CYBER SECURITY WITH IBM QRADAR

INTRODUCTION TO CYBERSECURITY

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security Application security Information security etc..

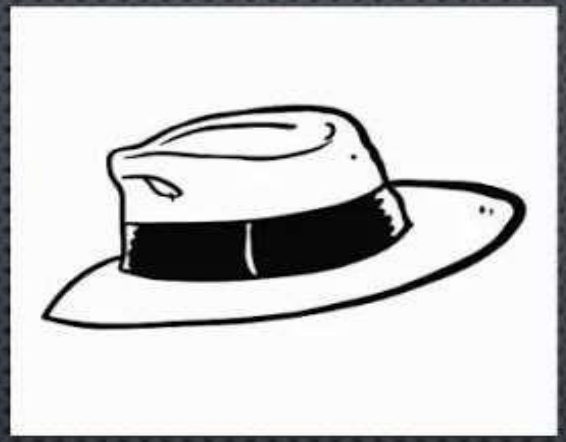
TYPES OF ATTACKS

TYPES OF HACKERS

BLACK HAT

A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

WHITE HAT



A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.

GREY HAT

A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

PHASES OF HACKING

The Reconnaissance Phase

This is the first stage in the ethical hacking process. The white-hat hacker collects all the information available about the networks and systems in place, as well as the security measures that have been implemented.

The Scanning Phase

The second phase in an ethical hacker's strategy is the scanning phase. This step involves using all the information obtained in the reconnaissance phase and applying it to look for vulnerabilities in the targeted area

The Gaining Access Phase

This is where the ethical hacker does the actual hacking. He uses all the information obtained and analyzed from the previous two phases to launch a full-fledged attack on the system or network the ethical hacker is trying to infiltrate.

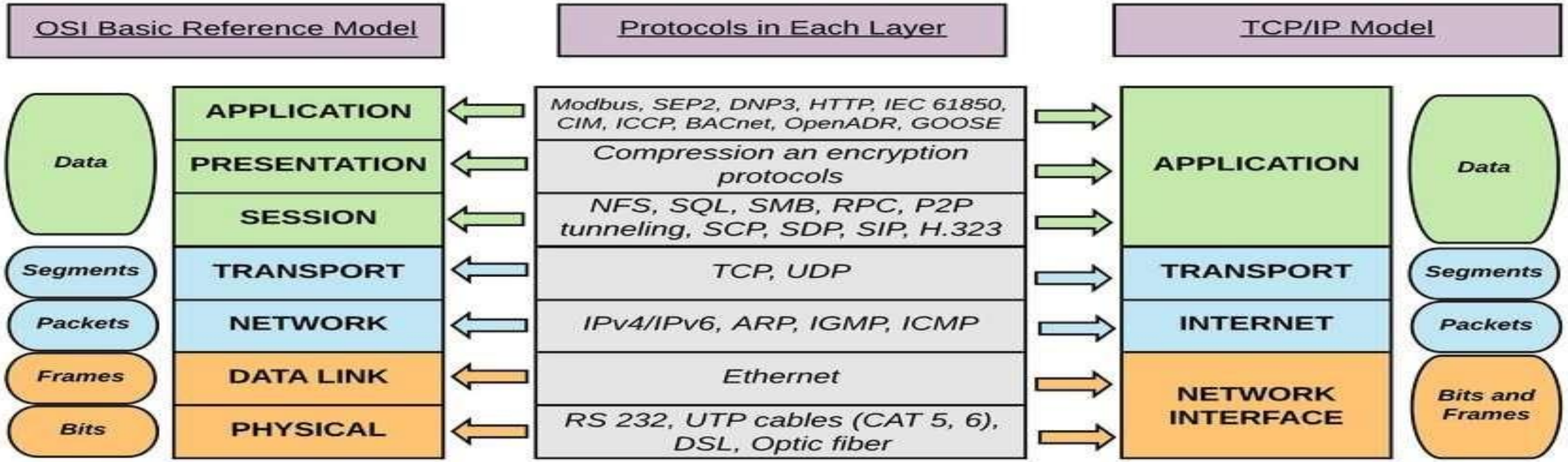
Maintaining Access Phase

The ethical hacker has to maintain his access to the server until he fulfills his goal. Ethical hackers usually employ Trojans and other backdoors or rootkits to accomplish this phase.

