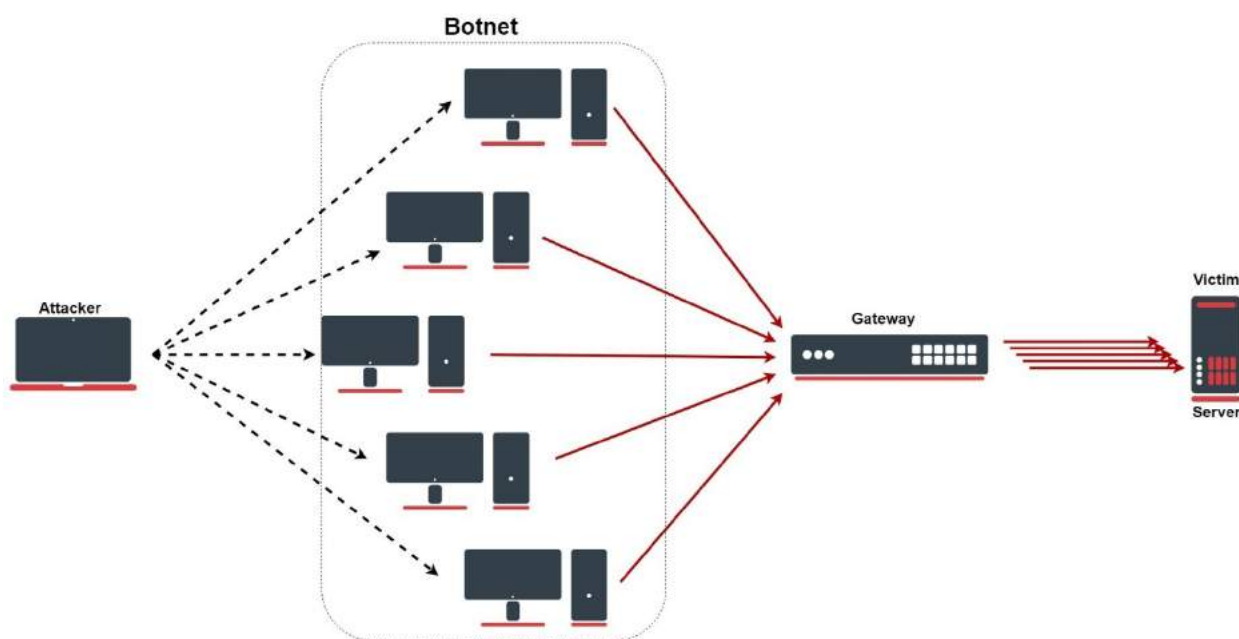


Figure 16 DoS

#### 3.3.1. Buffer overflow attacks

A memory buffer overflow might allow a machine to consume all available hard disk space, memory, or CPU time in this attack type. This type of exploit frequently causes sluggishness, system failures, or other harmful server behaviors, resulting in a denial-of-service attack.

#### 3.3.2. Flood attacks

A hostile actor can oversaturate server capacity by flooding a targeted server with an excessive quantity of packets, resulting in denial-of-service. The attacking actor must have more accessible bandwidth than the target in order for most DoS flood assaults to succeed.

#### 4. NETWORKING BASED ATTACKS

Network-based attacks eavesdrop on, intercept, and manipulate network communications in order to compromise network security. These can be active assaults, in which the hacker changes network activity in real time, or passive attacks, in which the attacker observes network activity but does not attempt to change it.

##### 4.1. Sniffing

Sniffing is a network data-stream attack in which an attacker reads, monitors, or captures complete packets of data passing between a client and a server. An unencrypted network packet intercepted by a hacker might inflict significant damage to the company or institution that owns the data. Sensitive information such as account credentials, bank data, and many types of Personally Identifiable Information may have been hacked (PII). Active sniffing attacks (which involve both data access and manipulation) and passive sniffing attacks (in which the attacker just sees the information but does not actively interfere with its transmission) are the two types of sniffing attacks.

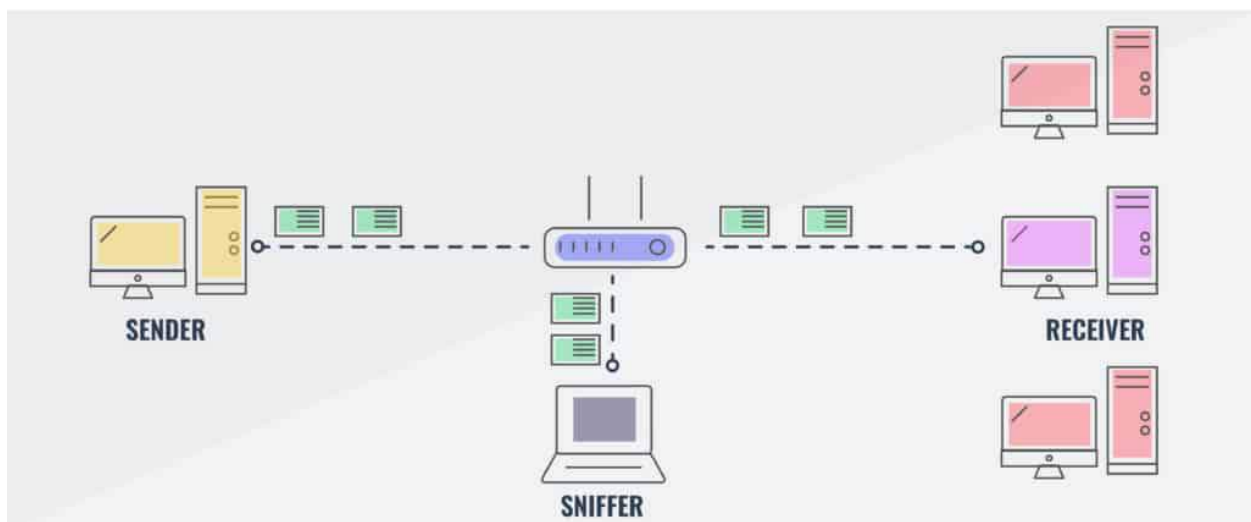


Figure 17 Sniffing



## 4.2. Spoofing

Spoofing is the practice of a bad actor impersonating a legitimate entity or someone they are not. It mainly refers to "a computer faking an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server" in the context of network security. Using IP address spoofing, attackers can get access to networks that employ IP addresses for user authentication that are normally off-limits. They may also employ ARP spoofing to link their own Media Access Control (MAC) to a legitimate IP address, allowing them access to data intended for someone else's IP address. DNS spoofing allows hackers to redirect traffic to an IP address other than the one intended. Attacks based on spoofing are utilized.

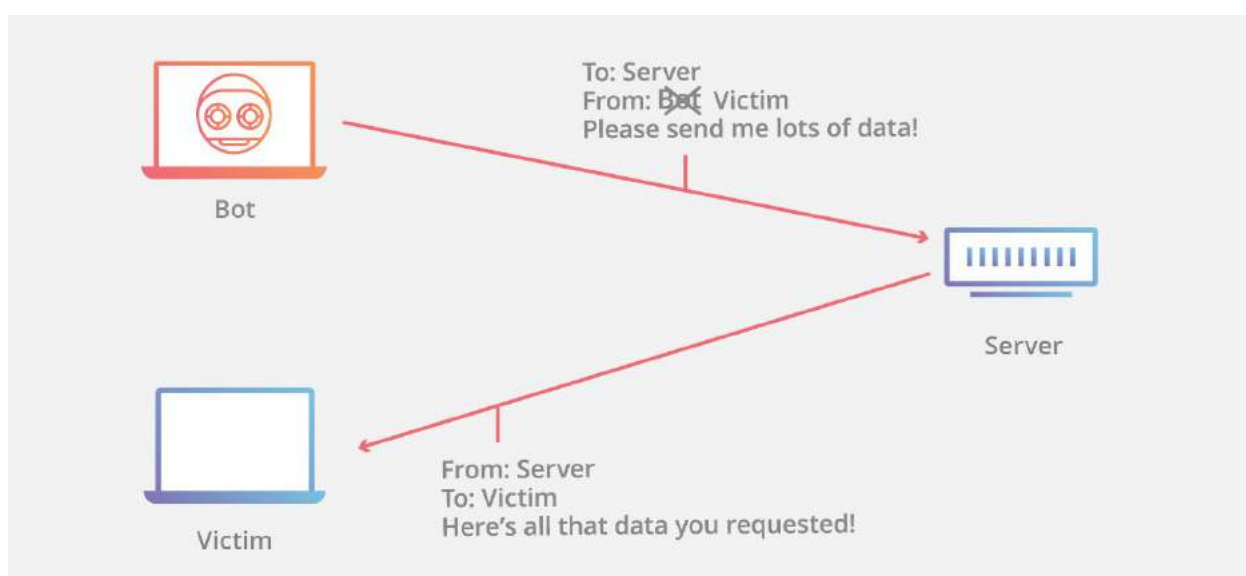


Figure 18 Spoofing

### 4.3. DDoS

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt a targeted server's, service's, or network's normal traffic by flooding the target or its surrounding infrastructure with Internet traffic.

DDoS assaults are effective because they use numerous compromised computer systems as attack traffic sources. Computers and other networked resources, such as IoT devices, are examples of exploited machinery.

- DDoS assaults are carried out via networks of machines that are linked to the Internet.
- These networks are made up of malware-infected PCs and other devices (such as IoT devices), which may be manipulated remotely by an attacker. Individual devices are known as bots (or zombies), while a botnet is a collection of bots.
- The attacker can direct an attack once a botnet has been built by delivering remote instructions to each bot.
- When a botnet targets a victim's server or network, each bot sends requests to the target's IP address, potentially overloading the server or network and causing a denial-of-service to normal traffic.

**Protection:** For DDOS attacks, we need to use a firewall for web applications (WAF). This firewall will help us prevent attacks from XSS, SQL Injection, Buffer Overflow, or DDOS. I have researched and suggested we should use Cloudflare so they can help us to prevent attacks and navigate. Besides, we need to monitor website downtime. Downtime is the period the website is not available to visitors. **Downtime** can happen because the website is attacked by a denial of service (DDoS), maybe the website is overloaded, or there is a problem with the Hosting service you are using. A website needs to maximize uptime and minimize downtime.

#### 4.3.1. Application layer attacks (HTTP Flood)

The purpose of a layer 7 DDoS assault (named after the OSI model's seventh layer) is to exhaust the target's resources and cause a denial-of-service attack.

The attacks go after the layer that generates and delivers web pages in response to HTTP requests on the server. On the client side, a single HTTP request is computationally cheap, but it can be costly for the target server to respond to, as the server must frequently load numerous files and do database queries to build a web page. Layer 7 assaults are difficult to protect against because distinguishing malicious from genuine traffic can be challenging.

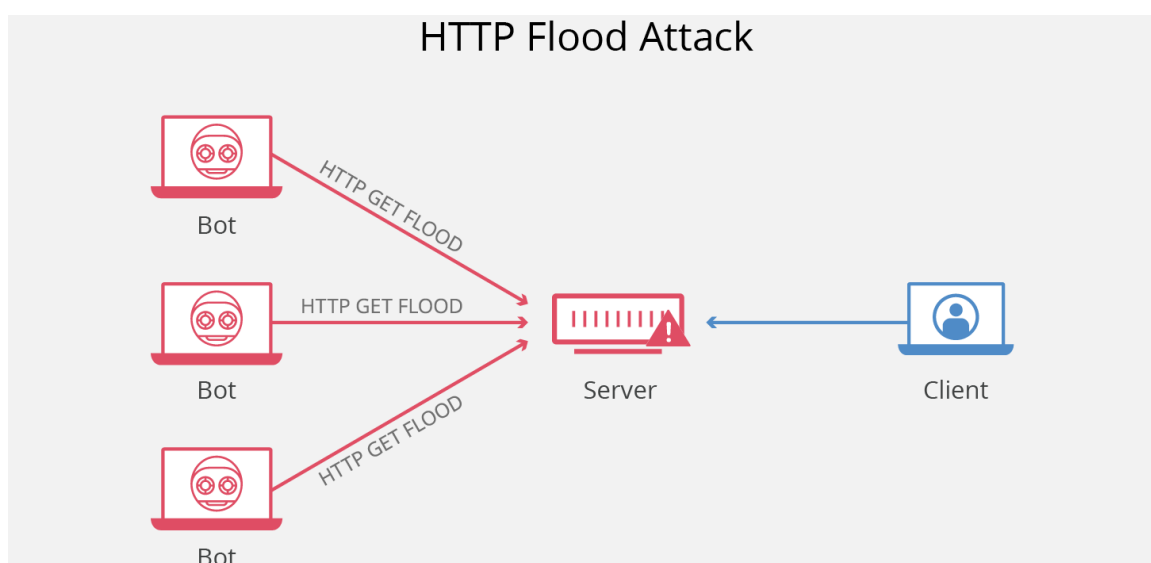


Figure 19 HTTP Flood

#### 4.3.2. Protocol attacks (SYN Flood)

Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.

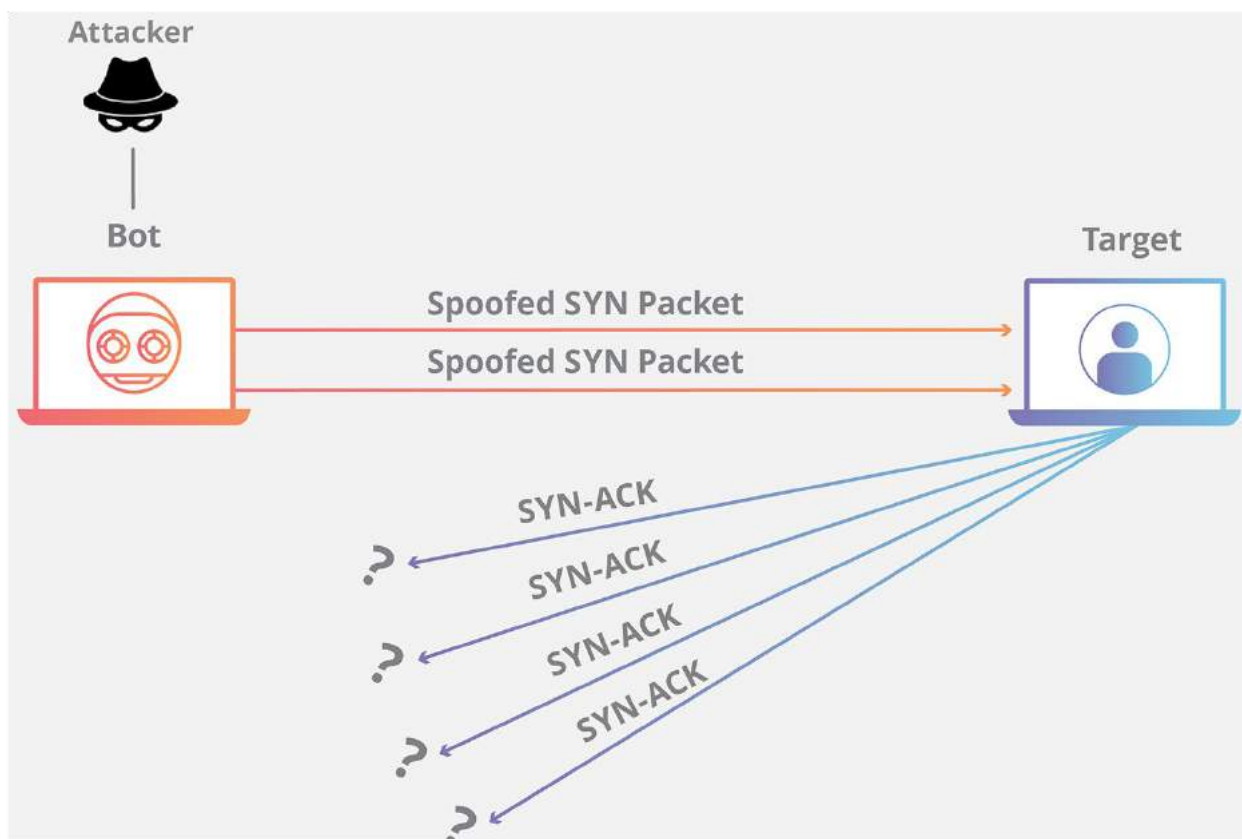


Figure 20 SYN Flood

### 4.3.3. Volumetric attacks (DNS Amplification)

This type of attack tries to clog up the Internet by absorbing all available bandwidth between the target and the rest of the world. Amplification or another method of creating big traffic, such as requests from a botnet, is used to send large amounts of data to a target.

