

**NATIONAL ALUMINIUM COMPANY LIMITED**

**NALCO BHAWAN,BHUBANESHWAR**

**A**

**PROJECT   
REPORT ON**

**CYBER SECURITY AND ACTIVE WINDOWS DIRECTORY**

**IN PARTIAL FULLFILLMENT FOR**

**THE AWARD OF DEGREEOF**

**BACHELOR IN COMPUTER SCIENCE AND COMMUNICATION ENGINEERING**

**ACKNOWLEDGEMENT**

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many. I would like to extend my sincere thanks to all of them. I would like to express my gratitude towards my parents for their kind co-operations and encouragement which helped me in the completion of this project. I would like to express my special gratitude to my friends also, as they provide me information as well as pictures they provided. I express my deep sense of gratitude to my Project Guide Mr.Roshan Chaudhury for his expert guidance and support, constant supervision, stimulating discussions as well continuous impetus throughout the period of this project. My thanks and appreciations also go to my colleagues in developing the project and people who have willing helped me out in any ways in the making of this project.

**DECLARATION**

I, Deepak Patnaik student of B. Tech, 2nd Semester hereby declare that PROJECT REPORT on Cyber Security and Active Windows Directory which is submitted by me to the Systems Department, NALCO, Bhubaneshwar, Odisha, is in partial fulfillment of requirement for the Award of the Degree of "Bachelor of Technology" in COMPUTER SCIENCE AND COMMUNICATION ENGINEERING.

