Module 2

Basics and Environment Setup

Ansh Bhawnani

Cyber Security Basics

Module 2

1. Limitations of Cyber Security

Module 2

Advantages of Cyber Security

- Protection against unwanted softwares
- Maintain privacy and secure data
- Preserving valuable resources
- Provides new career opportunities
- Keeping cyber space safe and clean

Limitations of Cyber Security

- Seriously, **costly**
- Bad configuration maybe **disastrous**
- **Difficult** to choose the right solution
- Generally **overlooked** (unawareness)
- Makes things **slower**

2. Cyber Defense

Module 2

Cyber Defense

- A sub section of cyber security
- Different from corporate cyber security

- Cyber defense is **resisting attacks**
- It is mission driven, more governmental side
- **Intelligence**, **planning**, **surveillance**, vs penetration testing and forensics

3. Skills of an Ethical Hacker

Module 2

Skills of an Ethical Hacker

- Everything taught in this **course**!!!
- **Hacker's mindset**
- Is **verbose**, but doesn't talk much
- **Logical** thinking
- Good **programming** and **networking** skills
- Don't learn it all, but know it all

Skills of an Ethical Hacker

- **Computer Basics**: Hardware, Software, processing methodology
- **Web and Internet**: HTTP, DNS, Web Servers, FTP, SMTP
- **Networking:** TCP/IP, ARP, Devices, types, Routing and Switching
- **Operating Systems**: Linux (Kali, Parrot, Red Hat), Windows, Android, iOS, MAC

Skills of an Ethical Hacker

- **Programming**:
  - Reverse Engineering- C, C++
  - Script Writing- Python, Ruby, Perl
  - Web App Testing- JavaScript, PHP, SQL, JSP, Python
  - Shell Scripting- Bash

Skills of an Ethical Hacker

- Knows the art of **Googling**!!
- At least one professional **certification** (OSCP, CEH, Sec+)
- Strong **cryptography** skills
- Strong **Social Engineering** skills
- **Patience** and **out-of-the-box** thinking
- Always **updated** and **optimistic**

4. Information Security Policies

Module 2

Information Security Policies

- Rules and regulations issued by an organization to ensure CIA of it's IT infrastructure
- **Objectives**: Security of digital assets comply with the rules and guidelines

- **Scope**: Varies, sometimes hierarchical
- **Implementation**: Workers sign an agreement and apply the necessary changes
- Trainings and evaluations may be organized

Information Security Policies

- If database needs to be encrypted, every person responsible should be made **aware** and make changes accordingly.
- **People** are the **weakest** part of defense!
- **Streamlined** with company's primary goals and strategies
- Only applicable within an organizations **boundaries** of authority

5. Vulnerability Research

Module 2

Vulnerability Research

- **White box** approach to software testing
- "Security engineers see the world differently than other engineers,"

Steps:

- Fuzzing and reverse engineering
- Network & Protocol Analysis
- Cryptography
- Web Applications, API's and Mobile Apps
- Hardware Analysis

Vulnerability Research

- How a system works X
- How a system **fails** Y

- Can be done by good or **bad** guys
- Deriving concepts from known attacks and applying **statistically** for current system
- **Periodic** operations helps to mitigate security attacks
- Helps to reduce **zero day** exploits

Operating Systems:
Linux

Module 2

Operating Systems: Linux

- Open Source, Cross Platform Operating System
- Derived from UNIX OS, modified by Linus Torvalds
- Developed and launched in 1991, one of the most widely used Kernel
- Runs on everything, smartphones, laptop, servers, home appliances, submarines or space rockets.
- UNIX shell based environment, just a kernel

1. Evolution of Linux

Module 2

Evolution of Linux

- UNIX project started at 1969 at Bell Laboratories, in C language
- Used in large organizations which later developed their own dialects of UNIX
- Wasn't open source and collaborative, so failed to gain popularity
- In 1991, Torvalds thought to write his own UNIX and make it freely available
- From 1992, Linux is under GNU GPL License and not available for commercial use
- Programmers have modified and released many flavors of Linux over the years