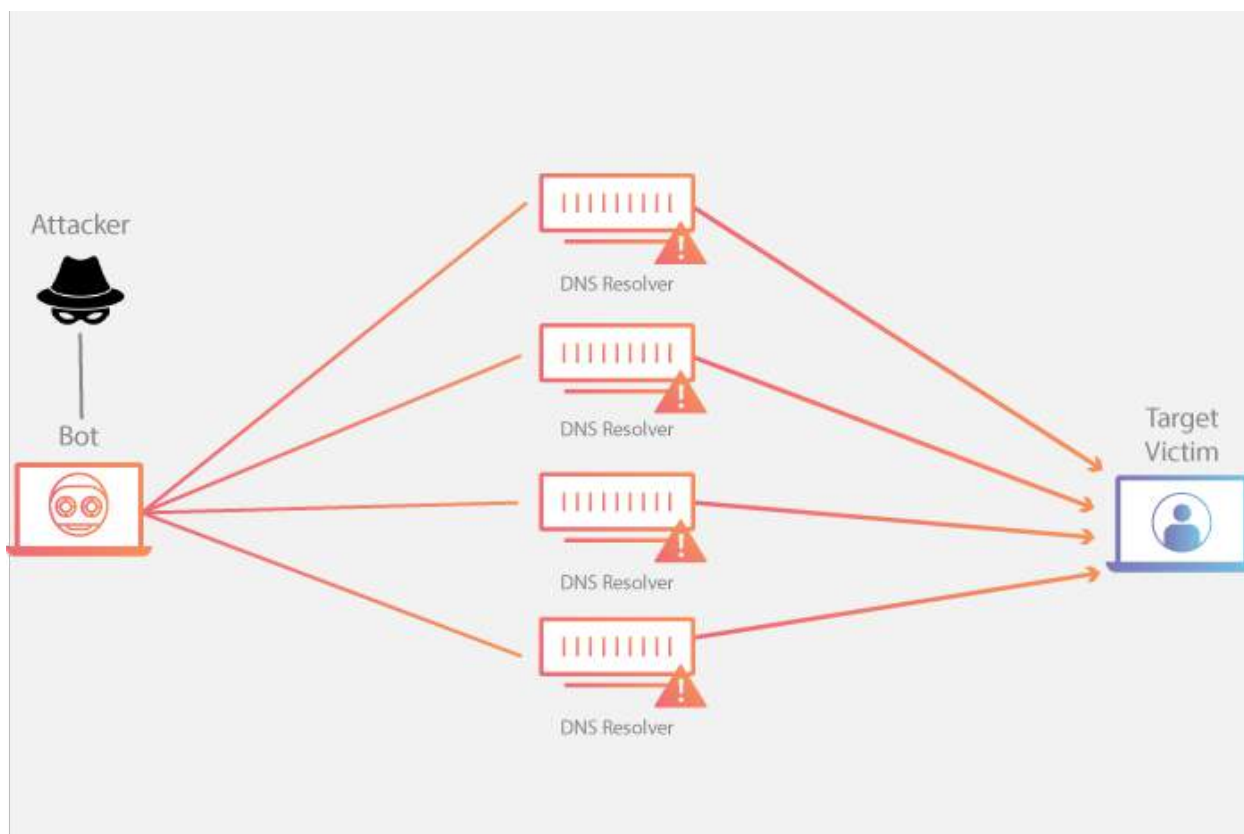


Figure 21 DNS Amplification

## Prevention Risk Organizations

I have given a security method for this project of NorthStar company this time, we need to set up a copyrighted anti-virus program, constantly updating the database. In addition, personal information needs to be confidential. NorthStar's system needs to decentralize users with security policies and procedures such as 2FA/MFA identity authentication. Prevent unauthorized applications (crack). Continuously back up data to the backup system to avoid risks. Use a firewall for websites, install the "Chống Lừa Đảo" extension to prevent fraudulent websites.

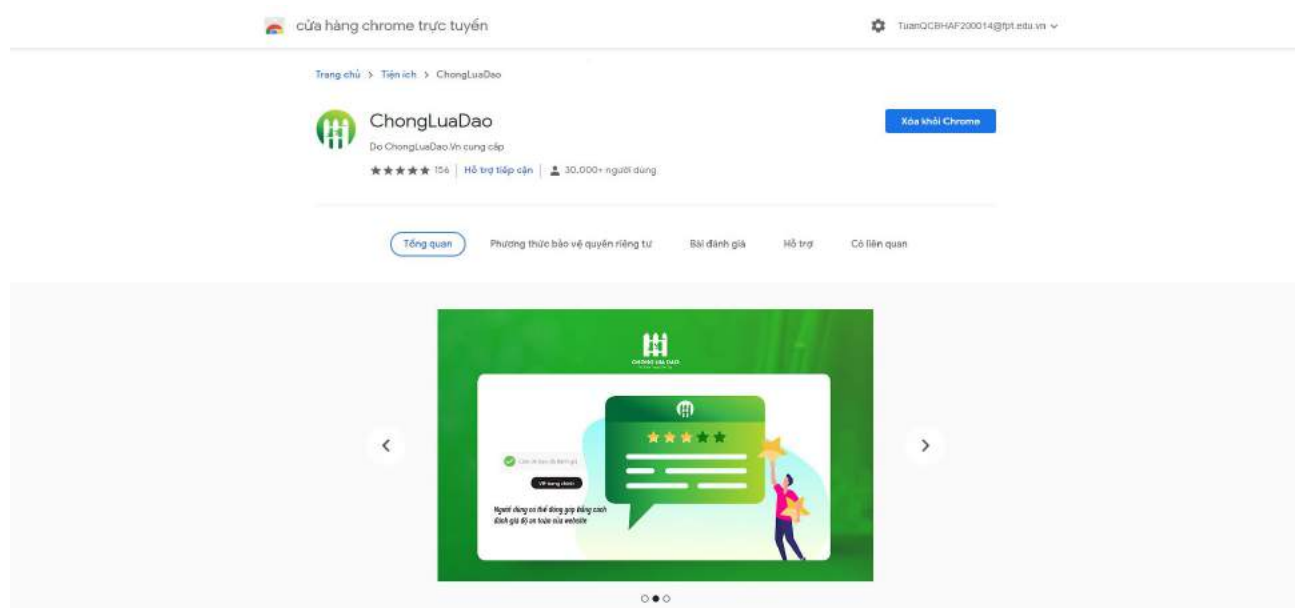


Figure 22 ChongLuaDao

## Example of a business that has been attacked

### BKAV – SQL Injection

As noted on August 4, 2021, at the \*\*\*\* Raid Forum, part of the internal data and source code of BKAV anti-virus software was posted by a hacker with the alias "Chunxiong". This hacker said he had infiltrated the server of this security firm BKAV and successfully extracted the source code of the anti-virus software developed by this company. In addition, this member also posted a lot of information about other internal projects of BKAV.

This hacker claimed to have used the SQL Injection attack method and easily accessed the system as a leader of BKAV, and at the same time, this member sold all BKAV's data for the money. is 580,000 USD and the buyer must pay in Monero coin (code XMR).

And until August 15, this hacker declared that he could not attack because BKAV actively closed the server and upgraded the security system. (Quy, 2021)

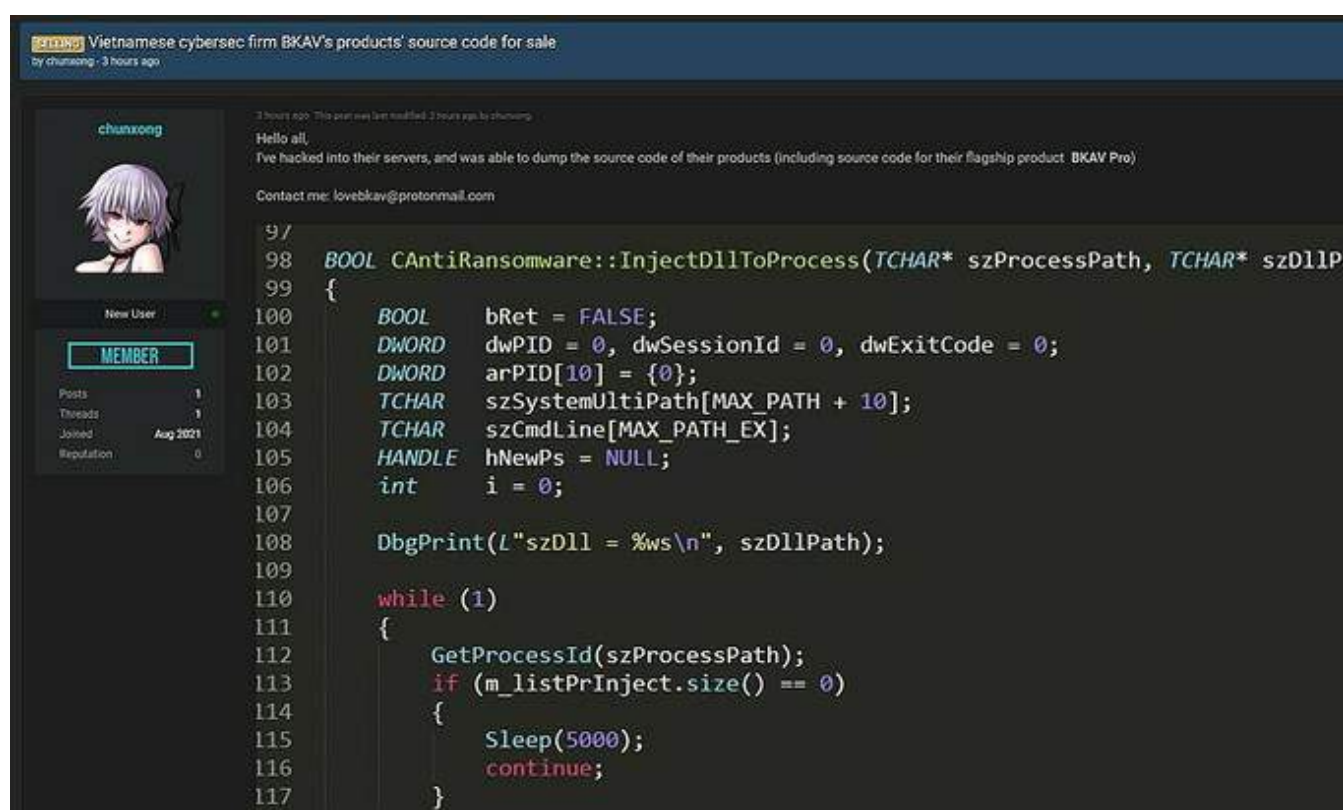


Figure 23 BKAV Example 1

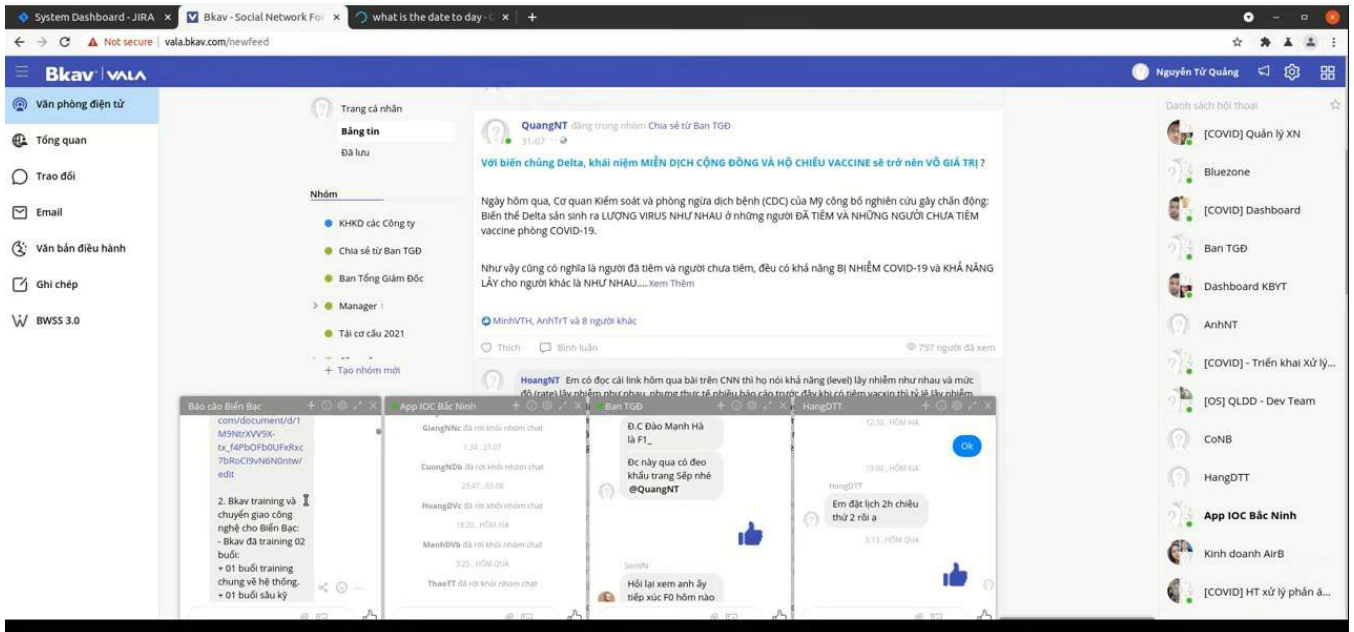


Figure 24 BKAV Example 2

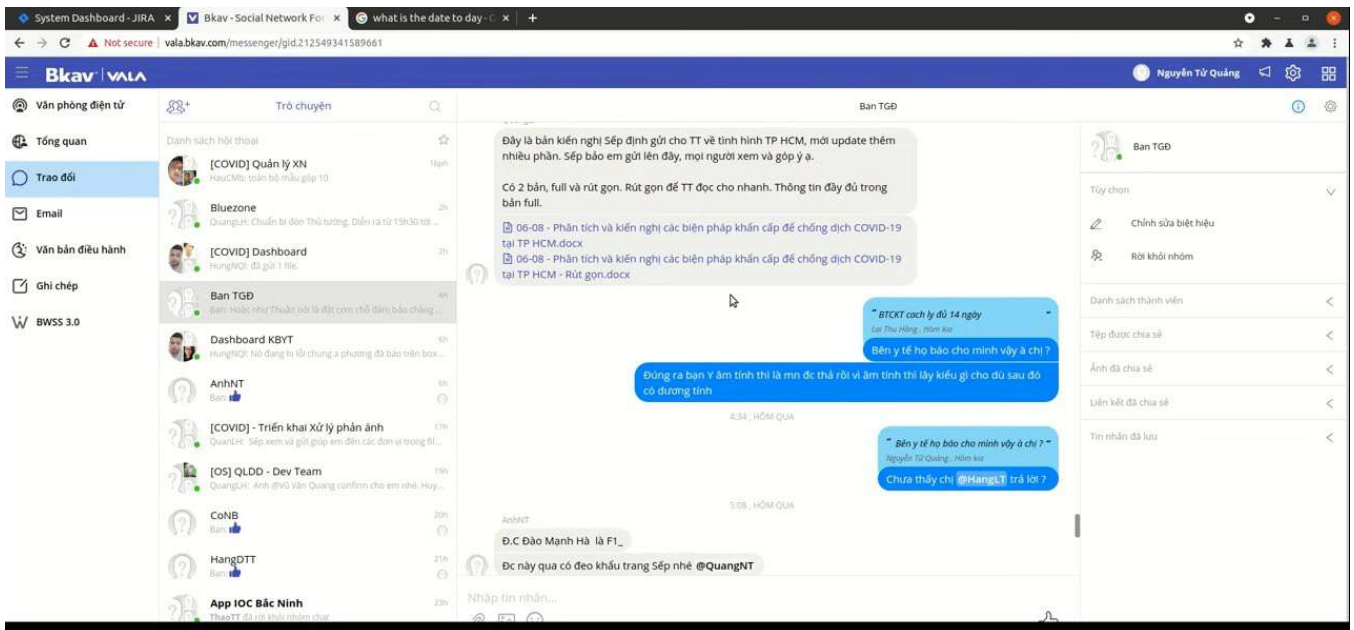


Figure 25 BKAV Example 3



## **P2. DESCRIBE ORGANIZATIONAL SECURITY PROCEDURES FOR NORTHSTAR.**

Procedures can be defined as a certain course of action or manner of operation. They characterize an activity or the method in which it is carried out in any action or process. The protocols detail the steps involved in requesting USERIDs, processing passwords, and destroying data. Procedures for seeking USERIDs or access modifications will be handled via email in the future, with simple templates prompting the requester for the necessary details. Requests can be expedited in minutes, resulting in increased productivity for all parties involved.

A security procedure is a set of steps that must be followed in order to complete a certain security duty or function. Procedures are typically developed as a set of actions to be performed in a consistent and repeatable manner to achieve a specific goal. Security procedures, once developed, give a set of established steps for performing the organization's security affairs, making training, process auditing, and process improvement easier. Procedures serve as a starting point for establishing the uniformity required to reduce variation in security procedures, hence improving security control inside the business. Reduced variety is also a smart method to get rid of it.

They can be viewed as logical and physical threats, requiring the implementation of security protocols. Use the procedures and tactics indicated below to safeguard the organization from logical threats:

## 1. Authentication

The process of ascertaining whether someone or something is who or what it claims to be is known as authentication. Authentication technology checks if a user's credentials match those in a database of authorized users or a data authentication server to offer access control for systems. SFA, which requires a user ID and password, or 2FA, which requires a user ID, password, and biometric signature, are just two examples of authentication factors. Multifactor authentication is defined as the use of three or more identity verification factors for authentication, such as a user ID and password, a biometric signature, and maybe a personal question that the user must answer.

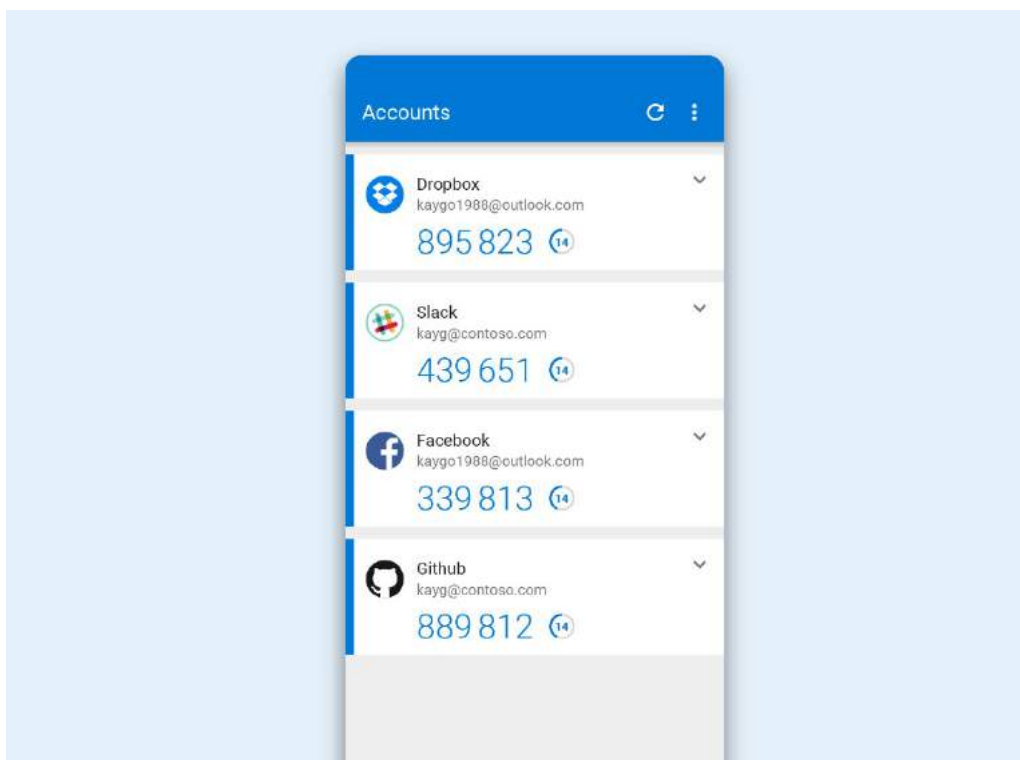


Figure 26 Authentication

## 2. Anti-Virus

Software designed to assist in the detection, prevention, and removal of malware (malicious software). Antivirus software is used to protect computers from viruses by scanning, detecting, and removing them. Most antivirus software operates in the background once installed, providing real-time protection against virus attacks. Comprehensive virus protection systems guard your files and hardware against malware like worms, Trojan horses, and spyware, and may also include features like customized firewalls and website blocking.