Signature

Deepak Patnaik

Date: 4th July 2022

B tech - Computer Science And Communication Engineering

2nd Semester

Roll number: 2029124

KIIT University

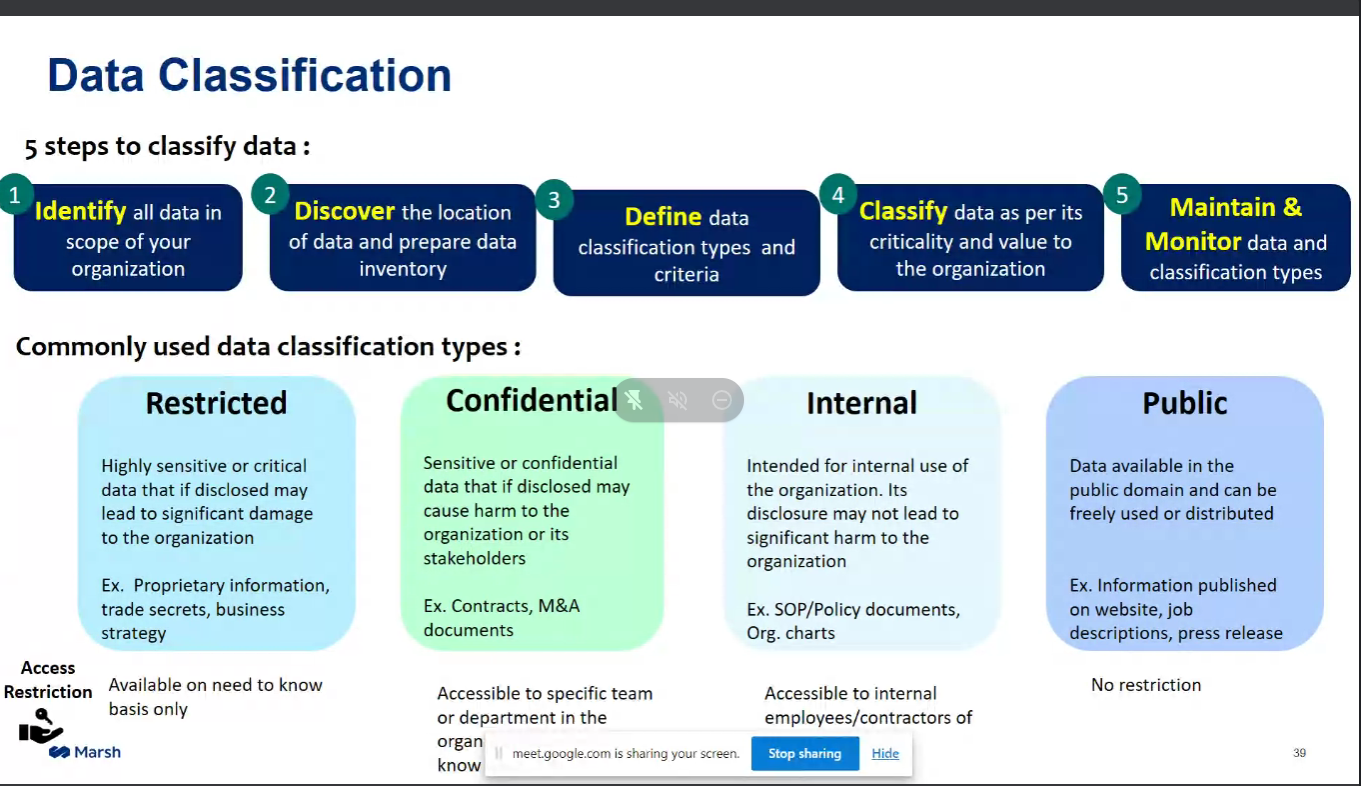
Bhubaneshwar, Odisha

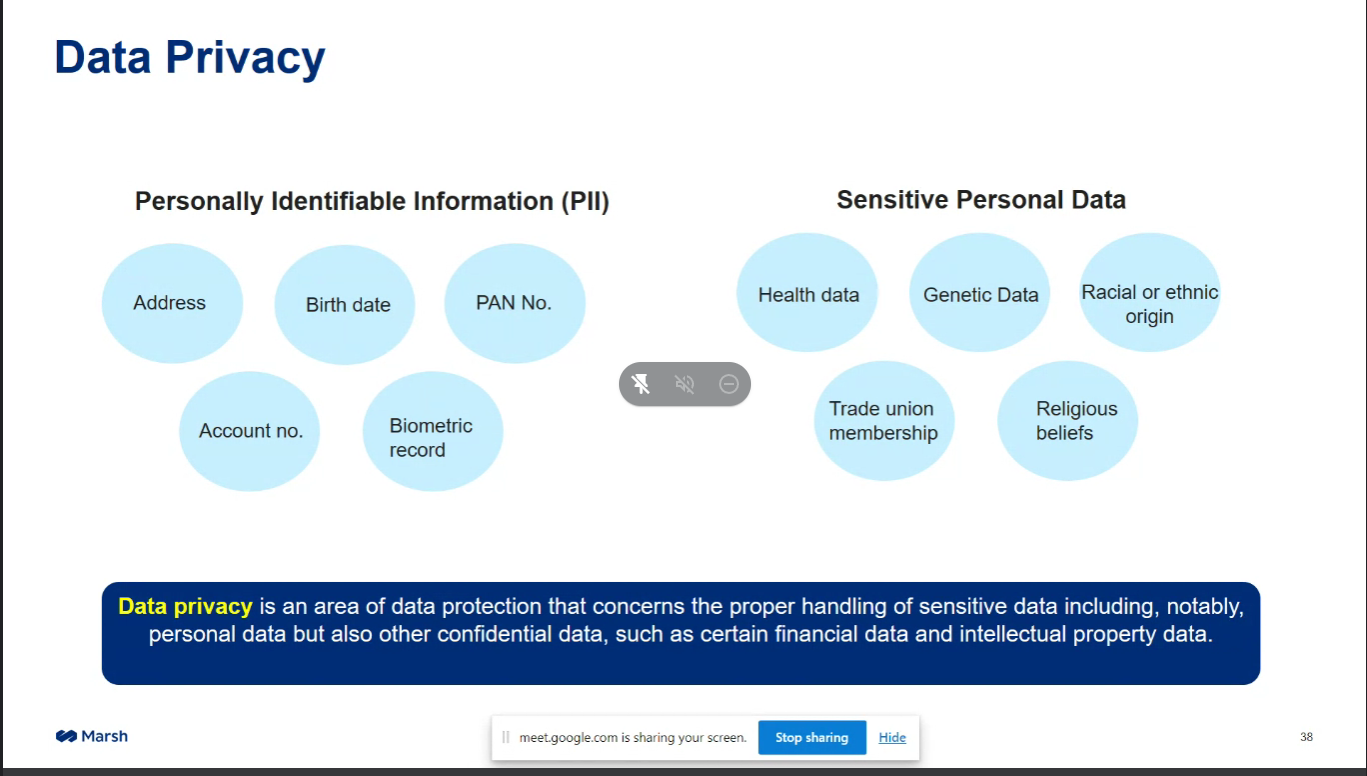
**CERTIFICATE**

On the basis of declaration submitted by Mr. DEEPAK PATNAIK, student of B.Tech , Roll Number 2029124, 2nd Semester from KIIT University. I hereby certify that The Project On CYBER SECURITY AND ACTIVE WINDOWS DIRECTORY is submitted to SYSTEMS DEPARTMENT, National Aluminium Company Ltd., Angul, Odisha, in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in COMPUTER SCIENCE AND COMMUNICATION ENGINEERING, as a contribution with existing knowledge and faithful record of work carried out by him under my guidance and supervision.

**CYBER SECURITY**

* TYPE OF DATA





* Impact of Cyber Attacks on the company

1. FINANCIAL LOSS

The company when cyber attacked would face a huge financial loss as the attackers steal loads of sensitive information which may be given to the rival company or sold in the deep web.

1. REPUTATIONAL LOSS

Moreover, The company might go undergo reputation loss due to the huge financial loss or stock price getting down.

1. JOB LESS

The company might experience yet another drastic difficulty I.e. it’s employees may get fired due to less profit over the year due to Cyber Attacks.