2. Distributions of Linux

Module 2

Evolution of Linux

- **Ubuntu**
  - Debian based, uses GNOME desktop environment
  - Most well-known Linux distribution.
  - Stable LTS release every 2 years
- **Linux Mint**
  - Irish distribution based on Ubuntu
  - Highly stable, full multimedia compatibility
- **Debian**
  - Base for many other distributions
  - Examples: Ubuntu, Kali Linux, MX linux

Evolution of Linux

- **openSUSE**
  - Beautiful desktop experience
  - KDE environment
- **CentOS**
  - Optimized for server environments
  - Package development and server testing, robust
- **Fedora**
  - Continuation of an older distribution "Red Hat Linux."
  - Advanced and enterprise users, used in workstations

3. Linux for Penetration Testing

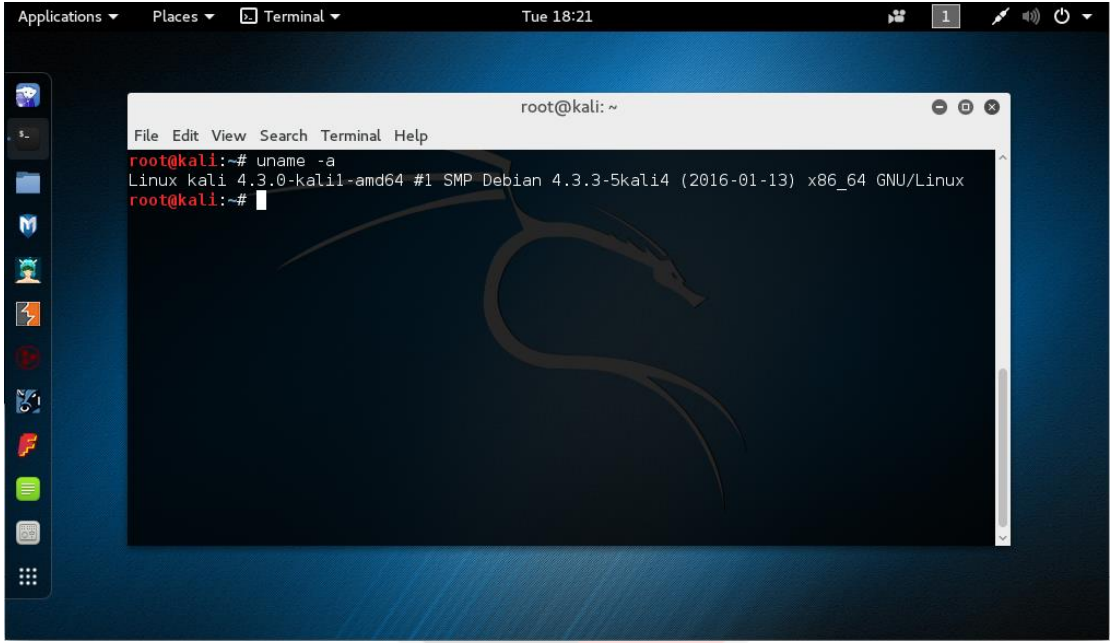
Module 2

Linux for Penetration Testing

Kali Linux

- Developed by Offensive Security as the rewrite of BackTrack
- 500+ preinstalled pen testing tools and applications
- Can run on different platforms like ARM and Vmware