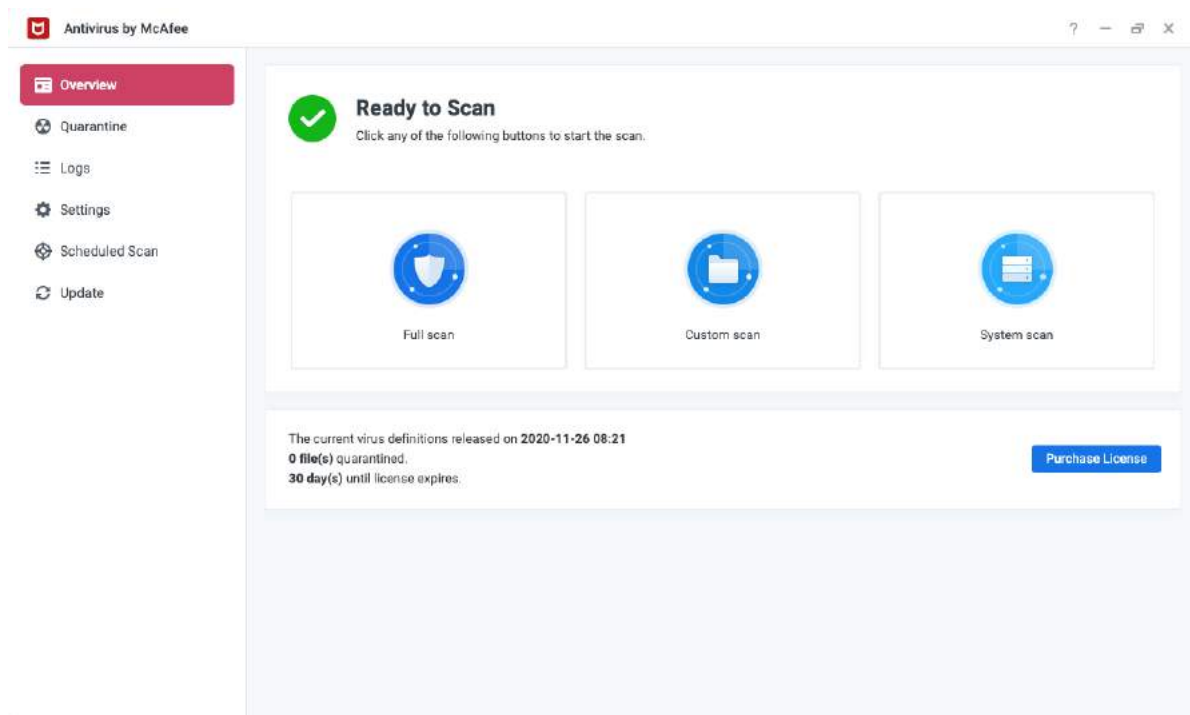


Figure 27 Antivirus

### 3. Cloudflare (Cloud Firewalls)

Cloud Firewalls are software-based network devices that are deployed in the cloud and are designed to prevent or mitigate unauthorized access to private networks. They are developed for modern business needs and sit within web application settings as a new technology.

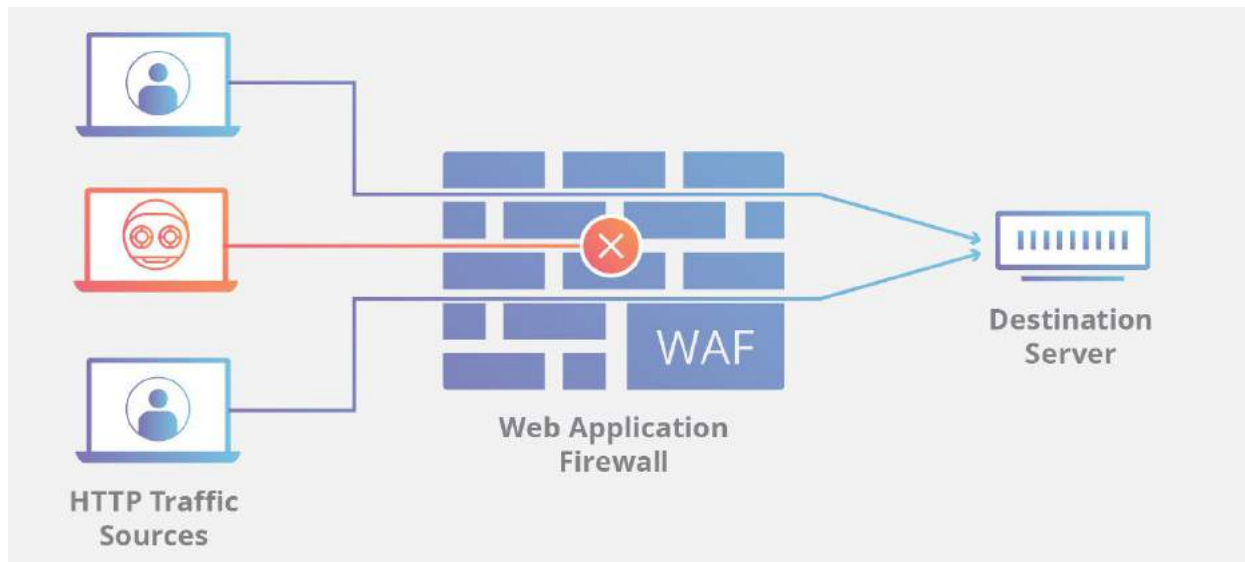


Figure 28 Cloud Firewall

#### 4. Ads Blocked and Pop-up Blocked

A pop-up blocker is software that blocks websites from displaying pop-up windows. They work by either shutting or disabling the command that causes the pop-up window to appear.

Advertisers typically employ pop-ups to convey adverts, but they detract from the user's experience and are generally regarded as a nuisance. Pop-ups used to be mostly harmless, but they have recently evolved into a potential hazard. If a person intentionally or unintentionally clicks on an advertisement, it is possible that they will be directed to a site with viruses and threats that will work unless certain precautions are taken to avoid negative results.

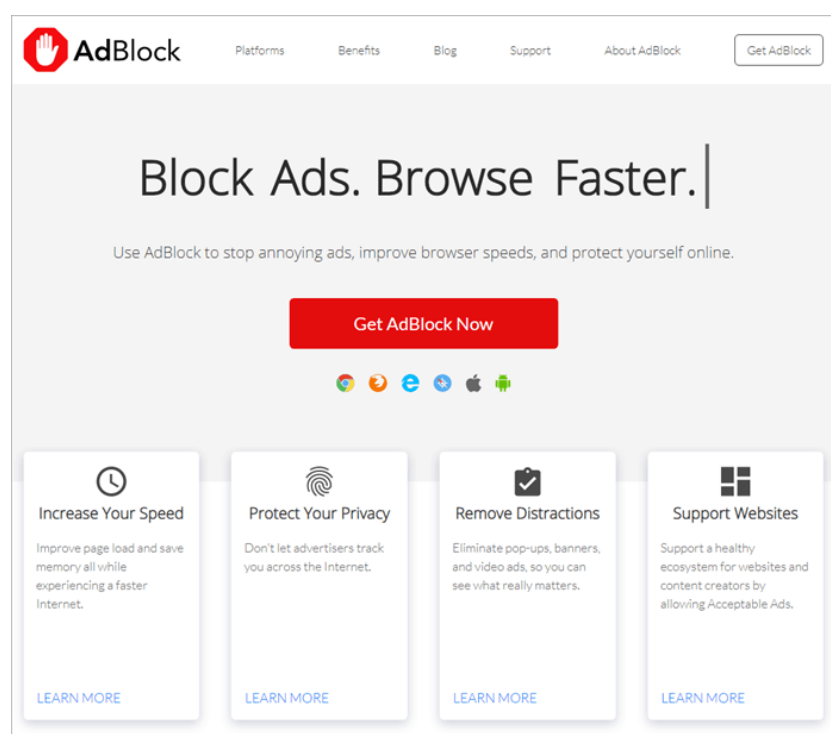


Figure 29 Ads Block

## 5. Employee training

Quality security training reduces the anxiety and uncertainty associated with typical online risks, resulting in a workforce that is more skilled, confident, and educated. As human error lowers, productivity will grow, and staff will be better positioned to identify and respond to security threats as they develop. This also relieves pressure on your IT department, allowing them to concentrate on more critical security issues and methods to improve your present security solutions.



Figure 30 Training

### **P3. IDENTIFY THE POTENTIAL IMPACT TO IT SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND IDS.**

#### **1. Firewall**

A firewall is a solution integrated into the network to combat unauthorized access, in order to protect internal sources of information and limit unwanted intrusion into the system. The function of the firewall Control the flow of information between the internal network and the Internet. Establish a mechanism for controlling the flow of information between the internal network and the Internet. There are 4 layers of firewall which are:

- **Firewall packet filter**

The package filter firewall works in the network layer of the OSI model, or the IP layer of the TCP/IP model. They are usually part of a router, which receives a package from one network and transfers the package to another. In the packet filter firewall, each package is compared to the standard set before it is forwarded. Based on the plan and standards, the firewall can cancel the plan, forward, or send a message to the plan creation site. For example, IP Chains, Router ACLs, ...

- **Circuit level gateways**

The network-level gateway works in the session layer of the OSI model, or the TCP layer of the TCP/IP model. They monitor the TCP compromise between packages to determine that a request session is appropriate. Information reaches the computer remotely via a network-level gateway, making the remote computer think the information comes from the gateway. This hides information about the protected network.

- **Application-level gateways**

Application-level gateways, also known as proxies, are similar to network-level gateways except for the designation of applications. They can filter packages in the application layer of the OSI model. In- or outgoing plans cannot access services without a proxy. For example, Gauntlet, Symantec Enterprise Firewall...

- **Stateful firewall**

Multi-layered firewalls are a formal combination of three types of firewalls. They filter packages in the network layer, identify the right packages, and evaluate the content of the packages at the application layer. For example, IP Tables, Net screen, ...

### 1.1. The Benefit of the firewalls:

- A firewall is a software or hardware based on a system that prevents unauthorized access to a private network. It acts as a barrier and checks data packets that come in or from a private network. It is often used to prevent unauthorized internet users from accessing a private network connected to an Internet.
- So much harm can be done if a hacker gets access to an organization's private network that steals information. Therefore, in order for policies and information to always be secure and secure, firewall and network security is put in place to prevent cyber-attacks from occurring.
- The firewall filters incoming information, via an internet connection to the network or personal computer system. It acts as a security checkpoint.
- Firewalls give companies or organizations control over how people connect and use their internet connection. You can prevent them from logging into certain websites or restrict the connections of certain users. The company can do this by establishing cybersecurity policies.
- The firewall is customizable. You can set policies and you can remove other policies. It all depends on what you want.
- An IP address (Internet protocol) is a digital mark assigned to each computer device connected to the internet. If an IP address is suspected, firewalls can block all traffic coming from the IP address. A company can block certain domains or allow access to specific domains.
- Servers make their service available with the internet using numbered ports.
- Separate firewall from a secure area and from a less secure area it controls communication between the two sides.



## 1.2. Firewall solution providers:

### 1.2.1. Cyberoam

Cyberoam is the new generation Firewall, with the best UTM Firewall and useful features. The machine can use 2 Wan connections at the same time, run load balancing and content filtering services. The device also has built-in VPN, IPS, Anti-Virus and Anti-Spyware, Anti-Spam, Web Filtering, Bandwidth Management, Multiple Link Management. Cyberoam also provides users with Multiple Security Zones to ensure network protection from hackers and malware

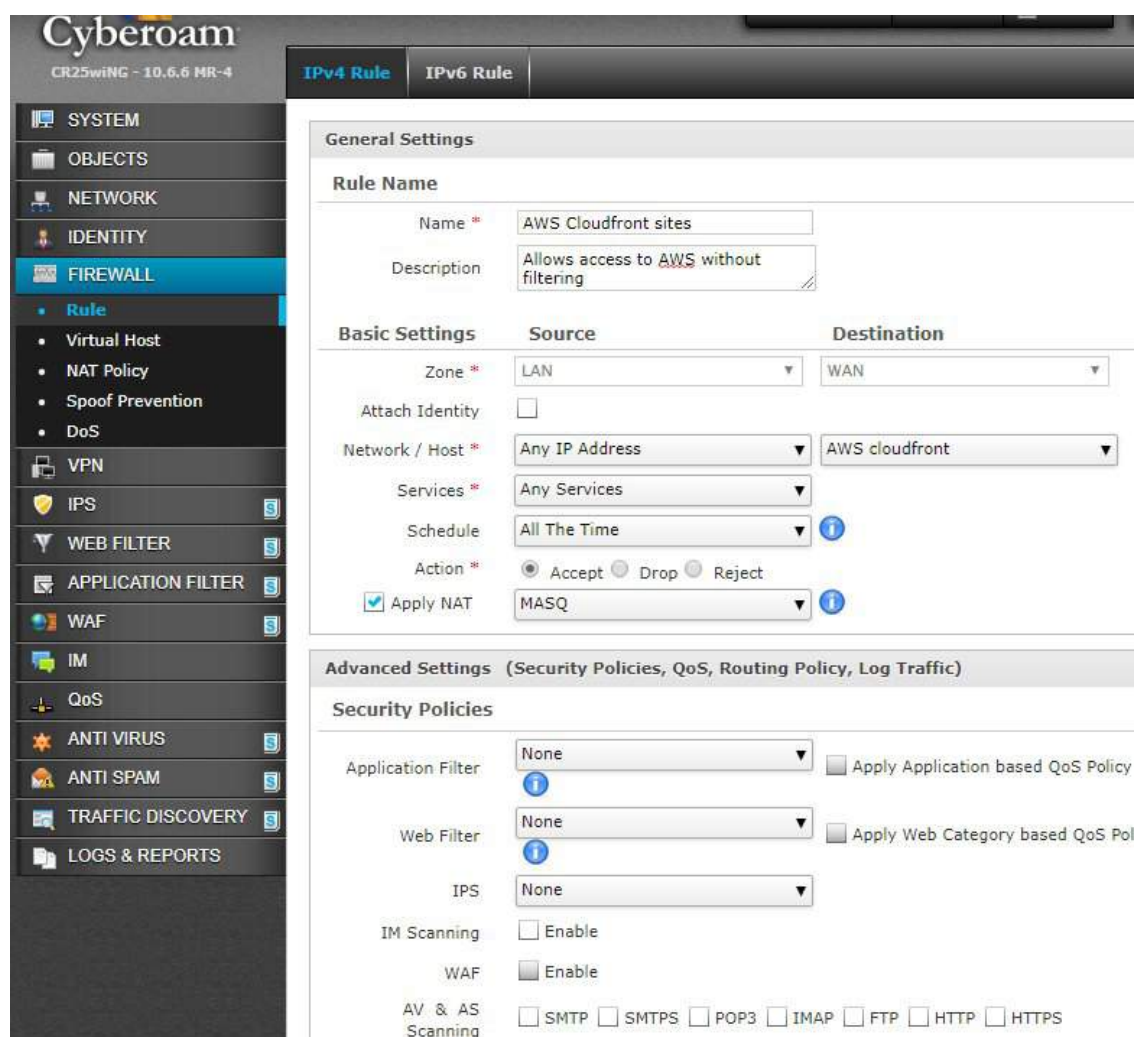


Figure 31 Cyberoam

### 1.2.2. Cisco

Cisco is one of the world's largest companies in the field of telecommunications equipment. In large networks, Cisco is always the first choice. Cisco SA 500 series products are believed to be the best Firewall for small and medium networks. The device is favored by IT people, used to monitor activities against hackers, spyware, malware with blocking unauthorized access from the outside. Cisco SA 500 Series has 4 LAN ports and 1 physical Wan port, and an optional Lan/Wan port that can be switched on demand.

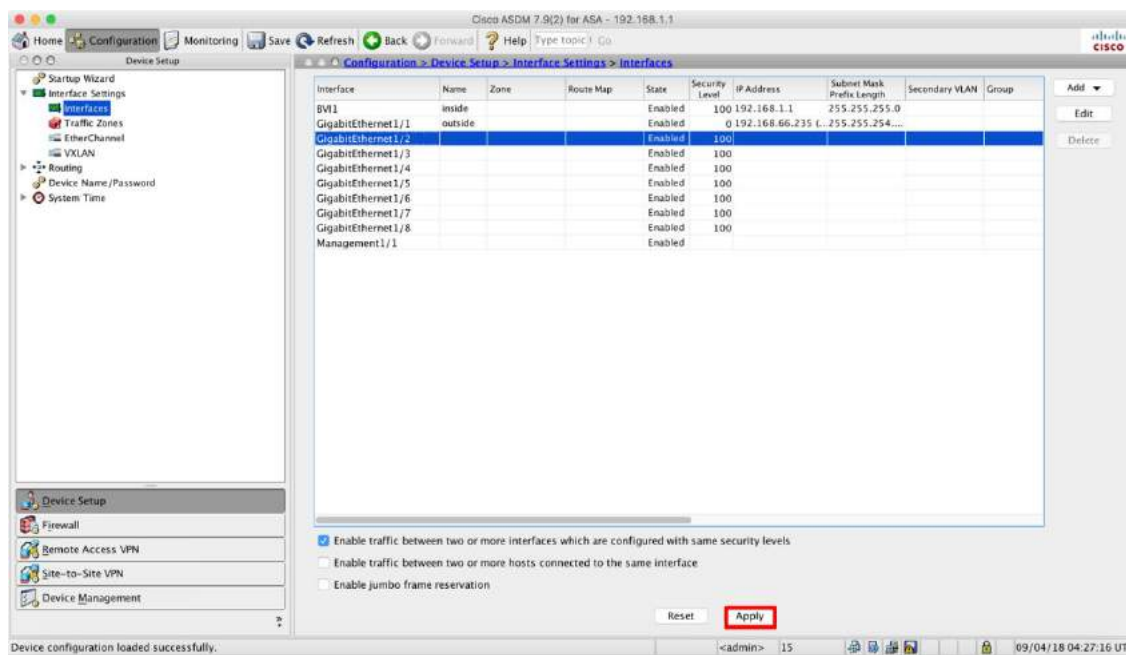


Figure 32 Cisco

### 1.2.3. Cloudflare

Cloudflare Firewall Rules is a flexible and intuitive framework for filtering HTTP requests. It gives you fine-grained control over which requests reach your applications. Firewall Rules complements existing Cloudflare tools by allowing you to create rules that combine a variety of techniques.