1. PENALTIES AND FINES

Many of its damages will be covered up by the insurance claiming companies but then the company still has to bear some penalties and fines to ts shares holders and other respective personale.

* KEY CHALLENGES FOR NALCO

1. Complex Supply Chain

Companies like NALCO have a huge supply chain hence making it complex. The Cyber attackers may take advantage of this facility such as they can disrupt the utilities such as electricity, water supply etc.

For example:In 2015 an Ukrainian power supply company became victim of this cyber attack and faces huge difficulties.

SOLUTION:

1. The technologies used needs to be addressed properly. For example, the company needs to spear fish old accounts and delete them.
2. There should be proper awareness in between the employees regarding the ways of how an attack can occur and what can they do to stop it.
3. DATA LEAKAGE

The companies throughout the world always face the threat of data leakage. Important information such as pricing data, geological data can be leaked to their competitors.

SOLUTION:

There should be proper regulation of this type of sensitive data. In India, personal data regulation bill will soon be passed hence, helping out the companies with better security.

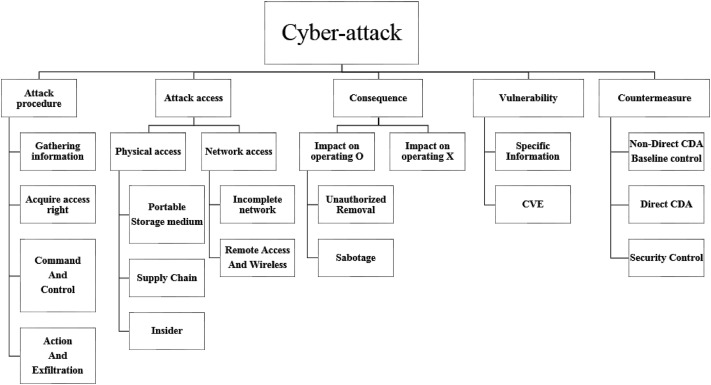
1. BOOSTING ORGANIZATIONAL RESILIENCE

There should be interconnected systems in organizations inside the company for easy communication.

1. CONVERGENCE OF IT AND OT

Convergence of IT and OT has increased risks because OT systems used to be accessed physically. Now, IT has made it easy to access them physically.

**THREAT TAXONOMY**



**SCADA SYSTEM COMPROMISE**

Information gathering---->Target---->Social engineering---->Login Abuse---->Exploit vulnerability---->Back Door---->Compromise Network---->SCADA compromise---->Power supply Disruption---->Block Process

**TYPES OF CYBER ATTACKS**

* PASSWORD ATTACK

Password attacks involve exploiting a broken authorization vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking of passwords. The attacker uses various techniques to access and expose the credentials of a legitimate user, assuming their identity and privileges. The username-password combination is one of the oldest known account authentication techniques, so adversaries have had time to craft multiple methods of obtaining guessable passwords.

* DDOS/DOS attack

A distributed denial-of-service (D Dos) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

* CRYPTO JACKING

Cryptojacking is a threat that embeds itself within a computer or mobile device and then uses its resources to mine cryptocurrency. Cryptocurrency is digital or virtual money, which takes the form of tokens or "coins." The most well-known is Bitcoin, but there are approximately 3,000 other forms of cryptocurrency and while some cryptocurrencies have ventured into the physical world through credit cards or other projects — most remain virtual.

* SQL Injection

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

* ZERO DAY EXPLOIT

A Zero-Day Vulnerability is an unknown security vulnerability or software flaw that a threat actor can target with malicious code. A Zero-Day Exploit is the technique or tactic a malicious actor uses to leverage the vulnerability to attack a system.

* MALWARE

Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware.

* CROSS-SITE SCRIPTING

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

* DNS ATTACK

A DNS Attack is any attack targeting the availability or stability of a network’s DNS service. Attacks that leverage DNS as its mechanism as part of its overall attack strategy, such as cache poisoning, are also considered DNS attacks. In this article, we will get an overview of the common types of DNS attacks out there.

* RANSOM WARE

Ransomware is a type of malware that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn’t pay in time, the data is gone forever or the ransom increases.