Linux for Penetration Testing

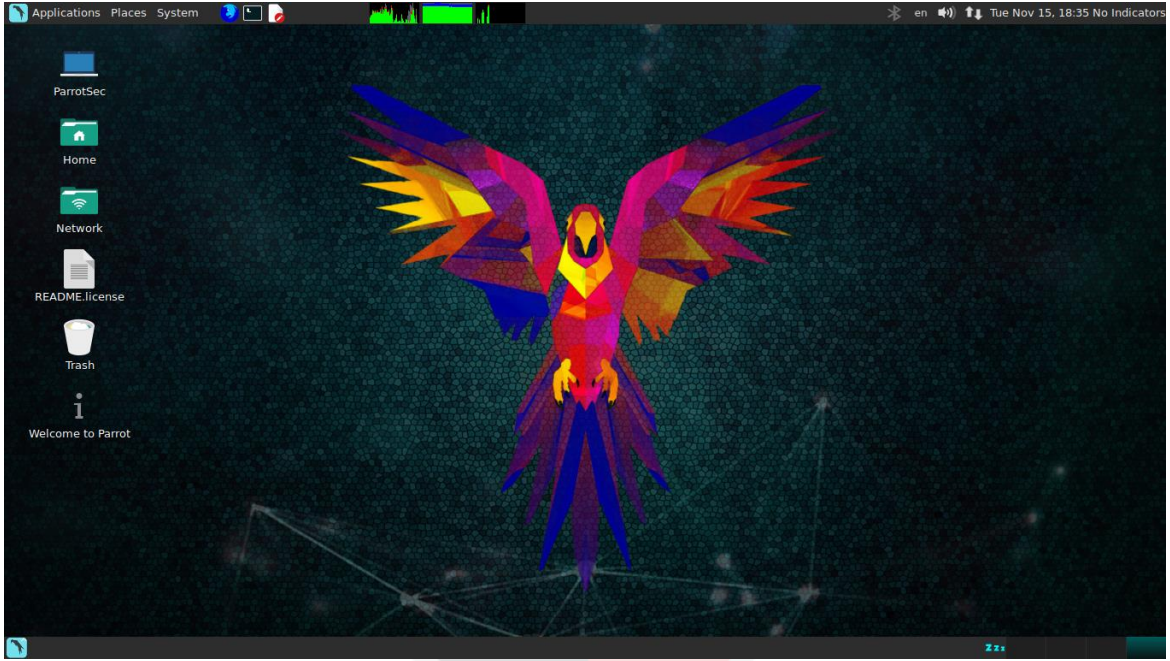


Linux for Penetration Testing

Parrot Security

- Debian-based OS that is developed by Frozenbox's team
- Cloud-friendly, lightweight operating system
- Highly customizable, strong community support

Linux for Penetration Testing



Linux for Penetration Testing

- **BlackArch Linux**
  - Arch Linux-based distribution
  - Window Managers preconfigured dwm, Fluxbox, Openbox, Awesome, wmii, i3, and Spectrwm.
  - Contains over 1800 tools for i686 and x86_64

Linux for Penetration Testing

Linux for Penetration Testing

- **BackBox**
  - Ubuntu-based operating system
  - Complete desktop environment

Linux for Penetration Testing

4. Advantages of Linux

Module 2

Advantages of Linux

- Open Source
- Security
- Legacy support
- Portable and flexible
- Software Updates
- Customizations
- Free of cost
- Various flavors (distributions)
- Community
- Performance
- Fast and Easy

Types of Hackers

Module 2

Types of Hackers

- **Script Kiddies**
  - Amateur hackers without coding skills, “neophyte”
  - Use other’s tools and techniques
  - To gain attention or impress someone, “noobs”
- **Green Hat Hackers**
  - Curious script kiddies
  - Engrossed in the hacking communities
  - Listen and learn with undivided attention

Types of Hackers

- **Blue Hat Hackers**
  - Novice hackers with vengeful agenda
  - No desire for learning
  - Just hack for revenge
- **Red Hat Hackers**
  - Similar to White Hats
  - Halting the acts of Blackhat hackers.
  - Just more ruthless towards them

Types of Hackers

- **Hacktivists**
  - Online version of activist
  - Hack government or large organizations
  - To raise voice for a political or social cause
- **Whistleblowers**
  - Secret agents with strategic insider threats
  - Exposes secret information, ethical or illegal, within private or public organization
  - Maybe hired by government or organizations

Phases of Hacking

Module 2

PHASES OF ETHICAL HACKING

Footprinting

Gaining as much information about the target

Scanning

Identifying loopholes and vulnerabilities in the information gathered

Gaining Access

Exploiting the vulnerabilities with tools and techniques

Maintaining Access

Creating and deploying backdoors for persistence

Clearing logs

Removing traces and records to avoid being caught

Penetration Testing

Module 2

Penetration Testing

- An authorized simulated cyberattack on a computer system
- To evaluate the security of the system
- Automated with software applications or performed manually
- Checking compliance requirements, its employees' security awareness and the organization's immunity towards security incidents
- Domain knowledge is more at an expert level
- Ethical hacking is learning, penetration testing is implementing

Phases of Penetration Testing

Module 2

Phases of Penetration Testing

1. Pre Engagement

Meeting with the client to have a crystal understanding of all their needs and vision

2. Planning and Recon

Test plan generation and public information gathering through scanning

3. Threat Modelling and Vulnerability Identification

Model of all the security concerns and ranking vulnerability severity

4. Exploitation

Gaining access by breaching security of a system or finding a bug to exploit in the software.