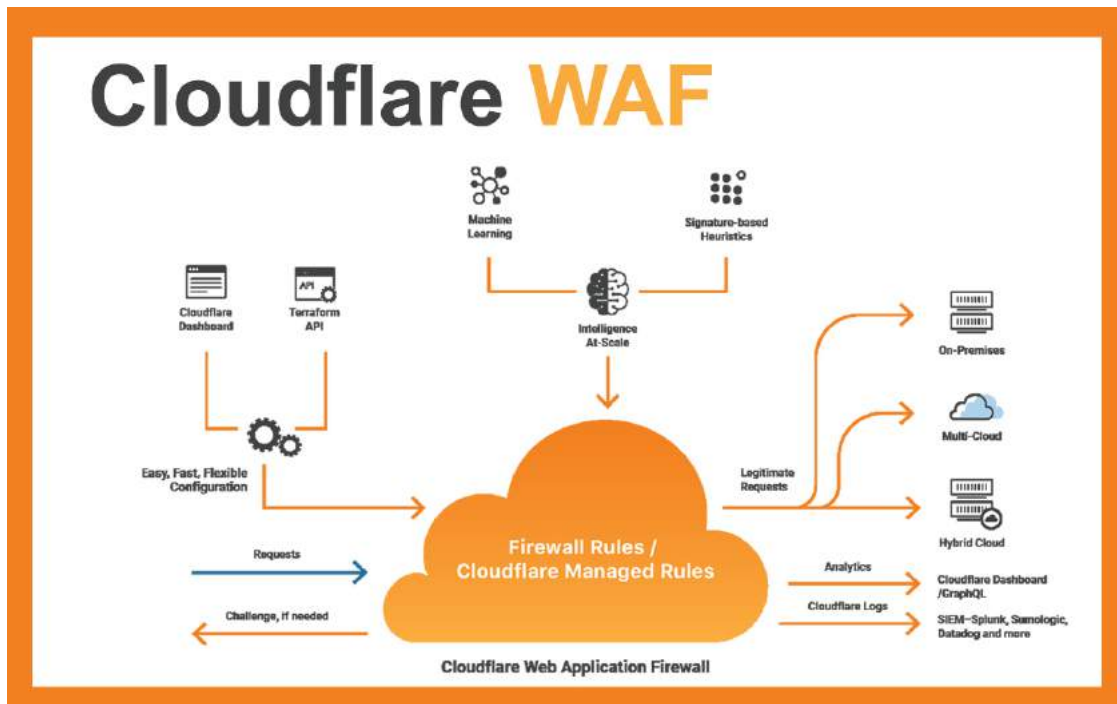


Figure 33 Cloudflare

## 2. IDS

The INTRUSION Detection System (IDS) is a network traffic monitoring system that detects anomalies, unauthorized activities, and systems. IDS can distinguish between internal (internal) or external attacks. IDS detection is based on specific indications of known risks (in the same way that antivirus software relies on special signs for detection and antivirus) or on comparing current network traffic with baseline (system-standard measurements that are acceptable right now) to find other signs often.

### 1. Function

- Monitor network traffic and suspicious activity.
- Network status alerts for systems and administrators.
- Combined with monitoring systems, firewalls, antiviruses form a complete security system.

### 2. There are two types of IDS in use: *NIDS* and *HIDS*:

- **NIDS:** network intrusion system. The system will gather the packet for deep analysis inside without changing the packet structure. NIDS can be software deployed on a server or as an appliance-integrated device.
- **HIDS:** Host intrusion detection system. Monitor unusual activities on separate hosts. HIDS is installed directly on the servers that need to be monitored.

### 3. Benefit of IDSs

- Provide a comprehensive view of the entire network traffic.
- Help check for problems with the network.
- Use to gather evidence for investigation and incident response.

#### **4. Legal System**

This is the set that will set the sign (sample) to compare, hungry with the data at the input. Normally, the law consists of many laws, each of which consists of two basic components: Rule Header and Rule Options.

**Rule header includes the following information:**

- Rule Action: Indicates that activities will be executed when "matching" the law (alert, log, pass, active, dynamic, drop ...).
- Protocol: Indicates the protocol will be tested (TCP, UDP, ICMP, IP...)
- IP address: Give information about IP address.
- Port number: Give information about the port.
- Direction: Indicates the direction of the data that is matched.

**Rule options are divided into 4 categories:**

- General: provides general information about the law (msg, reference, rev, classtype...).
- Payload: Search for the payload content of the packet (content, offset, depth, distance, within ...).
- Non-payload: Search for the non-payload content of the packet (ttl, ack, tos, id, dsize...).
- Post-detection: provides next execution methods (logto, session, tag...).

## 5. IDS implementation models

### 1. Set between router and firewall

When placed in this case, IDS will track all traffic on both directions. When deployed under this structure, IDS is subject to great pressure in volume, but has the ability to monitor the entire traffic of the network. Therefore, in this case it is recommended to choose IDS devices with high load capacity to improve performance.

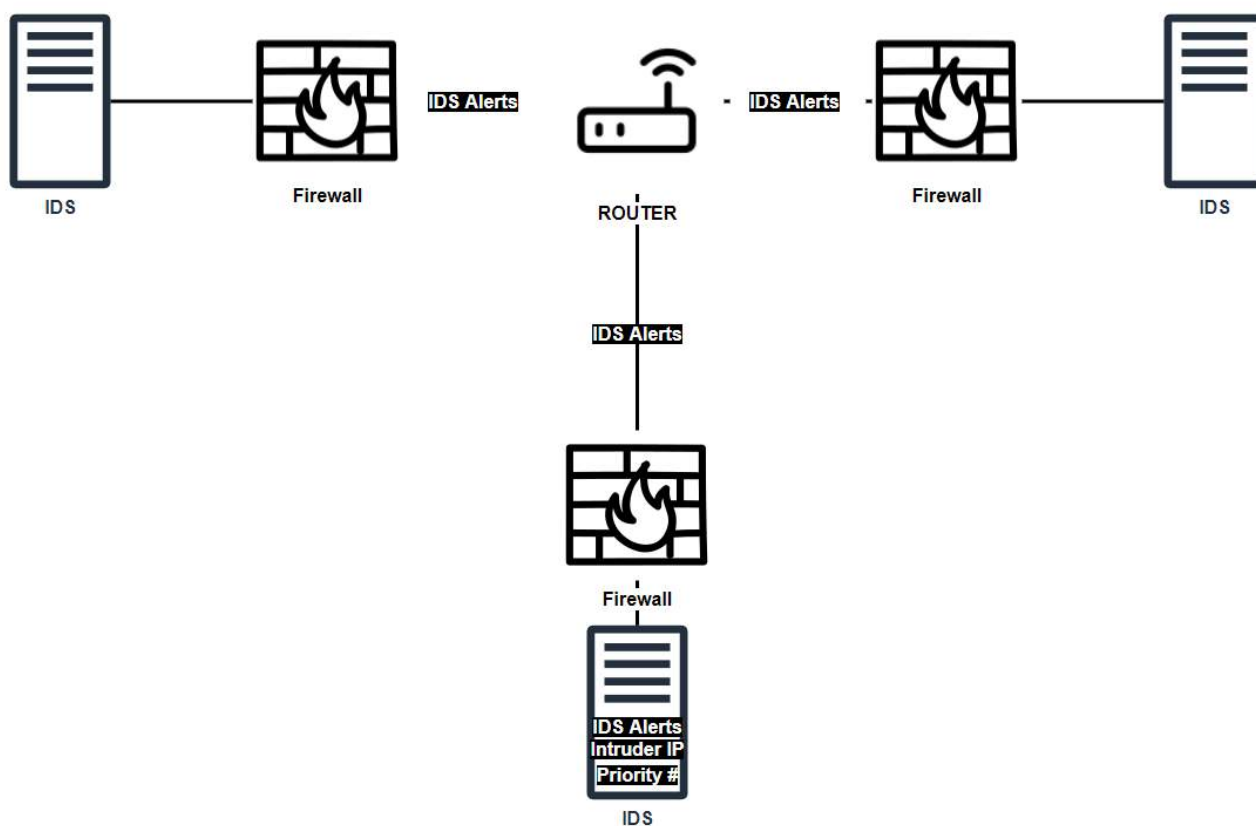


Figure 34 IDS-Model-1

## 2. Set in the DMZ

When placed in this case, IDS will track all in/out traffic in the DMZ domain

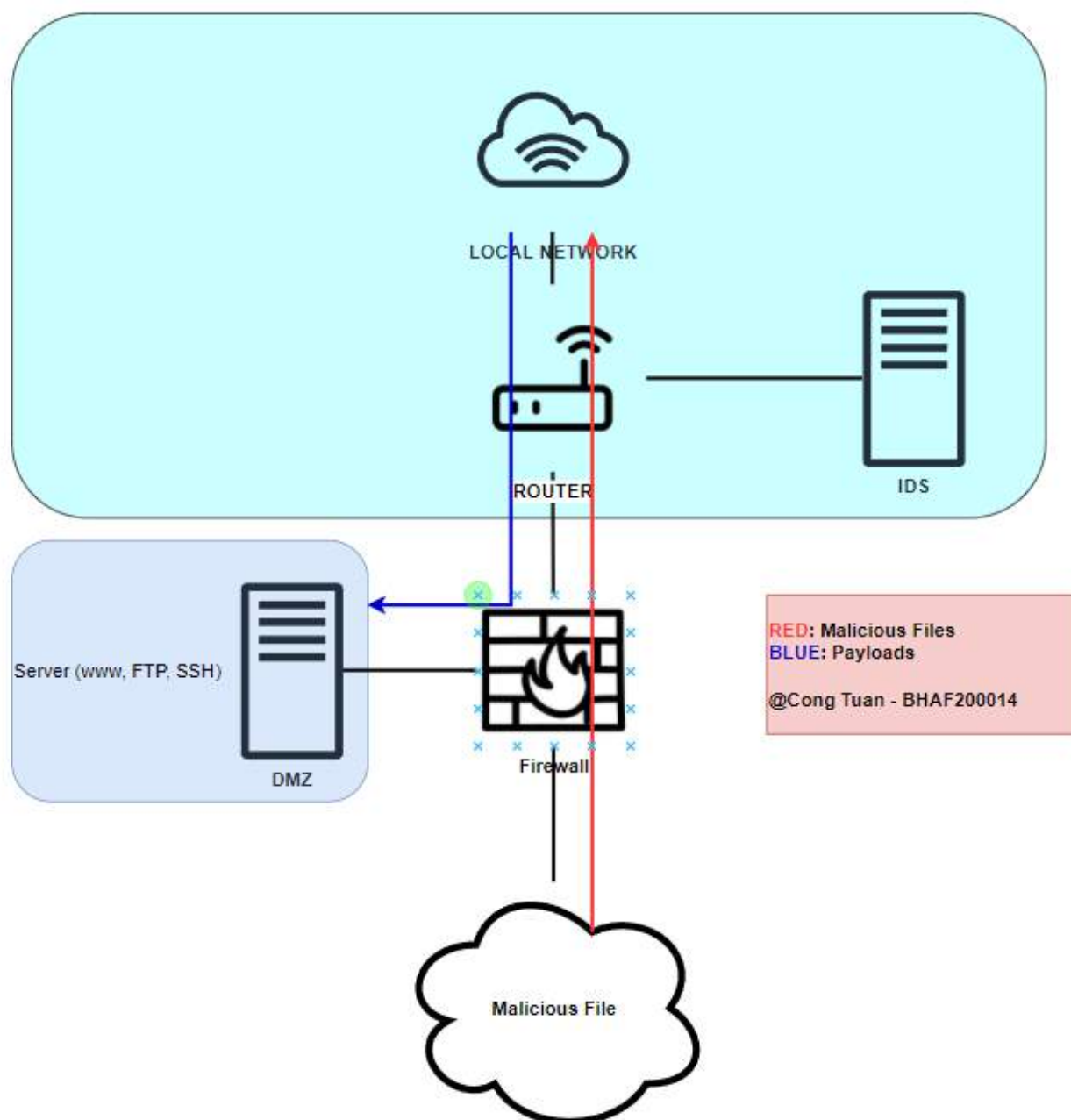


Figure 35 IDS-Model-2

### 3. Put behind firewall

When placed in this case, IDS will track all exchange traffic behind the firewall such as:

- Data exchanged in LAN.
- Data from LAN in/out of the DMZ and vice versa.

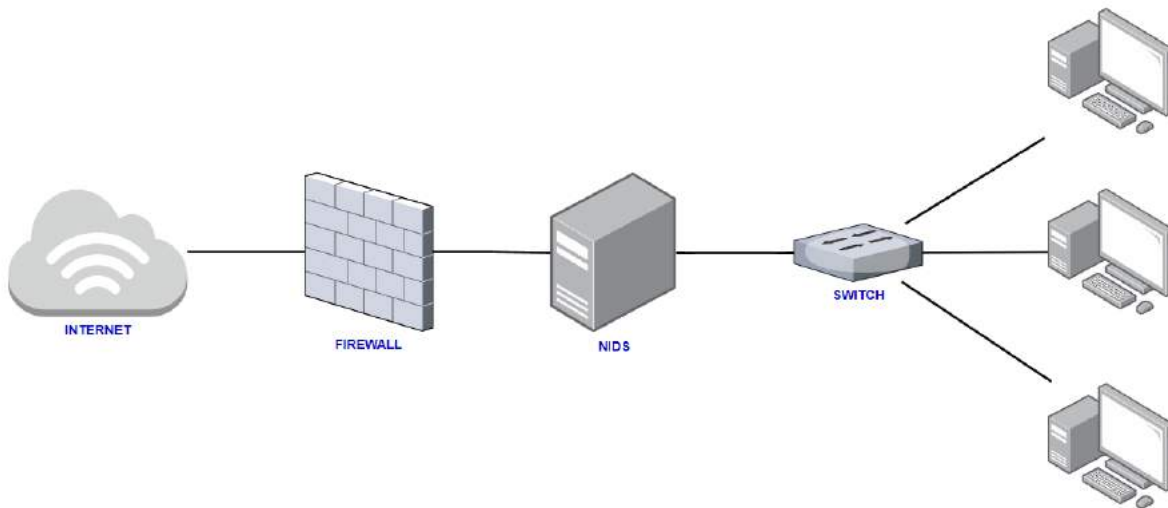


Figure 36 IDS-Model-3



#### P4. SHOW, USING AN EXAMPLE FOR EACH, HOW IMPLEMENTING A DMZ, STATIC IP AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY.

##### 1. DMZ

A DMZ Network is a perimeter network that protects an organization's internal local-area network from untrusted traffic and adds an extra degree of security. A DMZ is a subnetwork that connects the public internet to private networks. The purpose of a DMZ is to allow an organization to connect to untrusted networks, such as the internet, while maintaining the security of its private network or LAN. External-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, are often stored in the DMZ. DMZ networks have played a critical role in protecting global commerce. They protect organizations' sensitive data, systems, and resources by keeping internal networks separate from systems that could be targeted by attackers. DMZs also enable organizations to control and reduce access levels to sensitive systems.

For example, a cloud service like **Microsoft Azure** allows an organization that runs applications on-premises and on virtual private networks (VPNs) to use a hybrid approach with the DMZ sitting between both. This method can also be used when outgoing traffic needs auditing or to control traffic between an on-premises data center and virtual networks.

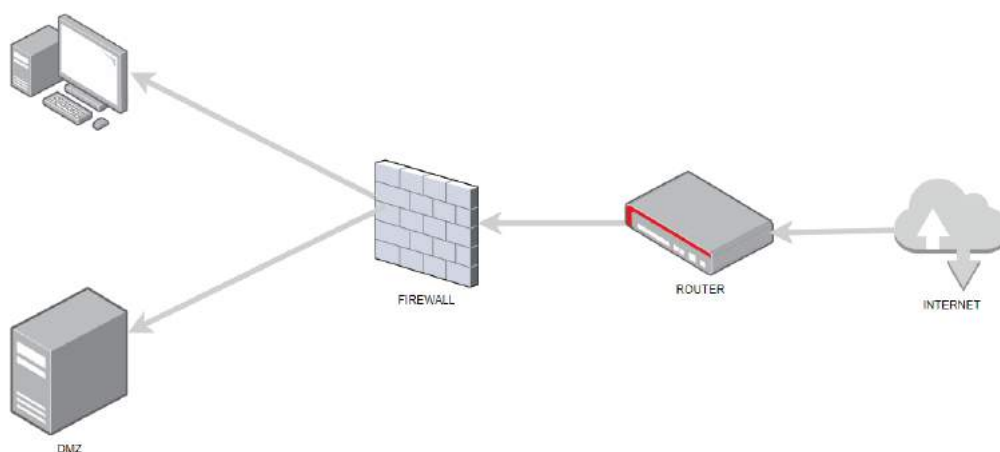


Figure 37 DMZ

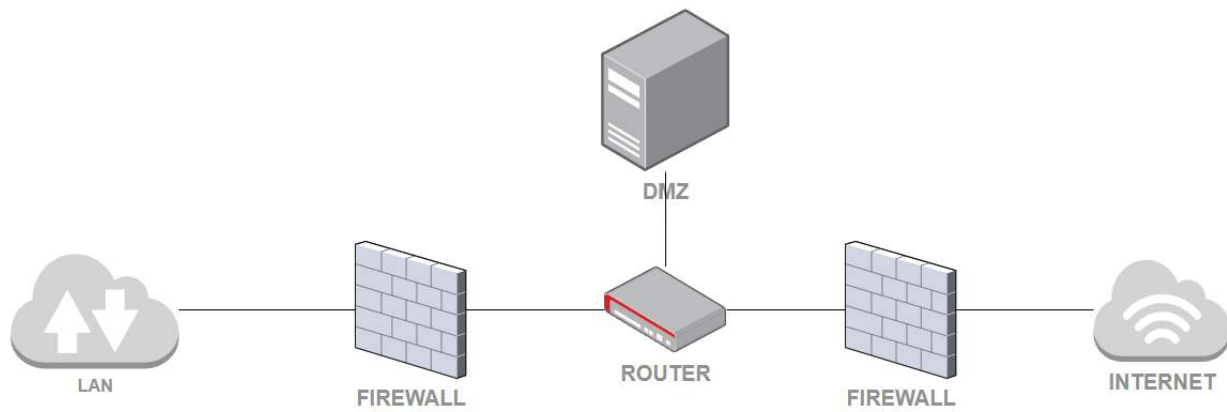


Figure 38 DMZ Network Architecture

## **2. IP**

### **2.1. IP Address**

An IP address is a unique number assigned to every device on a TCP/IP network. Just like your physical home address lets people know where to send your birthday card, IP addresses identify computers and devices and lets them communicate with each other.