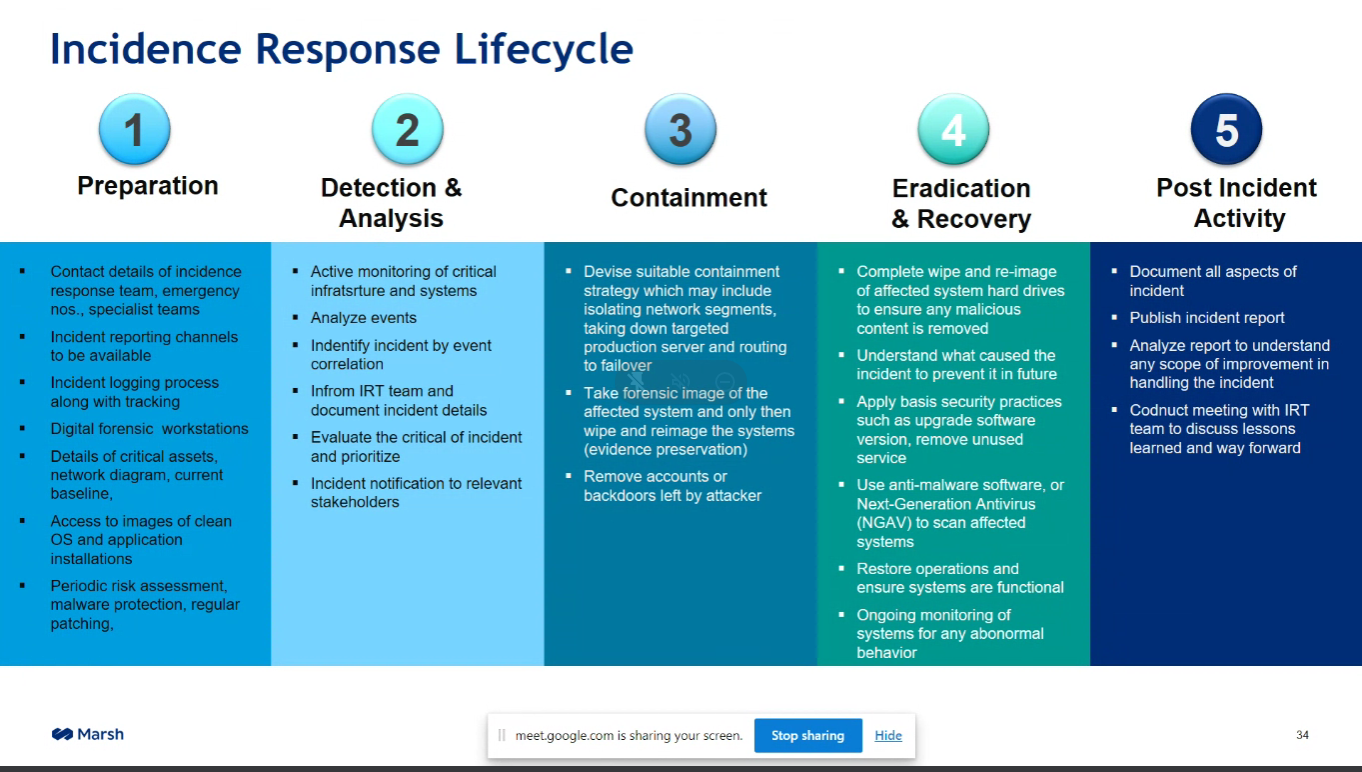
Ransomware attacks are all too common these days. Major companies in North America and Europe alike have fallen victim to it. Cybercriminals will attack any consumer or any business and victims come from all industries.

* MITM ATTACK

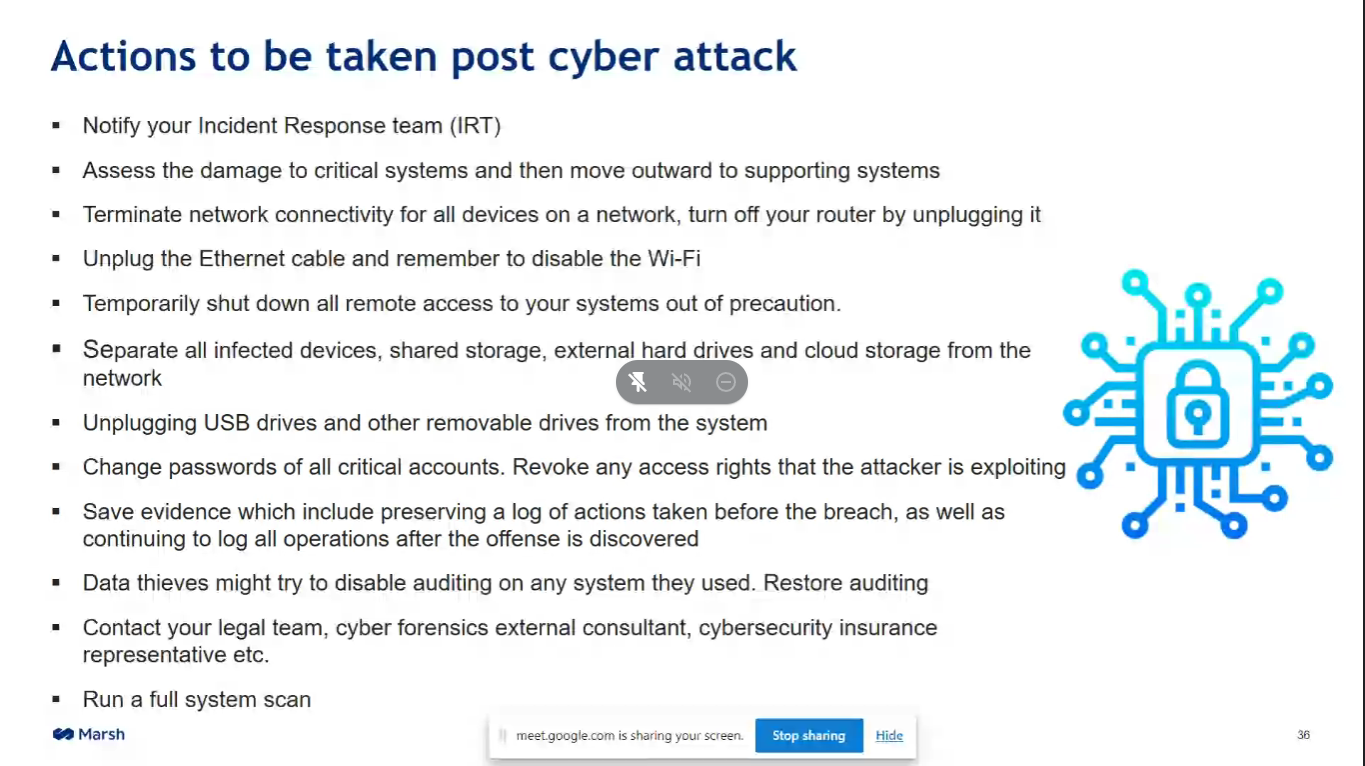
A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