5. Post Exploitation

Determining the value of the assets compromised and further attack propagation

Phases of Penetration Testing

6. Reporting

Detailing the vulnerabilities found, stating impact and remedies

7. Resolution and Re Testing

Resolving the issues and verify the fixes

Cyber Security vs Ethical Hacking

Module 2

Cyber Security vs Ethical Hacking

Cyber Security	Ethical Hacking
Deals with how to protect data and systems in the cyberspace	Deals with how to find vulnerabilities and attacks systems and report it
How to protect systems	How to attack systems
Broad term	Part of cyber security
Has many professional fields (Security analyst, SOC Engineer, CISO, etc)	No “Ethical Hacking” job as such, but penetration testers and security managers
Defensive side	Offensive side

Ethical Hacking Laws and Policies

Module 2

Ethical Hacking Laws and Policies

Is Ethical Hacking really ethical?

- In 2013, a member of parliament (MP) in the Netherlands faced legal actions for pointing out a security flaw in a medical center website
- Instead of acknowledging and thanking him, the medical center instead decided to prosecute him.

Ethical Hacking Laws and Policies

Why do we need laws and policies?

- What if the ethical hacker performs unethical actions during the course of the hacking job?
- A solicited hacker may exceed the scope of work and venture into software sections not allowed as per the agreement.

Ethical Hacking Laws and Policies

Legal laws must include:

- The definition of ethical hacking
- Should ethical hacking be done only when solicited formally? How will unsolicited hacking be viewed?
- Only formal and detailed agreements between the hacker and the organization will be treated as solicited hacking
- Will every organization facilitate swift acceptance of the issue description and necessary action?

Ethical Hacking Laws and Policies

Legal laws must include:

- Will unsolicited hackers be punished if they bypass bureaucratic procedures?
- The legal agreement between the hacker and organization should clearly state the ethical hacker's job scope.
- Definition of compensation and rewards for both solicited and unsolicited hackers
- How do you address the issue if the unsolicited hacker misuses the security flaw?

IT Act 2000

Module 2

IT Act 2000

Introduction

- Notified on October 17, 2000
- Deals with cybercrime and electronic commerce in India
- Contains **13 chapters** and **90 sections**.
- Provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

IT Act 2000

Features

- All electronic contracts made through secure electronic channels are legally valid.
- Digital Signatures will use an asymmetric cryptosystem and also a hash function
- The Act applies to offences or contraventions committed outside India
- Senior police officers and other officers can enter any public place and search and arrest without warrant
- It is based on The Indian Penal Code, 1860

Risk Management

Module 2

Risk Management

- Identifying your risks and vulnerabilities and applying administrative actions and comprehensive solutions to make sure your organization is adequately protected.
- Identification, analysis and evaluation of cyber risks, followed my risk management
- Considering the various potential risks or events before they occur, an organization can save money and protect their future.

Risk Management Methodology

Module 2

Risk Management Methodology

- **Establish context**
  - Understand the circumstances in which the rest of the process will take place. The criteria that will be used to evaluate risk should also be established and the structure of the analysis should be defined.
- **Risk identification**
  - The company identifies and defines potential risks that may negatively influence a specific company process or project.

Risk Management Methodology

- **Risk analysis**
  - Once specific types of risk are identified, the company then determines the odds of it occurring, as well as its consequences.
  - Understand each specific instance of risk, and how it could influence the company's projects and objectives.
- **Risk assessment and evaluation**
  - Assess the overall consequence
  - The company can then make decisions on whether the risk is acceptable and whether the company is willing to take it on based on its risk appetite.