### **2.2. Static IP Address**

An IP address that does not change is known as a static IP address. When your device is given a static IP address, it usually stays that way until it is retired or your network architecture changes. Servers and other key equipment typically utilize static IP addresses.

Internet Service Providers (ISPs) assign static IP addresses (ISPs). Depending on the terms of your service agreement, your ISP may or may not assign you a static IP address. Your options will be discussed later, but for now, expect that a static IP address will increase the cost of your ISP contract.

A static IP address might be IPv4 or IPv6; the crucial quality is static in this situation. Every piece of networked equipment we have may one day have a unique static IPv6 address. We haven't arrived yet. For the time being, permanent addresses are normally assigned to static IPv4 addresses.

### **2.3. Dynamic IP Address**

Dynamic IP addresses, as the name implies, are liable to change at any time, often without warning. Dynamic Host Configuration Protocol (DHCP) servers assign dynamic addresses as needed.

Because IPv4 does not give enough static IP addresses, we use dynamic addresses. A hotel, for example, might have a static IP address, but each device in its rooms might have a dynamic IP address.

Your ISP's DHCP server may assign a dynamic IP address to your home or workplace over the internet. Your network router is likely to assign dynamic IP addresses to your devices within your home or business network, whether they are personal PCs, cellphones, streaming media devices, tablets, or whatever else. Dynamic IP is the industry standard for consumer electronics.

## 2.4. Static IP Address can improve network security

There are numerous advantages to using a static IP address. Among these benefits are:

- Better DNS support: Static IP addresses are much easier to set up and manage with DNS servers.
- Server hosting: If you are hosting a web server, email server, or any other kind of server, having a static IP address makes it easier for customers to find you via DNS. Practically speaking that means it's quicker for clients to get to your websites and services if they have a static IP address.
- Convenient remote access: A static IP address makes it easier to work remotely using a Virtual Private Network (VPN) or other remote access programs.
- More reliable communication: Static IP addresses make it easier to use Voice over Internet Protocol (VoIP) for teleconferencing or other voice and video communications.
- More reliable geo-location services: With a static IP address, services can match the IP address with its physical location. For example, if you use a local weather service with a static IP address, you're more likely to get the weather report you need instead of the one for the next city over.

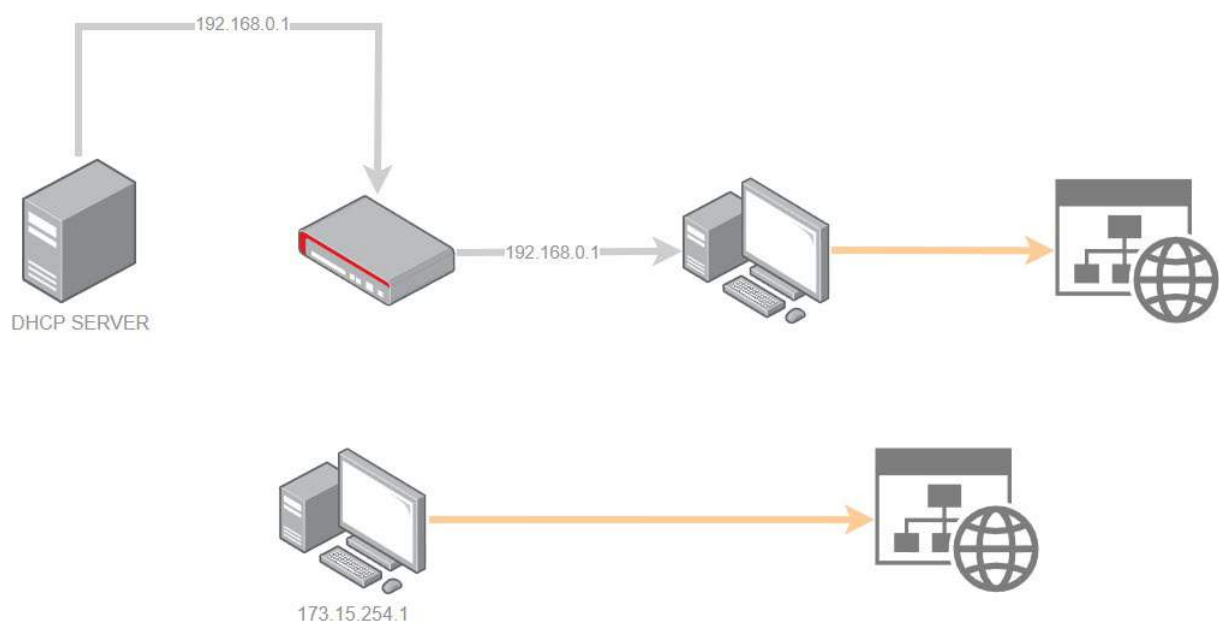


Figure 39 Static IP and DHCP

### 3. NAT

NAT is a technique that allows one or more intra-domain IP addresses to be converted to one or more out-of-domain IP addresses. NAT, also known as Network Address Translation, helps local network addresses (Private) access public networks (Internet). Locations to perform NAT are routers where these two types of networks are connected.

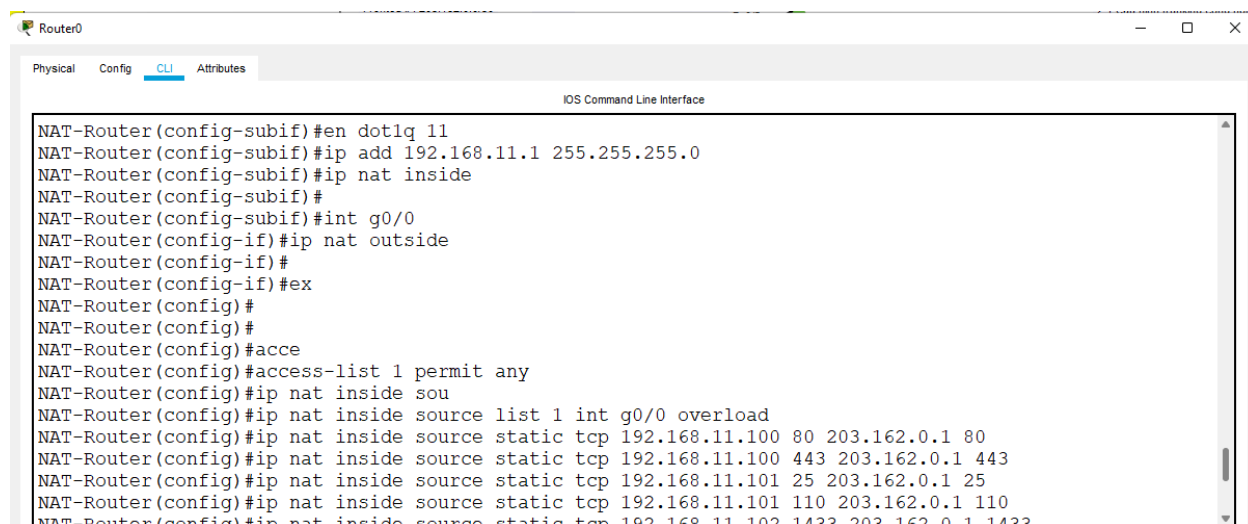
NAT is responsible for transmitting packets from one network layer to another in the same system. NAT will change the IP address inside the packet. Then switch to routers and network devices. NAT can act as a firewall. It helps users secure computer IP information. Specifically, if the computer has trouble connecting to the internet, the public IP address (previously configured) will be displayed instead of the local network IP.

- IP Private: Each device in the local area network (LAN) will have its own IP. Private IPs in the same LAN system can connect to each other through the Router network device, but cannot directly connect to the outside internet. These Private IPs will be converted to Public IP addresses through NAT technology to connect to the outside Internet.
- IP Public: Public IP, also known as an external IP, is a type of address provided by internet service providers such as FPT, VNPT, Viettel, ...

There are 3 types of NAT techniques are put into use such as Static NAT, Dynamic NAT, NAT Overload.

### 3.1. Static NAT (Post-Forwarding)

Static NAT is a technique used to change and turn one IP into another. By using specific fixation method from local IP address to Public. This whole process is done and installed manually. The static NAT method will be especially effective if the devices have a fixed address to access the internet from the outside.

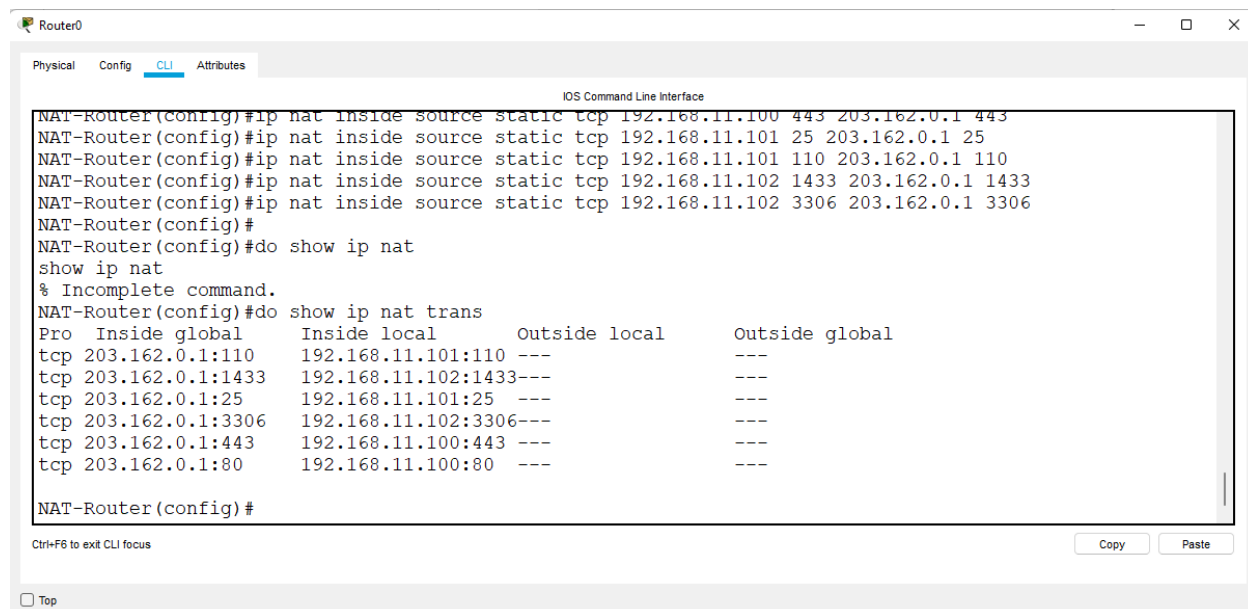


```

NAT-Router(config-subif)#en dot1q 11
NAT-Router(config-subif)#ip add 192.168.11.1 255.255.255.0
NAT-Router(config-subif)#ip nat inside
NAT-Router(config-subif)#
NAT-Router(config-subif)#int g0/0
NAT-Router(config-if)#ip nat outside
NAT-Router(config-if)#
NAT-Router(config-if)#ex
NAT-Router(config)#
NAT-Router(config)#
NAT-Router(config)#acce
NAT-Router(config)#access-list 1 permit any
NAT-Router(config)#ip nat inside sou
NAT-Router(config)#ip nat inside source list 1 int g0/0 overload
NAT-Router(config)#ip nat inside source static tcp 192.168.11.100 80 203.162.0.1 80
NAT-Router(config)#ip nat inside source static tcp 192.168.11.100 443 203.162.0.1 443
NAT-Router(config)#ip nat inside source static tcp 192.168.11.101 25 203.162.0.1 25
NAT-Router(config)#ip nat inside source static tcp 192.168.11.101 110 203.162.0.1 110
NAT-Router(config)#ip nat inside source static tcp 192.168.11.102 1433 203.162.0.1 1433

```

Figure 40 NAT-1



```

NAT-Router(config)#ip nat inside source static tcp 192.168.11.100 443 203.162.0.1 443
NAT-Router(config)#ip nat inside source static tcp 192.168.11.101 25 203.162.0.1 25
NAT-Router(config)#ip nat inside source static tcp 192.168.11.101 110 203.162.0.1 110
NAT-Router(config)#ip nat inside source static tcp 192.168.11.102 1433 203.162.0.1 1433
NAT-Router(config)#ip nat inside source static tcp 192.168.11.102 3306 203.162.0.1 3306
NAT-Router(config)#
NAT-Router(config)#do show ip nat
show ip nat
% Incomplete command.
NAT-Router(config)#do show ip nat trans

```

Pro	Inside global	Inside local	Outside local	Outside global
tcp	203.162.0.1:110	192.168.11.101:110	---	---
tcp	203.162.0.1:1433	192.168.11.102:1433	---	---
tcp	203.162.0.1:25	192.168.11.101:25	---	---
tcp	203.162.0.1:3306	192.168.11.102:3306	---	---
tcp	203.162.0.1:443	192.168.11.100:443	---	---
tcp	203.162.0.1:80	192.168.11.100:80	---	---

```

NAT-Router(config)#

```

Figure 41 NAT-2

### 3.2. Dynamic NAT (One-to-one)

Dynamic NAT is a technique used to automatically map one IP address to another (one-to-one). Normally, Dynamic NAT will convert the local network IP to a valid registered IP address.

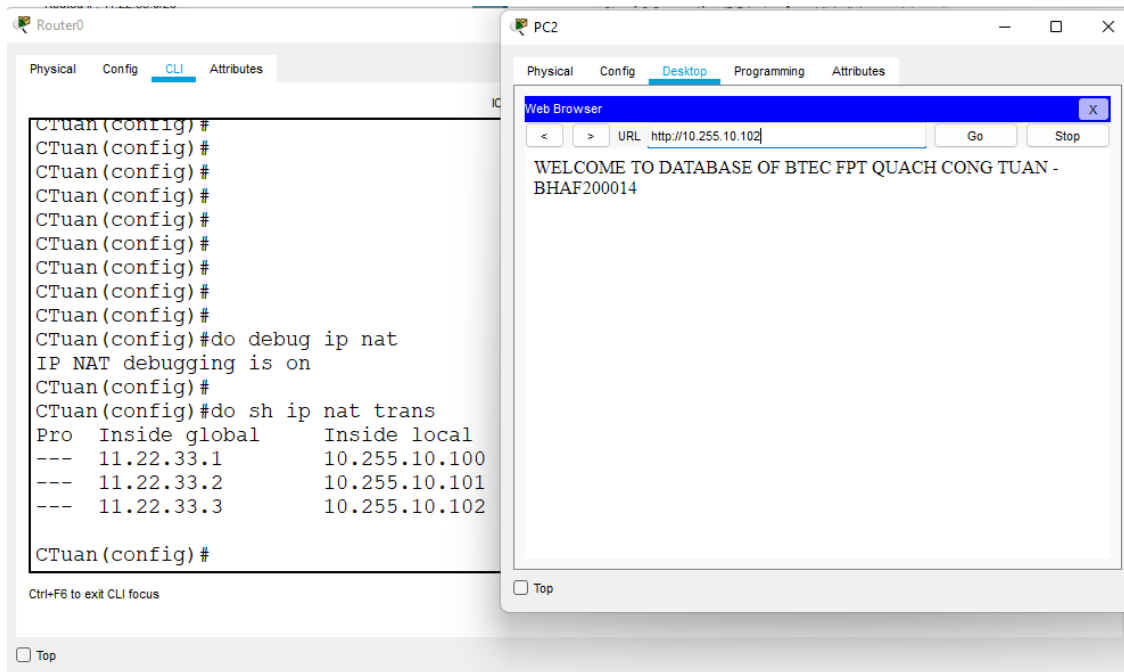
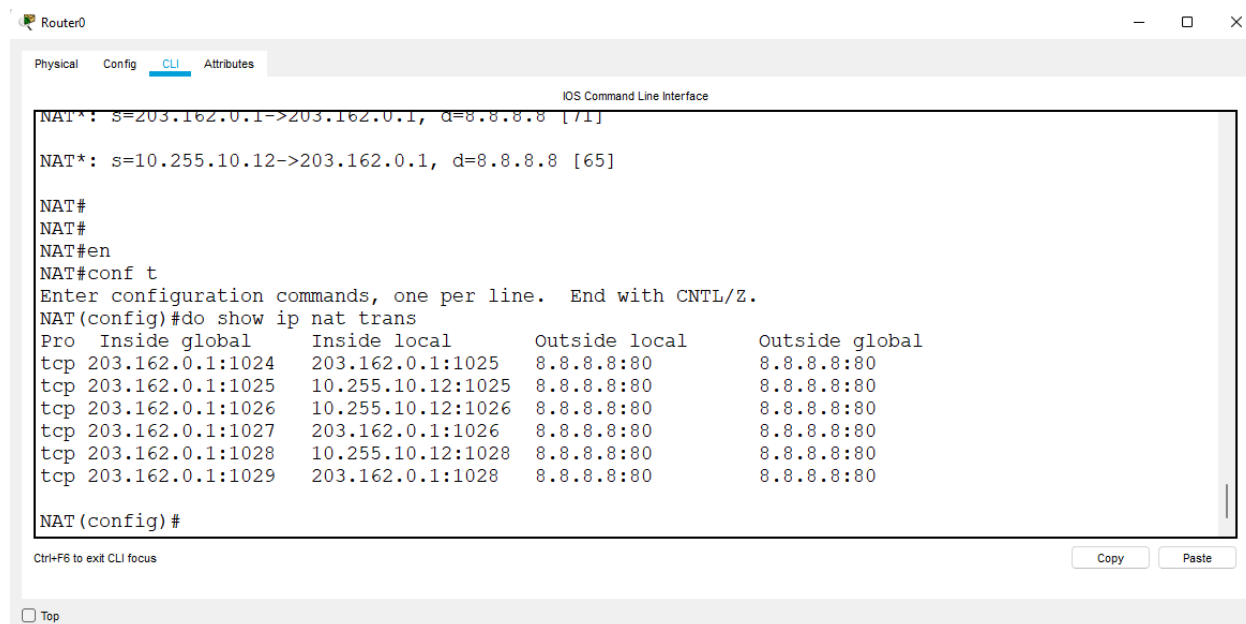