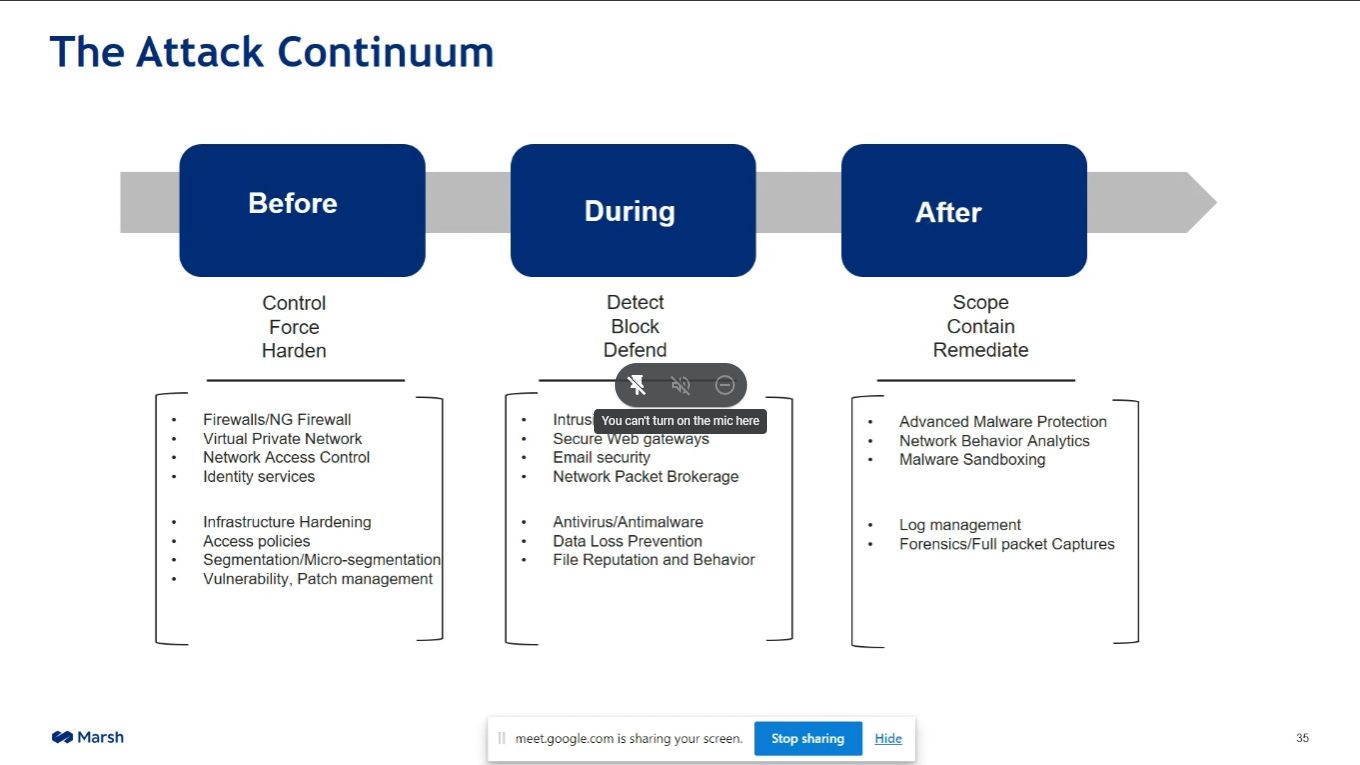
The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

* INCIDENT RESPONSE LIFECYCLE



* ACTIONS TO BE TAKEN POST CYBER ATTACK





**WINDOWS ACTIVE DIRECTORY**

Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

The database (or directory) contains critical information about your environment, including what users and computers there are and who’s allowed to do what. For example, the database might list 100 user accounts with details like each person’s job title, phone number and password. It will also record their permissions.