Risk Management Methodology

- **Risk mitigation**
  - Companies assess their highest-ranked risks and develop a plan to alleviate them using specific risk controls.
- **Risk monitoring**
  - Following up on both the risks and the overall plan to continuously monitor and track new and existing risks
- **Communicate and consult**
  - Internal and external shareholders should be included in communication and consultation at each appropriate step of the risk management process

Software and Hardware Requirements

Module 2

Hardware Requirements

- **Processor**
  - Minimum: 1.8 Ghz Intel i3 or AMD Ryzen 3 or A6
  - Recommended: Quad core 2.8 Ghz 64-bit Intel i5 or AMD Ryzen 5 or A9, or more
- **RAM**
  - Minimum: 4 GB DDR3
  - Recommended: 8GB DDR4 or more

Hardware Requirements

- **GPU** (for bruteforcing, etc.)
  - Minimum: Nvidia MX 940 or 150 (2GB)
  - Recommended: Nvidia GTX 1060 or more (4GB or more)
- **Hard Disk**
  - Minimum: 512 GB HDD
  - Recommended: 1 TB HDD or more, 128 GB SSD or more (SSD is faster)

Hardware Requirements

- **Network Adapters**
  - Minimum: Wireless LAN Adapter supporting AC protocol
  - Recommended: Wireless External Adapters supporting monitor mode (for Wireless PenTesting)
  - Wireless chipsets supporting Monitor mode:
    - **Atheros AR9271**
    - **Ralink RT3070**
    - **Ralink RT5372**
    - **Realtek 8187L**
    - **Realtek RTL8812AU**

Software Requirements

- Module Dependent
- **OS**: Updated ***Windows*** 10 or Updated ***Linux*** Kernel (Kali/Parrot)
- ***Python*** 2 and 3 installed
- Xampp/Lamp ***Server*** (Apache Enabled)
- ***Virtualization*** Software (VMWare/VirtualBox)

Dual Boot vs Virtual Machine

Module 2

Dual Boot vs Virtual Machine

Dual Boot

- Splitting your computer's resources between the two operating systems
- Each one will have its own dedicated partition on the same hard drive or an external drive
- You can't run both operating systems simultaneously

Dual Boot vs Virtual Machine

Advantage

- Access to fully dedicated hardware resources like CPU, RAM, etc.
- Perfect for running resource-intensive tasks and programs such as gaming, 3D animation, video editing, etc.

Disadvantage

- The installation process is a bit complex and an error can easily affect the whole system.
- You'll have to restart the computer every time you need to switch between operating systems.

Dual Boot vs Virtual Machine

Virtual Machine

- Dedicated virtual environment that resides within your operating system allowing you to simultaneously run two (or more) operating systems
- To get started, all you need is a good **virtualization software** such as VMWare or VirtualBox or Parallels, and the ISO file of the operating system you want to install.

Dual Boot vs Virtual Machine

Advantage

- Easy to set up and switch between operating systems, offers a safer environment due to ***sandboxing***
- Extra layer of security against malware and security vulnerabilities
- You can also create snapshots of the operating system
- Able to move them from one computer to another

Disadvantage

- No dedicated access of resources between OSes.
- Inconvenient for resource-intensive tasks.