Figure 42 NAT-3

### 3.3. NAT Overload (PAT)

NAT Overload is also known as PAT (Port Address Translation). This is another variation of Dynamic NAT. It also performs automatic IP address conversion. However, the address translation pattern of NAT Overload is many-to-one (mapping multiple IP addresses to 1 IP address) and uses different port numbers to distinguish each conversion.



```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
NAT*: s=203.162.0.1->203.162.0.1, d=8.8.8.8 [71]
NAT*: s=10.255.10.12->203.162.0.1, d=8.8.8.8 [65]
NAT#
NAT#
NAT#en
NAT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
NAT(config)#do show ip nat trans
Pro  Inside global      Inside local      Outside local      Outside global
tcp  203.162.0.1:1024    203.162.0.1:1025  8.8.8.8:80         8.8.8.8:80
tcp  203.162.0.1:1025    10.255.10.12:1025 8.8.8.8:80         8.8.8.8:80
tcp  203.162.0.1:1026    10.255.10.12:1026 8.8.8.8:80         8.8.8.8:80
tcp  203.162.0.1:1027    203.162.0.1:1026 8.8.8.8:80         8.8.8.8:80
tcp  203.162.0.1:1028    10.255.10.12:1028 8.8.8.8:80         8.8.8.8:80
tcp  203.162.0.1:1029    203.162.0.1:1028 8.8.8.8:80         8.8.8.8:80
NAT(config)#
Ctrl+F6 to exit CLI focus
Copy Paste
Top

```

Figure 43 NAT-4



## M1. PROPOSE A METHOD TO ASSESS AND TREAT IT SECURITY RISKS.

Risk assessments are used to identify, estimate, and prioritize hazards that arise from the operation and use of information systems to organizational operations and assets. Risk assessment is essentially a commercial concept that revolves around the concept of money. You must first consider how your firm produces money, how people and assets affect profitability, and what dangers could result in significant financial losses for the company. After that, consider how you may improve your IT infrastructure to limit the risks that could result in the most significant financial losses for the company.

### Establish a risk management framework

RMF, at its most basic level, requires NorthStar to determine which system and data risks we face and to take reasonable steps to reduce them. The RMF divides these goals into six stages, each of which is interconnected but distinct.

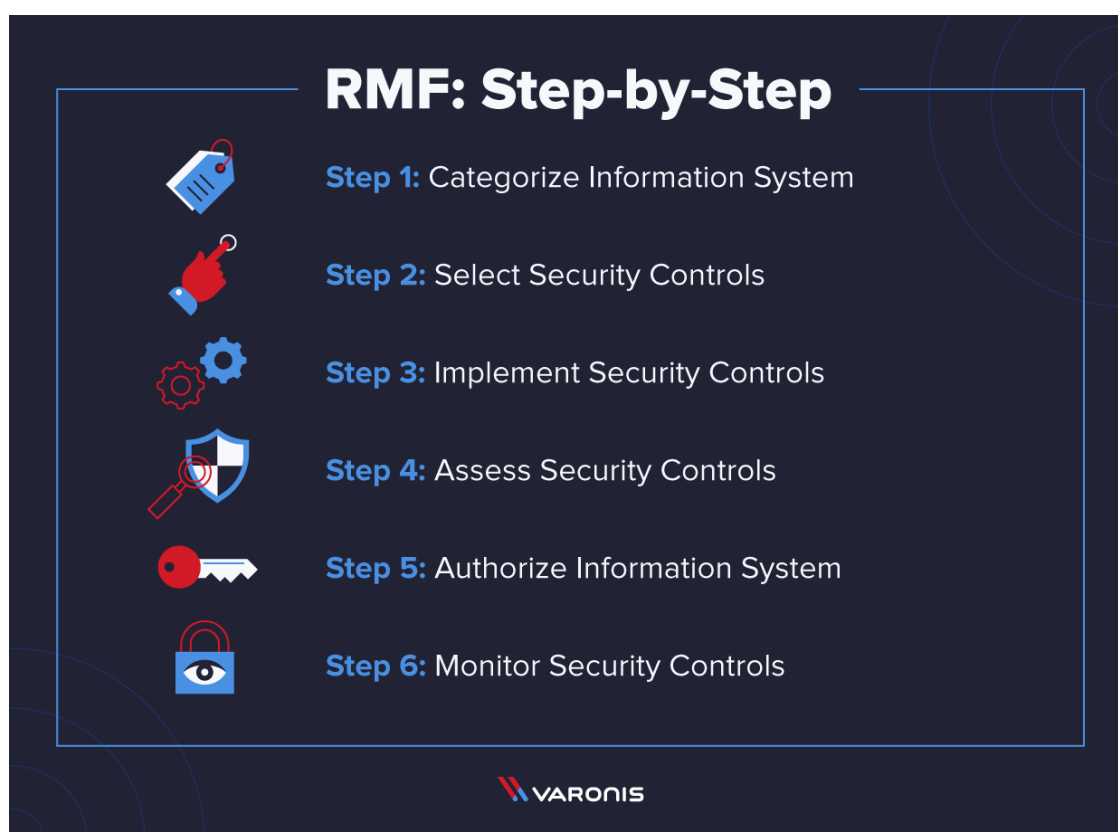


Figure 44 M1

### Identify risks

Determine what financial losses the organization would suffer if a given asset were damaged. Here are some of the consequences you should care about:

- Data loss
- System or application downtime
- Legal consequences

A threat is anything that might exploit a vulnerability to breach your security and cause harm to your assets. Here are some common threats:

- Natural disasters
- System failure
- Accidental human interference
- Malicious human actions (interference, interception or impersonation)

Identify vulnerabilities and assess the likelihood of their exploitation. A vulnerability is a weakness that allows some threat to breach your security and cause harm to an asset.

### Analyze risk

A security risk assessment identifies, assesses, and implements key security controls in applications. It also focuses on preventing application security defects and vulnerabilities.

### Evaluate risk

Administer a method for assessing the security threats that have been discovered for key assets. Determine ways to effectively and efficiently deploy time and resources to risk reduction after comprehensive review and assessment. The association between assets, risks, vulnerabilities, and mitigating controls must be examined using the assessment strategy or methodology.

### Select risk treatment option

Define a mitigation approach and enforce security controls for each risk. Implement tools and processes to minimize threats and vulnerabilities from occurring in firm's resources.

## **M2. DISCUSS THREE BENEFITS TO IMPLEMENT NETWORK MONITORING SYSTEMS WITH SUPPORTING REASONS.**

With today's advancements in information technology, network infrastructure creation requires special attention and consideration. It is necessary to solve performance and security challenges in information technology. We need to upgrade and use routers, switches, virtual servers, wireless devices, and any other sort of device/application that needs to be regularly monitored to ensure that NorthStar's network is always reliable and free of threats. We can detect flaws or threats to the system via monitoring. In addition, we need to put in place certain additional security measures to assist keep the network safe. A network monitoring system is used for this.

Network monitoring has numerous advantages. It's crucial for not only monitoring for problems 24 hours a day, but also for maintaining system performance, ensuring availability, and identifying areas for improvement. Continue reading to learn about five business advantages the North Star can obtain through good network monitoring.

IT infrastructures are becoming more complicated, therefore having a thorough monitoring and security system for my network is critical.

Maintaining the North Star network in good functioning order is critical. This will necessitate a solution with a wide range of capabilities, including an anomaly alert system for administrators. Network management systems can be used by technical employees to provide graphical interfaces, bespoke probes, and detailed status notifications. It is critical to have experts who can examine the network. The following are some of the advantages of network monitoring:

- Benchmarking standard performance
- Effectively allocating resources
- Managing a changing IT environment
- Identifying security threats
- Deploying new technology and system upgrades successfully

### **1. Benchmarking standard performance**

Network monitoring gives you the visibility to benchmark everyday performance and the foresight to pick up on any fluctuations in performance standards; allowing me to pre-emptively identify anomalies. Effective network monitoring empowers IT professionals to recognize early warning signs and rectify potential faults before they become major issues that might cause system downtime.

### **2. Effectively allocating resources**

By understanding the source of problems, IT teams are able to minimize tedious troubleshooting times and put in place proactive measures to ensure the business stays ahead of IT outages. I can fix cracks before they spring a leak.

### **3. Managing a changing IT environment**

Effective monitoring of the network can

- Provide IT teams with a comprehensive inventory of wired and wireless devices
- Enable analysis of long-term trends
- Facilitating optimum use of available assets
- Reduce expenses

### **4. Identifying security threats**

Without network insights, addressing persistent security threats every day can be extremely time-consuming for an IT team. Maintaining continued IT network security requires that:

- Security patches are continually updated
- Standardized security settings on all the individual workloads are maintained

Therefore, network monitoring will aid an IT team's ability to properly protect a company's data and systems.

### **5. Deploying new technology and system upgrades successfully**

With network monitoring, IT teams are able to gain historic insight into how equipment has performed over time and, with trend analysis, are able to determine if current technology can scale to meet business needs.

This allows IT staff to

- Create a clear picture of how able the network is to support the launch of new technology
- Mitigate any risks associated with a major change by monitoring performance
- Easily demonstrate ROI by providing pre- and post-performance metrics

Here are some tools used to monitor network logic:

### PAESSLER PRTG Network Monitor

Integrated technologies PRTG monitors the entire IT infrastructure. All-important technologies are supported:

- SNMP: ready-to-use and custom options
- WMI and Windows Performance Counters
- SSH: for Linux/Unix and macOS systems
- Traffic analysis using flow protocols or packet sniffing
- HTTP requests
- REST APIs returning XML or JSON
- Ping, SQL, and many more

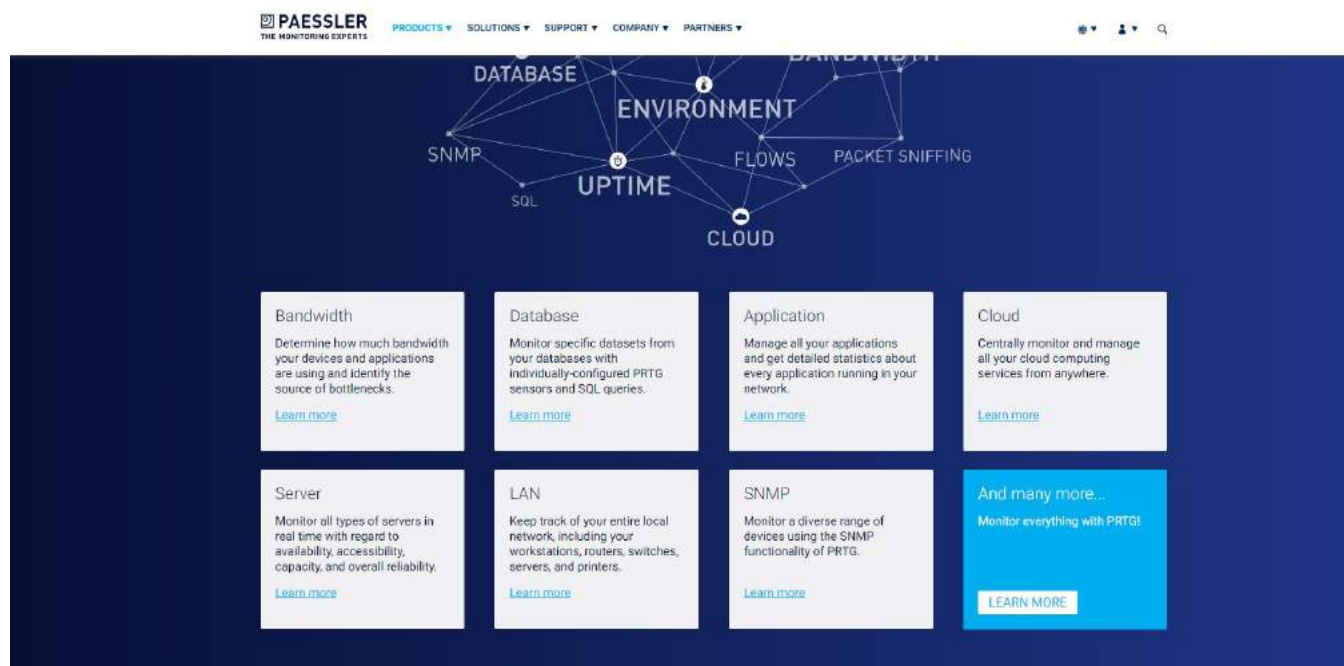


Figure 45 Tool Network Monitoring

## WIRE SHARK Network Monitor

Wireshark is a network protocol analyzer that is widely used around the world. It's the de factor standard across many commercial and non-profit organizations, government agencies, and educational institutions because it allows you to observe what's going on your network at a microscopic level. Wireshark development continues thanks to the volunteer contributions of networking specialists from all around the world, and is a continuation of Gerald Combs' 1998 initiative.

- The following are some of the features available in Wireshark:
- Hundreds of protocols have been thoroughly examined, with more being added all the time.
- Capture in real time and analysis later
- Packet browser with three panes as standard
- Multi-platform: Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and more operating systems are supported.
- The TTY-mode or a GUI can be used to browse the network data that has been captured. Sharks are really useful.
- The industry's most powerful display filters and detailed VoIP research.
- Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and other protocols can all be used to read live data (depending on your platform)
- Many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA, provide decryption capability.

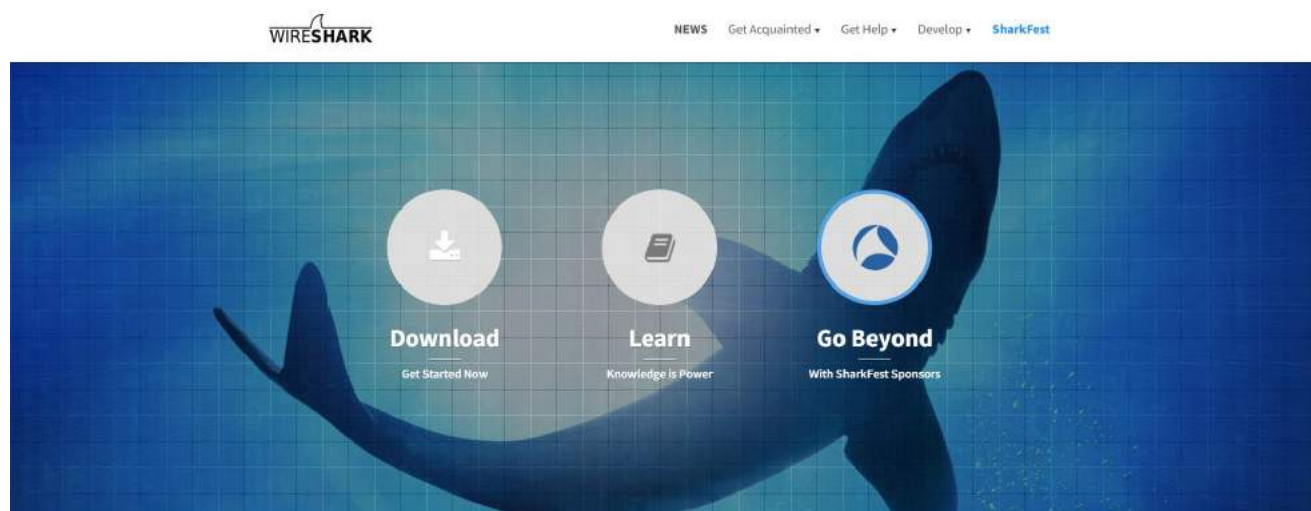


Figure 46 Wireshark



Figure 47 Slide

## Table of Content

# Introduction

In this assignment, I was assigned as a Trainee Security Specialist and Head of Security at NorthStar Secure Company. I will have to design a presentation so that they can train new employees in tools and techniques that support research and defense against information security threats with the organization's protection activities business-critical data and devices.

**P1.** IDENTIFY TYPES OF SECURITY RISKS TO ORGANIZATIONS.

**P2.** DESCRIBE ORGANIZATIONAL SECURITY PROCEDURES FOR NORTHSTAR.

**P3.** IDENTIFY THE POTENTIAL IMPACT TO ITS SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND THIRD-PARTY VPN.

**P4.** SHOW, USING AN EXAMPLE FOR EACH, HOW IMPLEMENTING A DMZ, STATIC IP, AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY.

**M1.** PROPOSE A METHOD TO ASSESS AND TREAT IT SECURITY RISKS.

**M2.** DISCUSS THREE BENEFITS TO IMPLEMENTING NETWORK MONITORING SYSTEMS WITH SUPPORTING REASONS.

**D1.** INVESTIGATE HOW A 'TRUSTED NETWORK' MAY BE PART OF AN IT SECURITY SOLUTION

Figure 48 Slide 2



P1

# IDENTIFY TYPES OF SECURITY RISKS TO ORGANIZATIONS

Figure 49 Slide 3



P1

## THREATS

A new or recently found occurrence that has the potential to harm a system or your firm as a whole is referred to as a threat. Threats can be divided into three groups:

- Floods, hurricanes, and tornadoes are all-natural disasters.
- Threats that are unintentional, such as an employee accessing incorrect information.
- Spyware, malware, adware firms, or the activities of a disgruntled employee are all examples of intentional dangers.