The services control much of the activity that goes on in your IT environment. In particular, they make sure each person is who they claim to be (authentication), usually by checking the user ID and password they enter, and allow them to access only the data they’re allowed to use (authorization).

MINIMUM EQUIREMENTS TO SET UP ACTIVE WINDOWS DIRECTORY

* 64 BIT OS AND PROCESSOR

Most modem server software (especially Windows Server) will require that you have a 64bit processor and Operating System. If you don't have access to a 64bit processor then your only option is to install older versions of Windows Server .

* ENABLE VIRTUALISATION IN YOUR BIOS

In order to create 64-bit VMs, you must enable virtualization in your BIOS. If you run into trouble when creating your VMs you can assume that virtualization is not enabled.

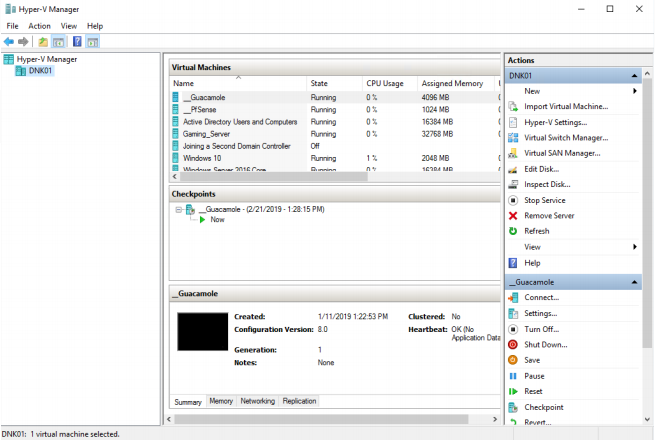
* AVAILABLE STORAGE

You will want to have at least 20gb of free storage space on your hard drive in order to download and install your VM operating systems plus software and updates.

What is a VM???

A virtual machine (VM) is a virtual environment that functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off- or on-premises). Software called a hypervisor separates the machine’s resources from the hardware and provisions them appropriately so they can be used by the VM.

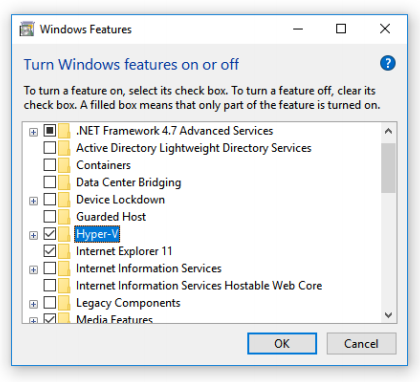
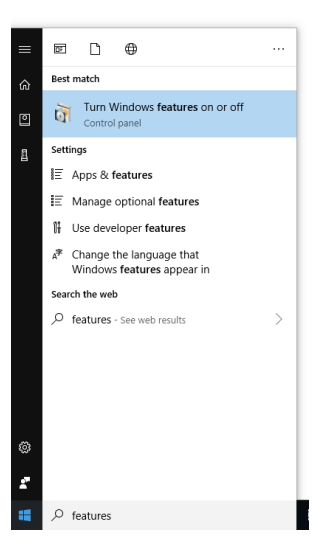
What is a hyperV?



Hyper-V is Microsoft's hardware virtualization product. It lets you create and run a software version of a computer, called a virtual machine. Each virtual machine acts like a complete computer, running an operating system and programs. When you need computing resources, virtual machines give you more flexibility, help save time and money, and are a more efficient way to use hardware than just running one operating system on physical hardware.

**CREATING AN IT LAB USING HYPERV**

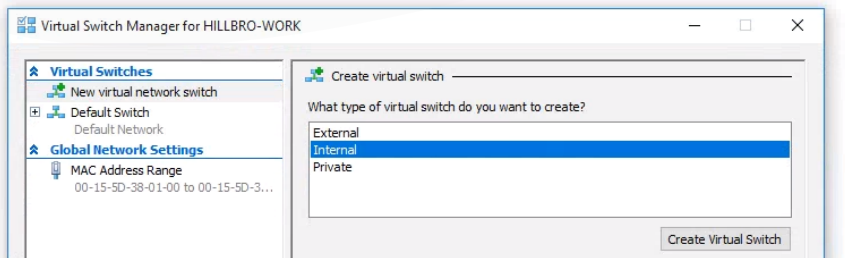
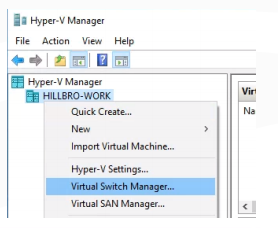
To get started you want to click the Windows button and search for "features". In the results you should see "Tum Windows features on or off" as shown in the image on the right. Open this tool and enable the "Hyper-V" checkbox as shown in the image below. This will often require a reboot of your computer to finalize the installation.