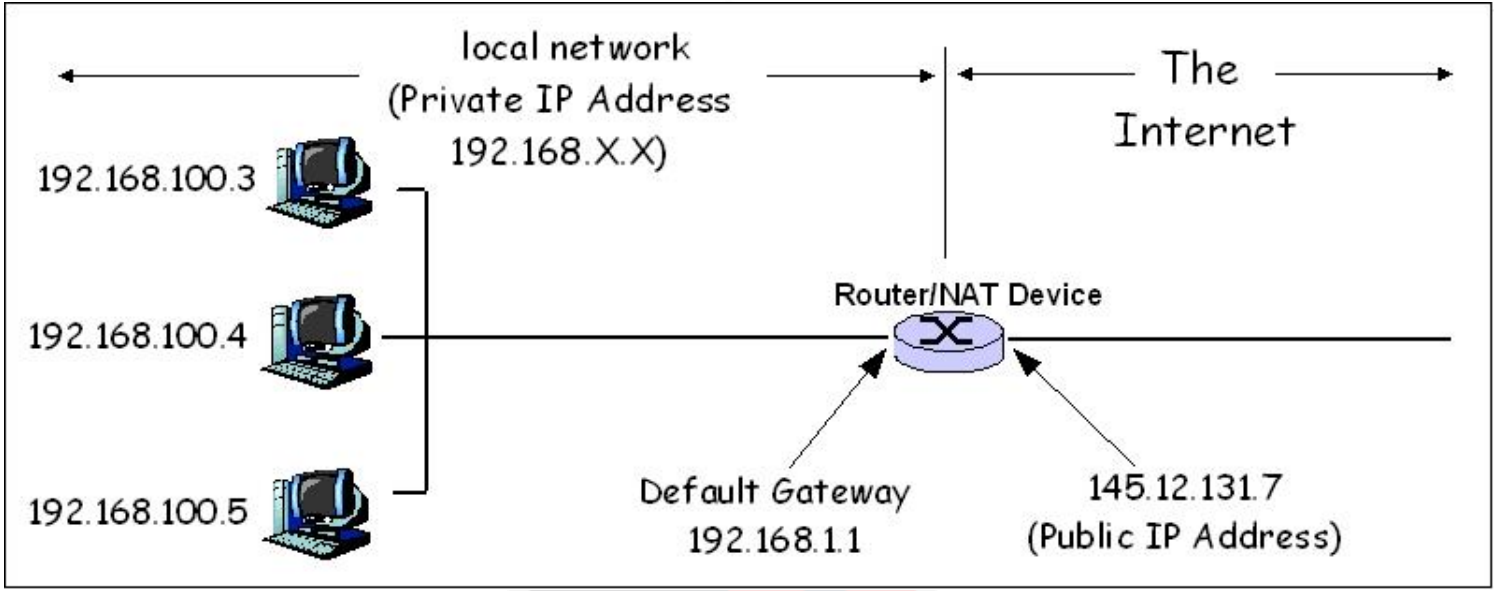
NAT vs Bridged vs Host Only

Module 2

NAT vs Bridged vs Host Only

- **NAT** (Network Address Translation)
  - Just like your home network with a wireless router, the VM will be assigned in a separate subnet.
  - Your VM can access outside network like your host, but no outside access to your VM directly, it's protected.
  - DHCP is internal