Figure 50 Slide P1



P1

# VULNERABILITY

A vulnerability is a recognized weakness in an asset (resource) that one or more attackers can exploit. To put it another way, it's a well-known flaw that permits an assault to succeed.



Figure 51 Slide P1



P1

# RISKS

When a danger exploits a vulnerability, the risk is defined as the possibility of loss or damage. Risk can also be calculated using the formula:  

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}.$$

Figure 52 Slide P1

# MALWARE

Malware refers to a variety of malicious software, such as viruses, ransomware, and spyware. Malware, short for malicious software, is a type of code created by cyberattacks with the goal of causing substantial data and system damage or gaining unauthorized network access. Malware is usually distributed via email as a link or a file, and it requires the user to click on the link or open the file in order for it to be executed.

Figure 53 Slide P1 Malware

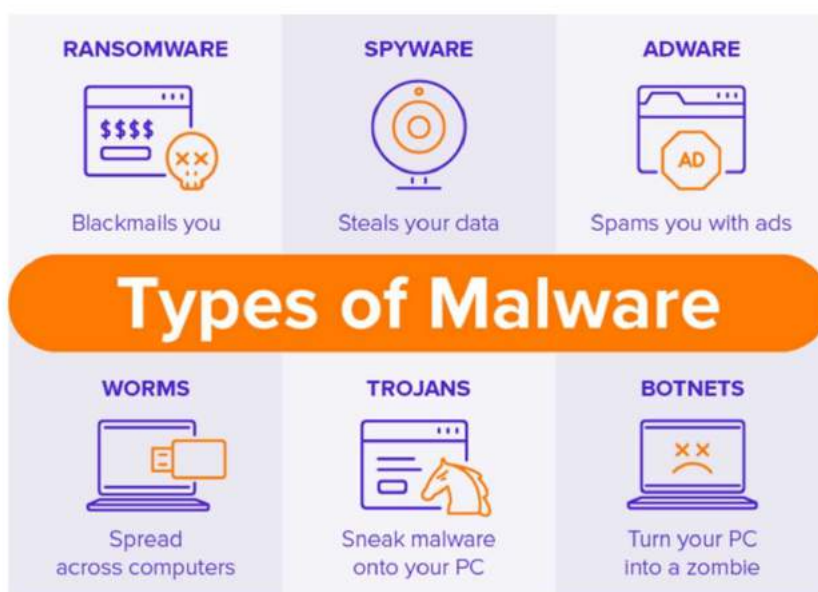


Figure 54 Slide P1 Malware

# SOCIAL ENGINEERING ATTACKS

The term "social engineering" refers to a variety of malevolent operations that are carried out through human relationships. It manipulates users' minds to make them make security mistakes or reveal important information.

Figure 55 Slide P1 SEA

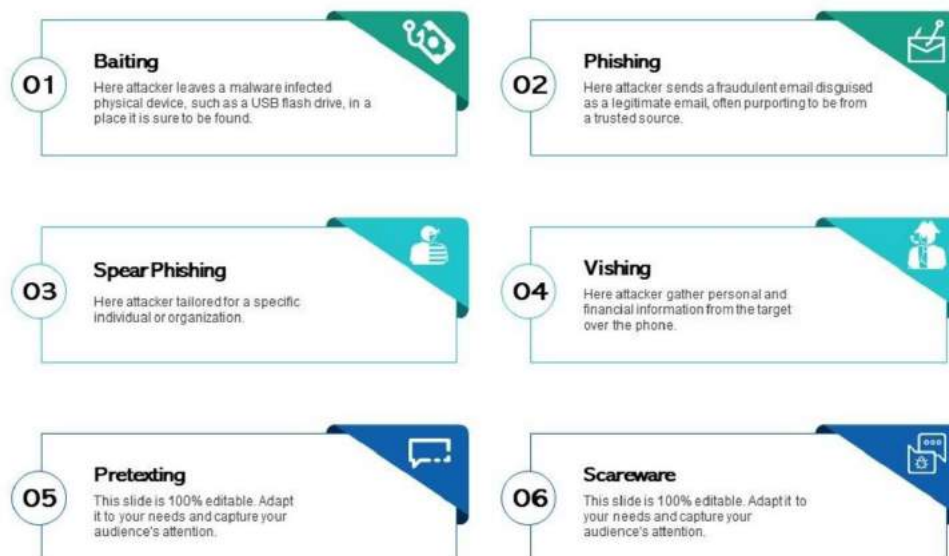


Figure 56 Slide P1 SEA

# WEB APPLICATION ATTACKS

Any attempt by a malicious actor to undermine the security of a Web-based application is referred to as a Web application attack. Web application attacks can either target the application itself in order to get access to sensitive data, or they can use the application as a staging area for attacks against the program's users.

Figure 57 Slide P1 WAA

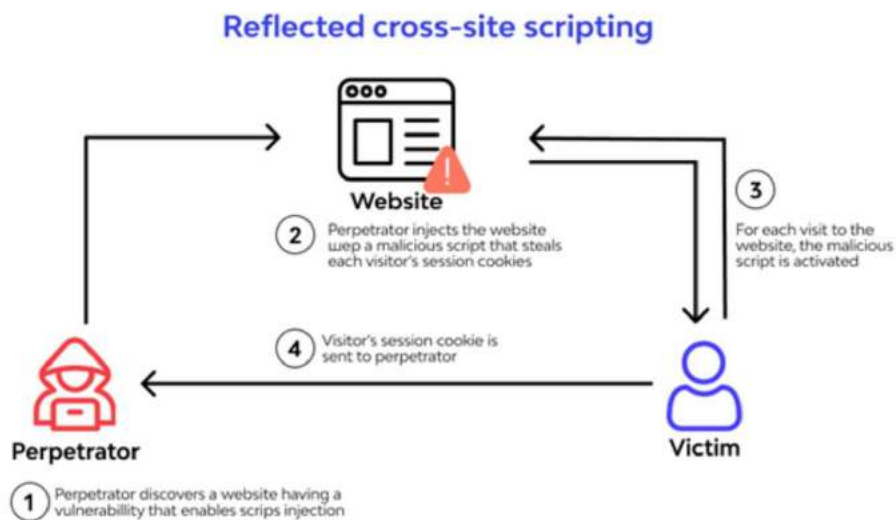


Figure 58 Slide P1 WAA

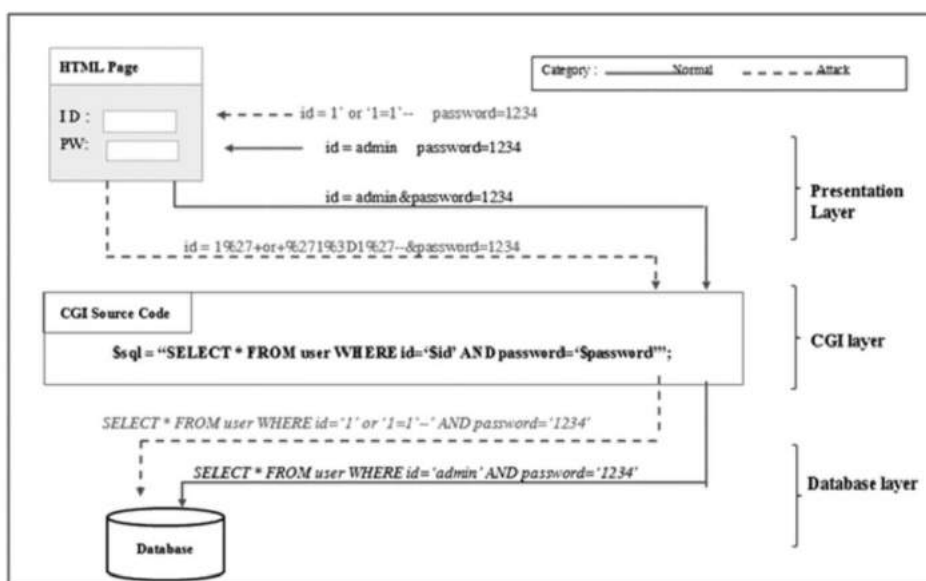


Figure 59 Slide P1 SQL

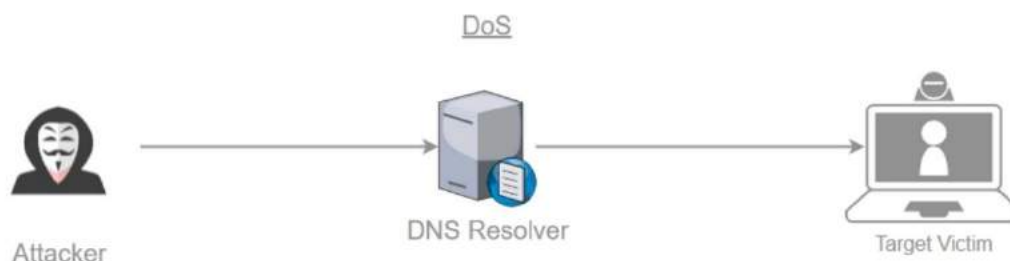


Figure 60 Slide P1 DOS

# NETWORKING BASED ATTACKS

Network-based attacks eavesdrop on, intercept, and manipulate network communications to compromise network security. These can be active assaults, in which the hacker changes network activity in real-time, or passive attacks, in which the attacker observes network activity but does not attempt to change it.

Figure 61 Slide P1 NBA

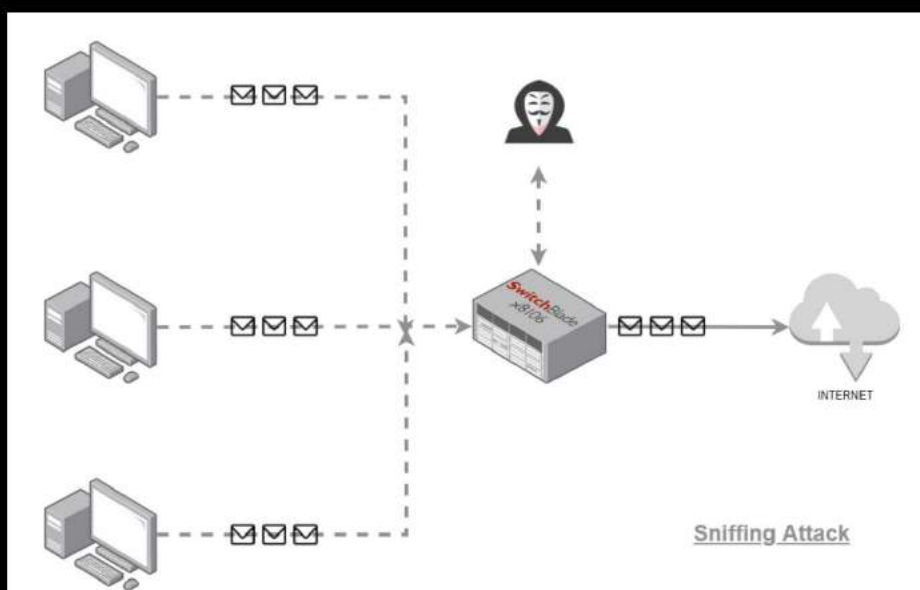


Figure 62 Slide P1 NBA



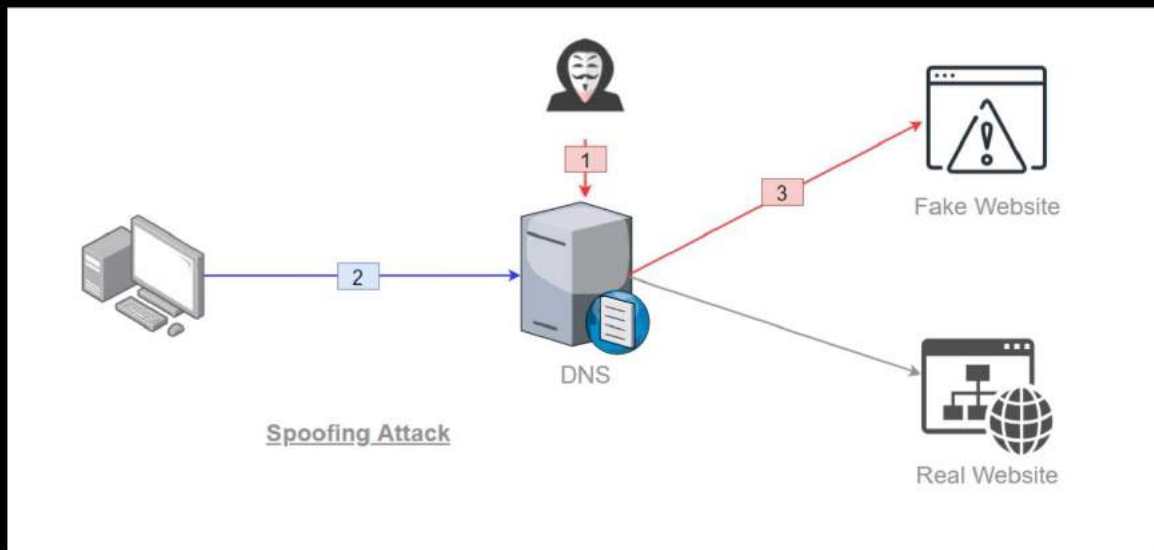


Figure 63 Slide P1 NBA

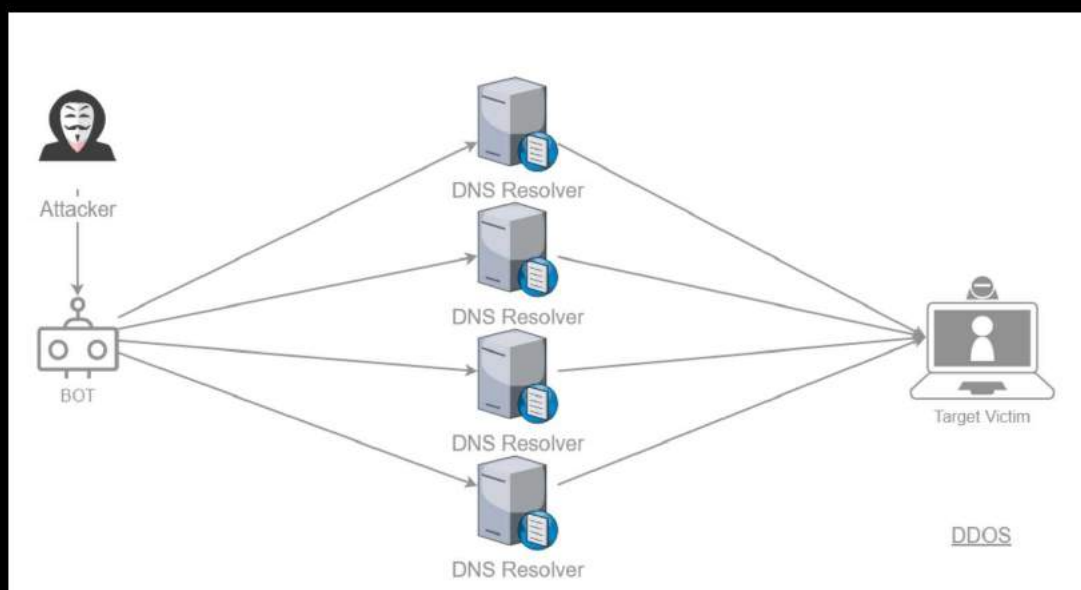


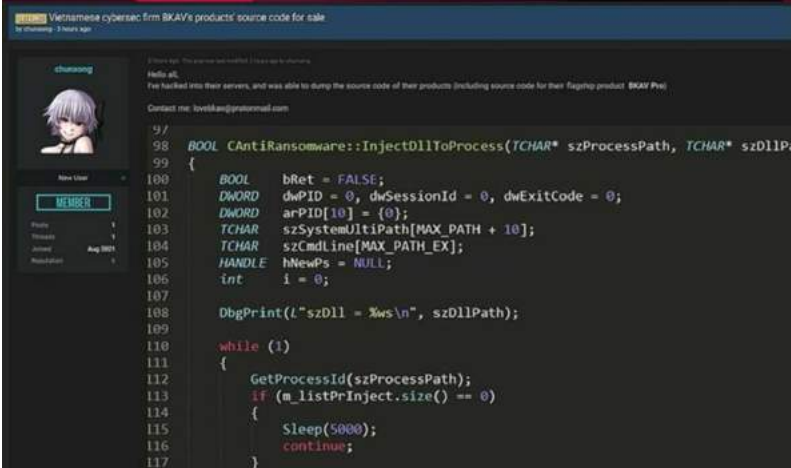
Figure 64 Slide P1 NBA

## Prevention Risk

I have given a security method for this project of NorthStar company this time, we need to set up a copyrighted anti-virus program, constantly updating the database. In addition, personal information needs to be confidential. NorthStar's system needs to decentralize users with security policies and procedures such as 2FA/MFA identity authentication. Prevent unauthorized applications (crack). Continuously back up data to the backup system to avoid risks. Use a firewall for websites, install the "Chống Lừa Đảo" extension to prevent fraudulent websites.

Figure 65 Slide P1 Prevention

# Example



As noted on August 4, 2021, at the \*\*\*\* Raid Forum, part of the internal data and source code of BKAV anti-virus software was posted by a hacker with the alias "Chunxong". This hacker said he had infiltrated the server of this security firm BKAV and successfully extracted the source code of the anti-virus software developed by this company. In addition, this member also posted a lot of information about other internal projects of BKAV.

Figure 66 Slide P1 Example



P2

# DESCRIBE ORGANIZATIONAL SECURITY PROCEDURES FOR NORTHSTAR.

Figure 67 Slide P2

P2

## Definition

Procedures can be defined as a particular course or mode of action. They describe an act or manner of proceedings in any action or process. The procedures explain the processes required in requesting USERIDs, password handling, and destruction of information. The procedures for requesting USERIDs or access changes will be conducted in the future via E-mail with easy-to-use templates that prompt the requester for all the information required. Requests can be expedited in a matter of minutes providing greater productivity for all concerned.

Figure 68 Slide P2 Definition



P2

## Authentication

The process of ascertaining whether someone or something is who or what it claims to be is known as authentication. Authentication technology checks if a user's credentials match those in a database of authorized users or a data authentication server to offer access control for systems. SFA, which requires a user ID and password, or 2FA, which requires a user ID, password, and biometric signature, are just two examples of authentication factors. Multifactor authentication is defined as the use of three or more identity verification factors for authentication, such as a user ID and password, a biometric signature, and maybe a personal question that the user must answer.