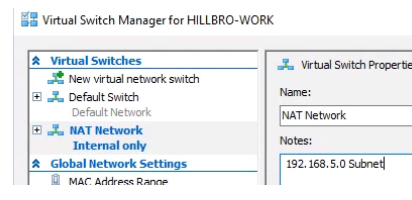
Once you reboot your computer Hyper-V will be installed and you can use the Windows button to search for and launch the Hyper-V Console.

Once the console has been launched, we will need to create a Virtual Machine and a NAT Network which will allow your VMs to share your host PCs internet connection with your VM.

When the console is open, you will want to right-click on your Hyper-V host name and select "Virtual Switch Manager". Next we need to create a new internal virtual switch. On the window that appears, select "Internal" and "Create Virtual Switch" (see image below). This will create a new switch that we can use to network your new VMs together.



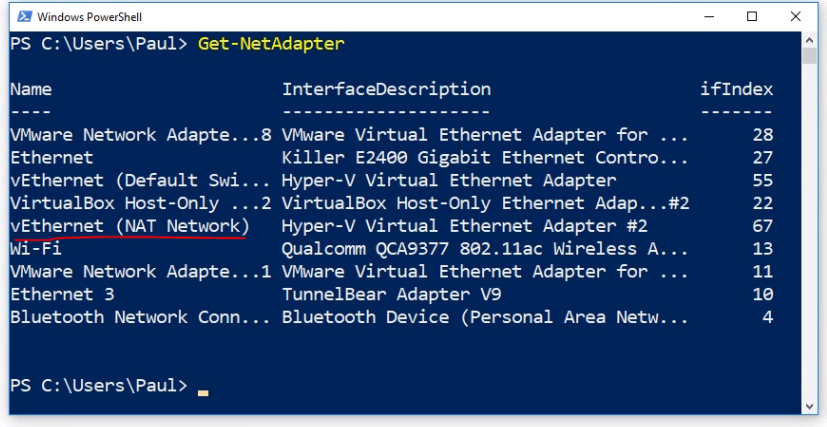
Once you create the switch you should change the name and optionally add some notes. I preferto add the subnet that I plan to use forthat internal network in the notes and this will especially come in handy if you want to create a NAT Network later on. I am going to use the 192.168.5.0/24 subnet so I will add this to the notes forfuture reference. Enterthe same subnet or whatever subnet you would like to use then click OK to save your new internal switch.

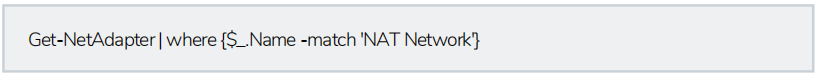


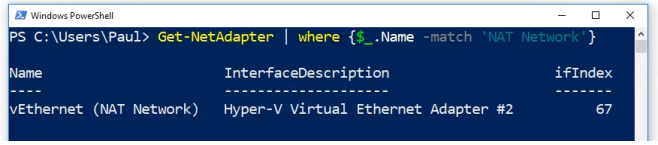
First, launch Windows PowerShell by clicking the Windows button and searching for "PowerShell" (see image on the right). Be sure to hold left-shift and press right-click to launch PowerShell as an administrator.



You should be able to identify your network by the name you chose when you created the switch on the previous page. For example, I created one and named it "NAT Network".When I execute the command above, I can see the switch is listed below. We are interested in the "ifIndex"