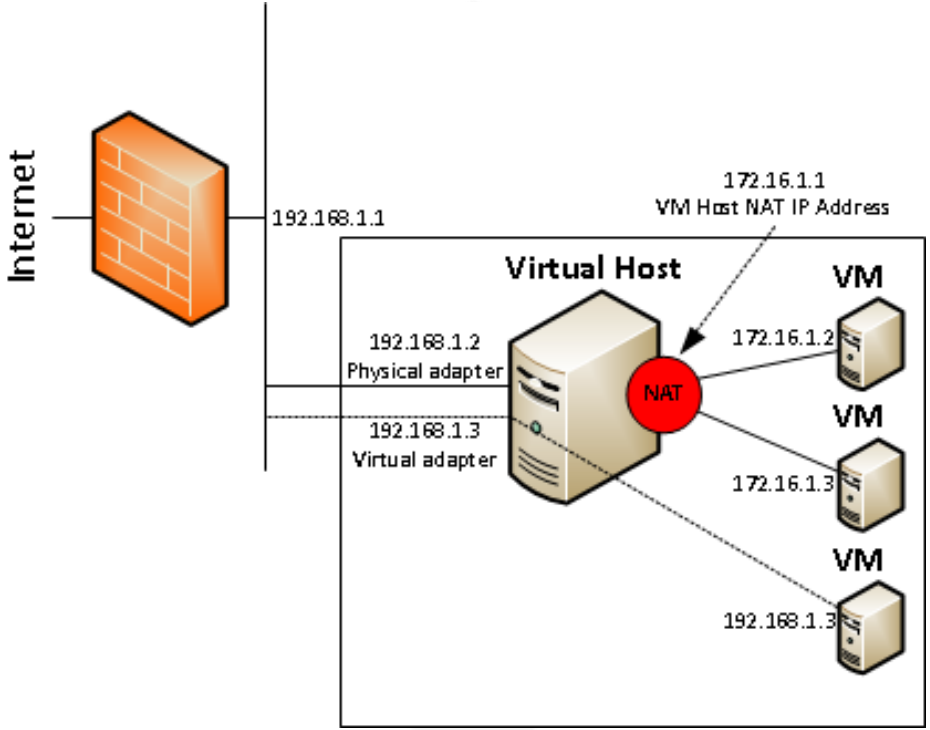
NAT vs Bridged vs Host Only



NAT vs Bridged vs Host Only

- **Bridged**
  - Your VM will be in the same network as your host
  - It can be accessed by all computers in your host network.
  - DHCP is external

NAT vs Bridged vs Host Only



NAT vs Bridged vs Host Only

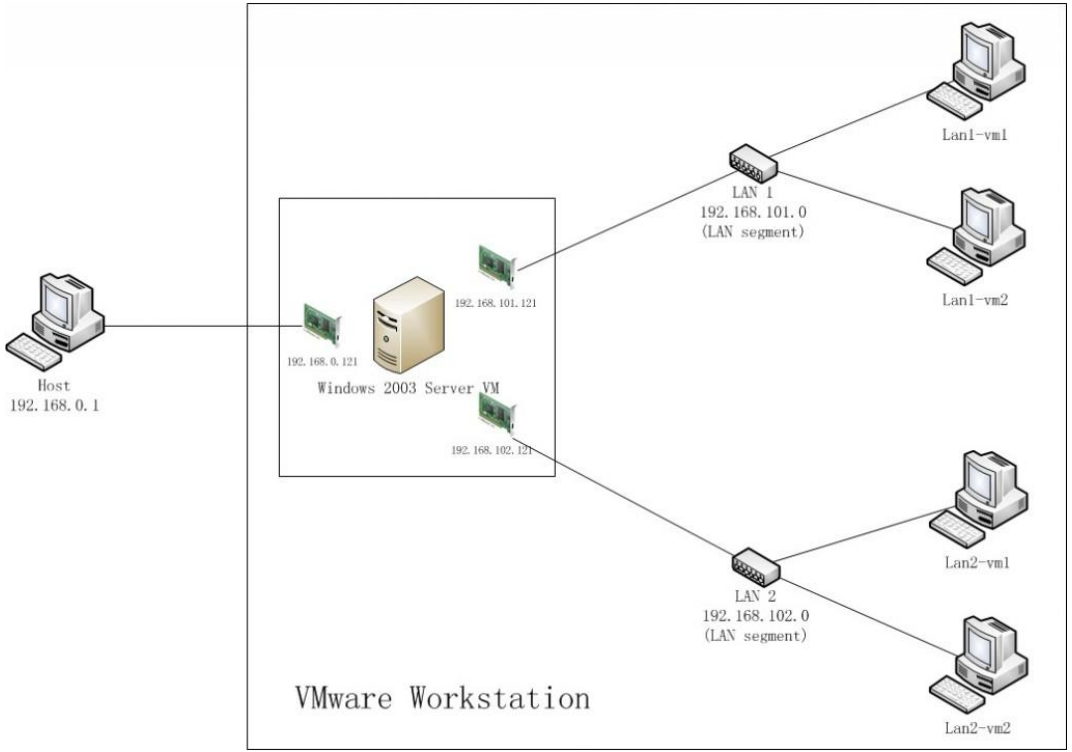
- **Host only**
  - Host-only networking creates a network that is completely contained within the host computer.
  - This means that all VMs connected to a host-only network will be visible to the ***host and to each other***.

NAT vs Bridged vs Host Only

LAN Segments

- An internal network which logically divides a private network into network segments, that is completely contained within the host computer.
- This means that all VMs connected to an internal network will be visible *to each other but not to host*.

NAT vs Bridged vs Host Only



NAT vs Bridged vs Host Only

	VM ↔ Host	VM1 ↔ VM2	VM → Internet	VM ← Internet
Host-only	+	+	–	–
Internal	–	+	–	–
Bridged	+	+	+	+
NAT	–	–	+	Port forwarding
NAT Network	–	+	+	Port forwarding

HACKING

Is an art, practised through a creative mind.