Figure 69 Slide P2 -1

P2

## Anti-Virus

Software designed to assist in the detection, prevention, and removal of malware (malicious software). Antivirus software is used to protect computers from viruses by scanning, detecting, and removing them. Most antivirus software operates in the background once installed, providing real-time protection against virus attacks. Comprehensive virus protection systems guard your files and hardware against malware like worms, Trojan horses, and spyware, and may also include features like customized firewalls and website blocking



Figure 70 Slide P2 -2

P2



# Cloudflare

Cloud Firewalls are software-based network devices that are deployed in the cloud and are designed to prevent or mitigate unauthorized access to private networks. They are developed for modern business needs and sit within web application settings as a new technology.

Figure 71 Slide P2 -3

P2

# Employee Training

Quality security training reduces the anxiety and uncertainty associated with typical online risks, resulting in a workforce that is more skilled, confident, and educated. As human error lowers, productivity will grow, and staff will be better positioned to identify and respond to security threats as they develop. This also relieves pressure on your IT department, allowing them to concentrate on more critical security issues and methods to improve your present security solutions.



Figure 72 Slide P2 -4



Figure 73 Slide P3



P3

## Firewall

A firewall is a network security system that filters incoming and outgoing network traffic according to a set of user-defined rules. The goal of a firewall, in general, is to minimize or remove undesired network communications while allowing all authorized communication to pass freely. Firewalls are an important layer of security in most server infrastructures that, when paired with other measures, prevent intruders from gaining unwanted access to your servers. The following are the five types of firewalls:

- Packet Filtering Firewall
- Circuit-Level Gateway
- Application-Level Gateway (Aka Proxy Firewall)
- Stateful Inspection Firewall
- Next-Generation Firewall (NGFW)

Figure 74 Slide P3 Firewall



P3

# IDS

The INTRUSION Detection System (IDS) is a network traffic monitoring system that detects anomalies, unauthorized activities, and systems. IDS can distinguish between internal (internal) or external attacks. IDS detection is based on specific indications of known risks (in the same way that antivirus software relies on special signs for detection and antivirus) or on comparing current network traffic with baseline (system-standard measurements that are acceptable right now) to find other signs often.

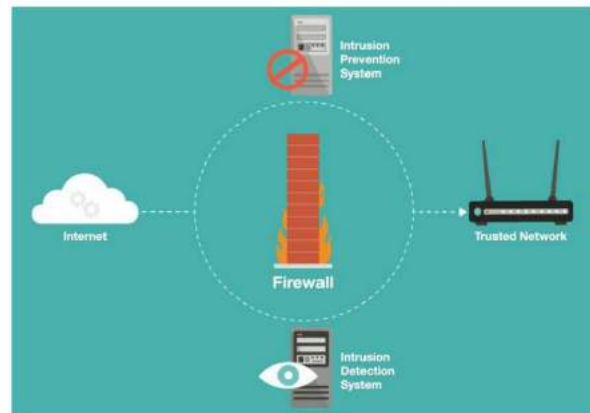


Figure 75 Slide P3 IDS

P4

**SHOW, USING AN EXAMPLE FOR EACH, HOW IMPLEMENTING A DMZ, STATIC IP AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY.**

Figure 76 Slide P4

P4

## DMZ

A DMZ Network is a perimeter network that protects an organization's internal local-area network from untrusted traffic and adds an extra degree of security. A DMZ is a subnetwork that connects the public internet to private networks. The purpose of a DMZ is to allow an organization to connect to untrusted networks, such as the internet, while maintaining the security of its private network or LAN. External-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, are often stored in the DMZ. DMZ networks have played a critical role in protecting global commerce.

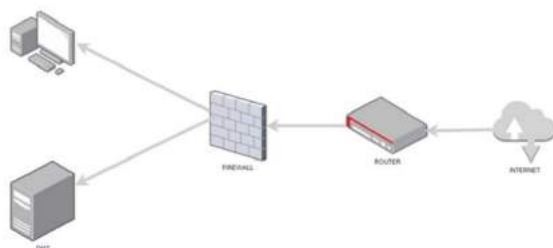


Figure 77 Slide P4 DMZ

P4

## STATIC IP

**IP Address:** An IP address is a unique number assigned to every device on a TCP/IP network. Just like your physical home address lets people know where to send your birthday card, IP addresses identify computers and devices and let them communicate with each other.

**Static IP Address:** A static IP address is simply an address that doesn't change. Once your device is assigned a static IP address, that number typically stays the same until the device is decommissioned or your network architecture changes. Static IP addresses generally are used by servers or other important equipment.

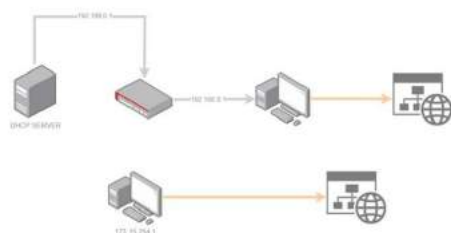


**Dynamic IP Address:** As the name suggests, dynamic IP addresses are subject to change, sometimes at a moment's notice. Dynamic addresses are assigned, as needed, by Dynamic Host Configuration Protocol (DHCP) servers.

Figure 78 Slide P4 Static IP

P4

# STATIC IP WITH BENEFIT



- Better DNS support: Static IP addresses are much easier to set up and manage with DNS servers.
- Server hosting: If you are hosting a web server, email server, or any other kind of server, having a static IP address makes it easier for customers to find you via DNS. Practically speaking that means it's quicker for clients to get to your websites and services if they have a static IP address.
- Convenient remote access: A static IP address makes it easier to work remotely using a Virtual Private Network (VPN) or other remote access programs.
- More reliable communication: Static IP addresses make it easier to use Voice over Internet Protocol (VoIP) for teleconferencing or other voice and video communications.
- More reliable geolocation services: With a static IP address, services can match the IP address with its physical location. For example, if you use a local weather service with a static IP address, you're more likely to get the weather report you need instead of the one for the next city over.

Figure 79 Slide P4

P4

# NAT

NAT gates hide individual IP addresses by allowing numerous devices with different network addresses to connect to the internet using a single IP address. As a result, attackers scanning a network for IP addresses are unable to collect detailed details, resulting in increased security. In the same way that proxy firewalls function as an intermediate between a group of computers and outside traffic, NAT firewalls do the same. Some of the advantages of having a NAT are as follows:

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

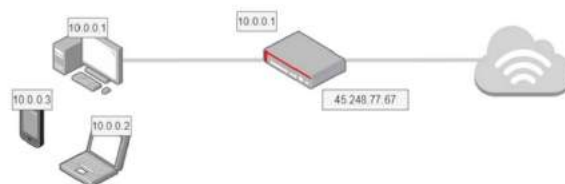
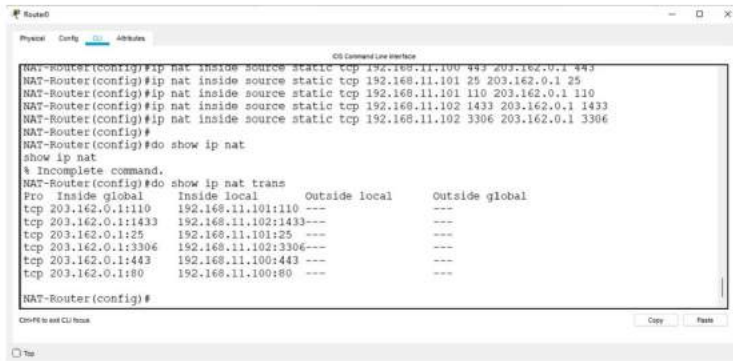


Figure 80 Slide P4 NAT

# Static NAT

Static NAT is a technique used to change and turn one IP into another. By using a specific fixation method from local IP address to Public. This whole process is done and installed manually. The static NAT method will be especially effective if the devices have a fixed address to access the internet from the outside.



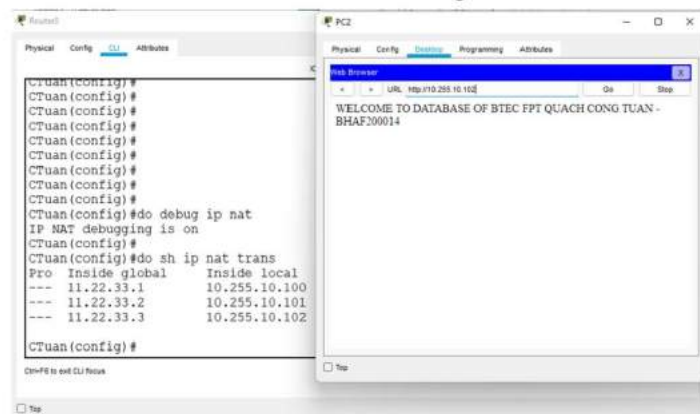
```

NAT-Router(config)#ip nat inside source static tcp 192.168.11.100 80 203.162.0.1 80
NAT-Router(config)#ip nat inside source static tcp 192.168.11.101 25 203.162.0.1 25
NAT-Router(config)#ip nat inside source static tcp 192.168.11.102 110 203.162.0.1 110
NAT-Router(config)#ip nat inside source static tcp 192.168.11.102 1433 203.162.0.1 1433
NAT-Router(config)#ip nat inside source static tcp 192.168.11.102 3306 203.162.0.1 3306
NAT-Router(config)#
NAT-Router(config)#do show ip nat
show ip nat
% Incomplete command.
NAT-Router(config)#do show ip nat trans
Pro Inside global Inside local Outside local Outside global
tcp 203.162.0.1:110 192.168.11.101:110 --- ---
tcp 203.162.0.1:1433 192.168.11.102:1433 --- ---
tcp 203.162.0.1:25 192.168.11.101:25 --- ---
tcp 203.162.0.1:3306 192.168.11.102:3306 --- ---
tcp 203.162.0.1:443 192.168.11.100:443 --- ---
tcp 203.162.0.1:80 192.168.11.100:80 --- ---
NAT-Router(config)#
  
```

Figure 81 Slide P4 Static NAT

# Dynamic NAT

Dynamic NAT is a technique used to automatically map one IP address to another (one-to-one). Normally, Dynamic NAT will convert the local network IP to a valid registered IP address.



```

CTuan(config)#
CTuan(config)#
CTuan(config)#
CTuan(config)#
CTuan(config)#
CTuan(config)#
CTuan(config)#
CTuan(config)#do debug ip nat
IP NAT debugging is on
CTuan(config)#
CTuan(config)#do sh ip nat trans
Pro Inside global Inside local
--- 11.22.33.1 10.255.10.100
--- 11.22.33.2 10.255.10.101
--- 11.22.33.3 10.255.10.102
CTuan(config)#
  
```

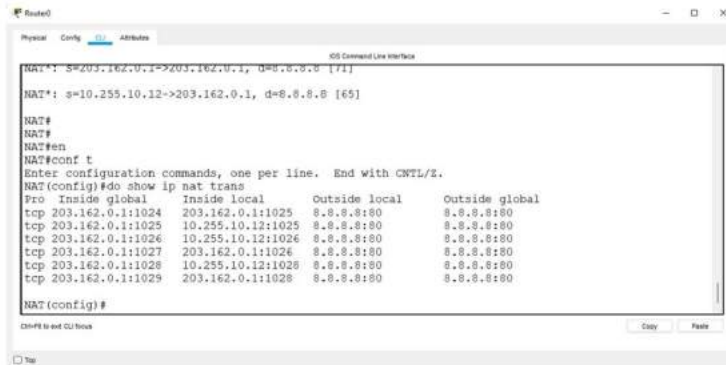
PC2 Web Browser: <http://10.255.10.102>  
WELCOME TO DATABASE OF BTEC FPT QUACH CONG TUAN - BHAF200014

Figure 82 Slide P4 Dynamic NAT



# NAT Overload

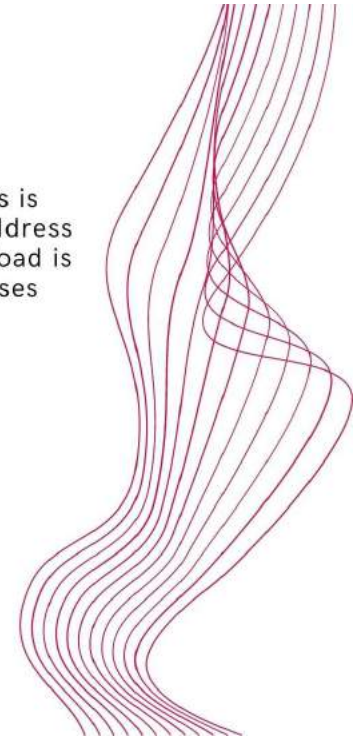
NAT Overload is also known as PAT (Port Address Translation). This is another variation of Dynamic NAT. It also performs automatic IP address conversion. However, the address translation pattern of NAT Overload is many-to-one (mapping multiple IP addresses to 1 IP address) and uses different port numbers to distinguish each conversion.



```

Router#
Router(config)#
Router(config)#ip nat pool NAT_POOL 203.162.0.1 203.162.0.1 netmask 255.255.255.0 [74]
Router(config)#ip nat inside source list 10 pool NAT_POOL overload
Router(config)#
Router#
Router#show ip nat trans
NAT* s=10.255.10.12->203.162.0.1, d=8.8.8.8 [65]
NAT#
NAT#
NAT#en
NAT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
NAT(config)#do show ip nat trans
Pro Inside global Inside local Outside local Outside global
tcp 203.162.0.1:1024 203.162.0.1:1025 8.8.8.8:80 8.8.8.8:80
tcp 203.162.0.1:1025 203.162.0.1:1026 8.8.8.8:80 8.8.8.8:80
tcp 203.162.0.1:1026 203.162.0.1:1027 8.8.8.8:80 8.8.8.8:80
tcp 203.162.0.1:1027 203.162.0.1:1028 8.8.8.8:80 8.8.8.8:80
tcp 203.162.0.1:1028 203.162.0.1:1029 8.8.8.8:80 8.8.8.8:80
NAT(config)#
  
```

Figure 83 Slide P4 NAT Overload



## CONCLUSIONS

In this assignment, I gave my personal views on secure networks. At P1, I explained the types of security risks related to how to infiltrate and attack the network security system such as malware, SQL Injection and I gave some illustrative examples of the company BKAV was hacked company-wide database in 07/2021. Continuing in P2 I solved and described the security procedure with the elements that need to be included to improve the security of the system. In section P3 I also explained the definition of firewall and VPN, then I covered the types and analyzed the benefits and risks of misconfiguration. In P4 I explain more about DMZ, Static IP, and NAT to show their benefits in improving network security. With sections M1, M2 and D1 I gave my personal opinion and further analyzed the benefits, factors and investigated the reliability of the network.

## REFERENCES

Anon., 2021. *What is a Firewall?*. [Online]

Available at: <https://www.forcepoint.com/cyber-edu/firewall>

[Accessed 05 November 2021].

Avast, 2021. *What is a static IP address?*. [Online]

Available at: <https://www.avast.com/c-static-vs-dynamic-ip-addresses>

[Accessed 05 November 2021].

Cloudflare, 2021. *What is a cloud firewall? What is firewall-as-a-service (FWaaS)?*. [Online]

Available at: <https://www.cloudflare.com/learning/cloud/what-is-a-cloud-firewall/>

[Accessed 05 November 2021].

Comptia, 2019. *What Is NAT?*. [Online]

Available at: <https://www.comptia.org/content/guides/what-is-network-address-translation>

[Accessed 05 November 2021].

Fortinet, 2020. *What is a DMZ Network?*. [Online]

Available at: <https://www.fortinet.com/resources/cyberglossary/what-is-dmz>

[Accessed 05 November 2021].

Imperva, 2020. *Social Engineering*. [Online]

Available at: <https://www.imperva.com/learn/application-security/social-engineering-attack/>

[Accessed 30 October 2021].

John J. Fay, D. P., 2018. *Security Procedure*. [Online]

Available at: <https://www.sciencedirect.com/topics/computer-science/security-procedure>

[Accessed 05 November 2021].

Johnson, R., 2019. *Top 5 Network Security Risks And Threats*. [Online]

Available at: <https://cybersecurityventures.com/top-5-network-security-risks-and-threats/>

[Accessed 30 October 2021].

Network Monitoring System, 2021. *Basics of Network Monitoring*. [Online]

Available at: <https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html>

[Accessed 05 November 2021].

Netwrix, 2021. *Information Security Risk Assessment Checklist*. [Online]

Available at: [https://www.netwrix.com/information\\_security\\_risk\\_assessment\\_checklist.html](https://www.netwrix.com/information_security_risk_assessment_checklist.html)

[Accessed 05 November 2021].

Quy, L., 2021. *Hacker attacked Bkav from a basic error*. [Online]

Available at: <https://vnexpress.net/hacker-da-tan-cong-bkav-tu-mot-loi-co-ban-4341131.html>

[Accessed 05 November 2021].

Shea, S., 2018. *What is cybersecurity?*. [Online]

Available at: <https://searchsecurity.techtarget.com/definition/cybersecurity>

[Accessed 05 November 2021].

Synopsys, 2020. *Security Risk Assessment*. [Online]

Available at: <https://www.synopsys.com/glossary/what-is-security-risk-assessment.html>

[Accessed 05 November 2021].

Touhid, 2019. *Common Types of Security Threats to Organizations*. [Online]

Available at: <https://cyberthreatportal.com/types-of-security-threats-to-organizations/#:~:text=There%20are%20different%20types%20of%20security%20threats%20to,Worm%206.%20Denial-of-Service%20%28DoS%29%20Attacks%207.%20Phishing%208.>

[Accessed 30 October 2021].

Verizon, 2020. *Antivirus*. [Online]

Available at:

<https://www.verizon.com/info/definitions/antivirus/#:~:text=Antivirus%20is%20a%20kind%20of,time%20protection%20against%20virus%20attacks.>

[Accessed 05 November 2021].

Verizon, 2021. *Spamfilters*. [Online]

Available at: <https://www.verizon.com/info/definitions/spamfilter/>

[Accessed 05 November 2021].