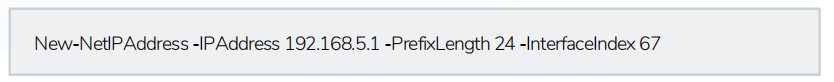


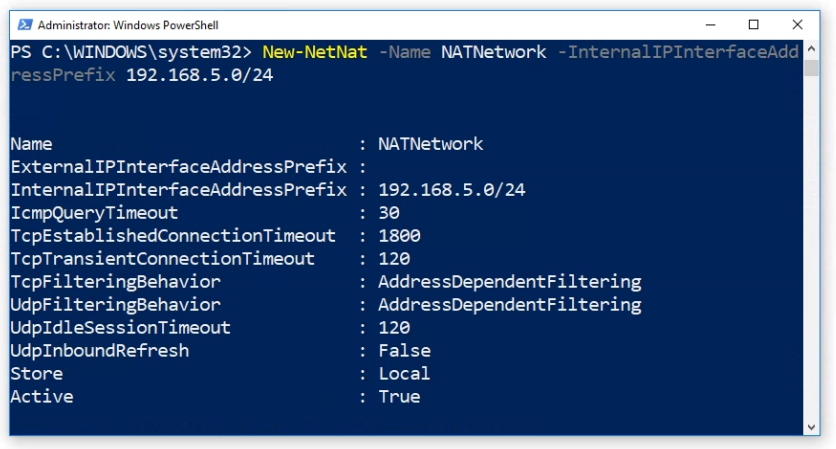


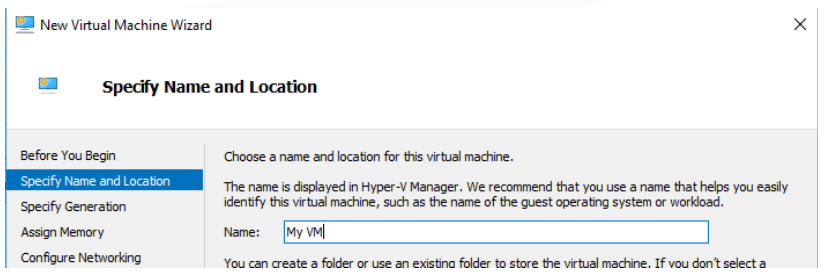
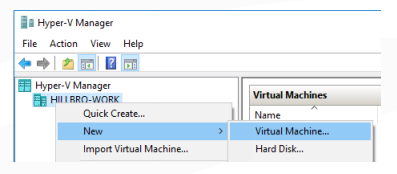


Next we need to create a gateway for our virtual switch.Remember the subnet we put into the notes of the virtual switch?We are going to use the 192.168.5.0/24 subnet. This means that all hosts and IP addresses on this network need to start with 192.168.5.X (x being any number from 0 - 255). Our gateway is going to be .1. And the prefix length is the /24. This basically means the first 24 bits (first three octets) are part of the network address and not usable by hosts.

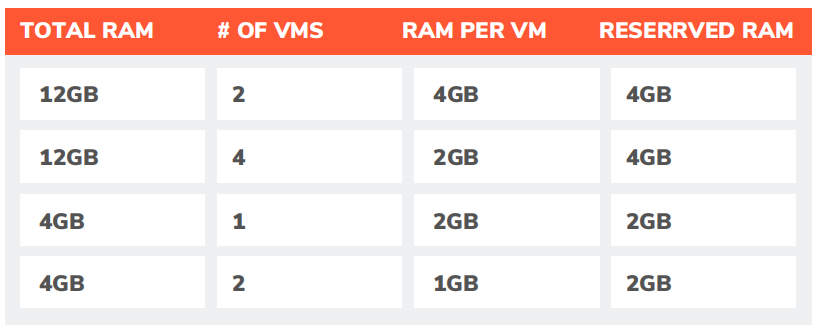
Execute the command below to create the new gateway:







Most of the time you can use a Generation 1VM, so you can go with the default settings and click next. On the "Assign Memory" screen you need to chose the amount of memory that you would like your VM to use. Keep in mind that your VM can only use up to the amount of RAM that your host computer has. The number you pick will also determine how many VMs you wish to run. To make things simple, you could use 2GB of RAM or you could be more calculated about it and use a method like the one outline below. Let's say our host computer has 10GB of RAM.We will use 70% of the RAM for the VMs and reserve 30% for our host computers. This means we will have 7GB forVMs and 3GB for our host computer. Keep in mind if 70% of your total RAM comes out to a fraction, it's OK to round up or down to keep from using weird numbers (like 3.3333 GBRAM per VM). Below are some examples you could use:



**INSTALLING SERVER ROLES**

**Active Directory Domain Services**

The ADDS server role is used to create and manage Windows domains.When you install this role, you build a Windows Domain and the Active Directory and Group Policy tools are installed.

**DNS (Domain Name System)**

The DNS server role allows computer IP address and name resolution. This server role is automatically installed when you install the AD DS serverrole. Anytime computers needs to communicate they are likely using DNS.

**DHCP (Dynamic Host Configuration Protocol)**

The DHCP server role automatically configures computer IP addresses on your network. Generally DHCP will only service workstations or computers and is used to simplify the process of connecting a desktop or laptop to your network.

**WSUS (Windows Server Update Services)**

The WSUS role allows you to manage and deploy Windows updates to your domain computers. You can do things like force computers to install important security updates and exclude certain updates from being installed on certain computers.

**WDS (Windows Deployment Services)**

WDS allows you to deploy operating systems remotely.WDS automates most of the installation process and allows the administrator to avoid installing the OS while being physically present at the computer. Keep in mind that there are many more services that we didn't list here that you will encounter while working in the IT field.

**IIS (Internet Information Services)**

The IIS server role allows your server to host HTTP/s, FTP/s, SMTP and NNTP protocols. This role transforms your server into a Web Server.

**CONCLUSION**

Presently the systems department is on full functionality and is secure to be precise and abiding the rules of security pretty nicely. Due to this, I had a very fortunate experience to see it for myself. The vocational training has been of great help to me and has increased my knowledge whatsoever about Cyber Security and Active Windows Directory.