Cyber Security

M.SANDEEP REDDY

KALLAMHARANADHAREDDYINSTITUTE OF TECHNOLOGY

208X1A 4252

Introduction to Cybersecurity

Cybersecurityis the practice of safeguarding systems, networks, and programs from digital attacks.

These attacks can take various forms, such as attempting to access, alter,

or destroy

nseonrmsitailv e information, extorting money through ransomware, or

disrupting
business processes

Cybersecurity professionals deal with a wide range of threats, including

malware,
phishing, denial-of-service attacks, and more.

Different types of cyber security attacks

- Malware
- DosAttacks
- Phishing
- Man-in-the Middle
- SQL Injection
- DNS Tunneling ETC…

Networking TCP and OSI model

TCP/IP Model:

Themodel is a practical
andT wraidneslmy iusseiodn f rCaomnterwolo Prkro ftoorc noel/tIwnoterkrn ceotm Pmroutoncicoal t(iToCn

Layers:

- Physical Layer
- Network Layer
- Transport Layer
- Application Layer

Networking TCP and OSI model

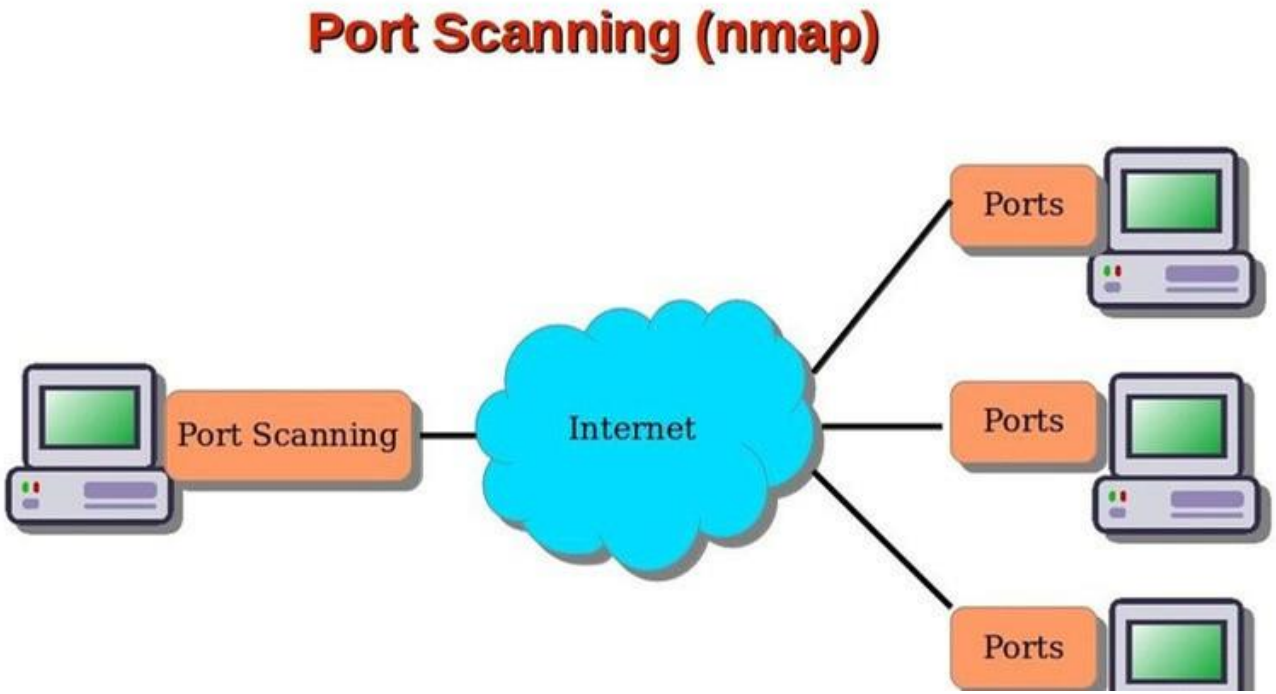
OSI Model:

TheOpen Systems Interconnectionmodel is a generic, protocol-independent framework that describes (OSI) all forms of network
communication.

Layers:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Ports


Port Scanning (nmap)
Port Scanning
Internet
Ports
Ports
Ports

Ports

Well-Known Ports

Service	Port	Function
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20, 21	File transfer
DNS	53	Name resolution
SMTP	25	Internet mail
POP3	110	Post Office Protocol (POP) mailbox
IMAP	143	Internet Message Access Protocol (IMAP) Mailbox
Telnet	23	Remote login
SSH	22	Secure remote logn

Protocols

Secure Sockets Layer (SSL) Protocol.

Transport Layer Security (TLS) Protocol.

Secure Hyper-Text Transfer Protocol (SHTTP).

Secure Electronic Transaction (SET) Protocol.

Internet Protocol Security (IPSec).

Virtual Private Network (VPN).

These protocols work together to ensure the confidentiality, integrity, and availability of data.

Introduction to Python in Cyber Security

Python is a powerful programming language widely used in the field of cybersecurity. Here are some key points about Python in cybersecurity:

1. Foundational Concepts
2. Automation and Efficiency
3. Cybersecurity Applications etc..

Introduction to Python in Cyber Security

Foundational Concepts:

- Python is a high-level language known for its readability and concise syntax.
- It supports various data types, including strings, lists, dictionaries, and sets.
- Variables, conditional statements, loops, and functions are fundamental concepts in Py thon.

Automation and Efficiency:

- Python’s automation capabilities are crucial for cybersecurity professionals.
- It allows you to automate repetitive tasks, such as scanning, data extraction, and reporting.
- By writing custom Python scripts, you can streamline processes and save time.

Introduction to Python in Cyber Security

Cybersecurity :

- Applications: Python can automate reconnaissance tasks, gathering information about Rtaercgoent nsayisstseamnsc.e
- Network Scanni:n Ugse Python to scan networks, identify vulnerabilities, and discover open ports.
- Credential Acce:s Psython scripts can help crack passwords or manipulate credentials.
- Command-and-:C Eosntatrbollish

Thank you!