Cleaning tracks

This is the final step to complete the entire ethical hacking process. If this phase is completed successfully, the ethical hacker has managed to hack into a system or network.

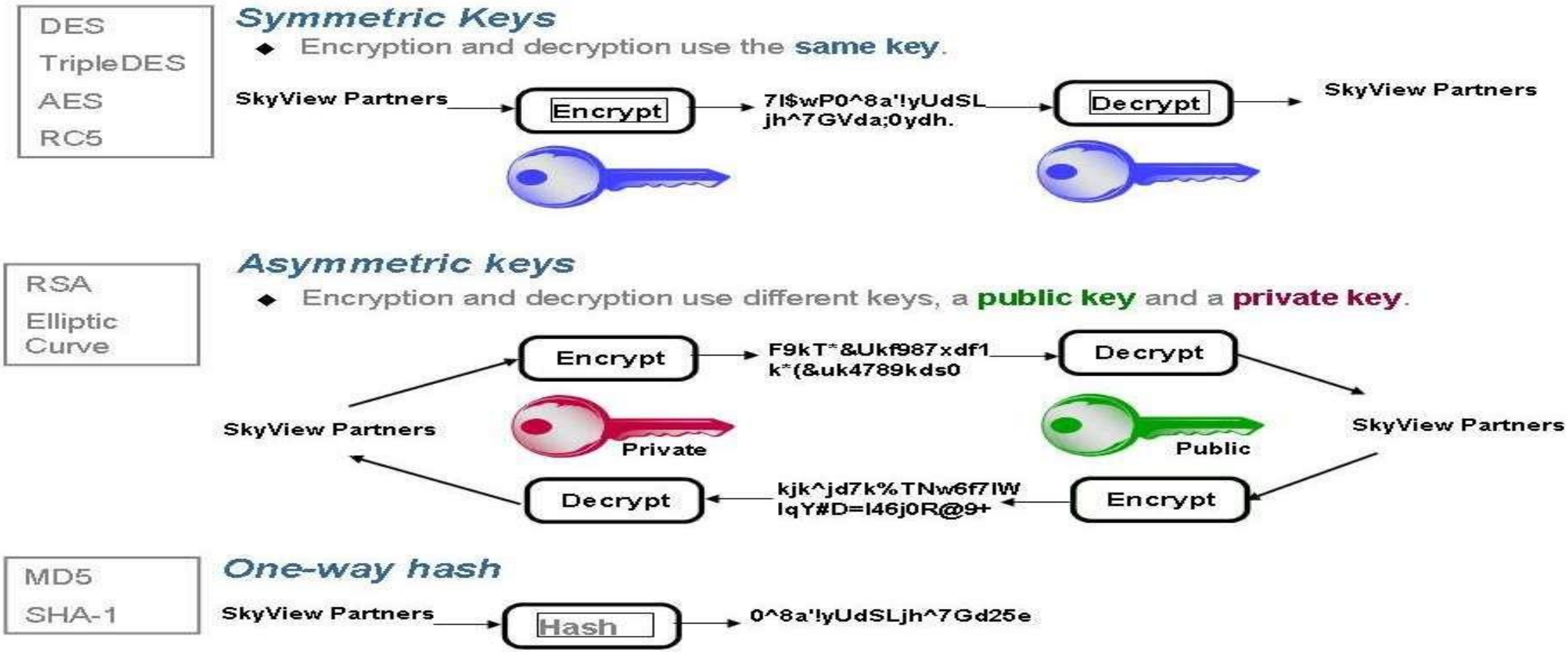
OSI ,TCP MODEL



TYPES OF ENCRYPTIONS

Encryption

Encryption is a form of data security in which information is converted to ciphertext. Only authorized people who have the key can decipher the code and access the original plaintext information.



STEPS FOR PYTHON

1. Create a folder in system
2. Open folder in VSCode
3. Open terminal in VSCode
4. For creating virtual environment command

   python-m venv env
5. To activate

   ./env/Scripts/Activate.ps1

CRYPTOGRAPHIC HASH FUNCTION

- Cryptographic hash functions take an input (message) and produce a fixed-size output
- They are fast and deterministic, always producing the same output for the same input.
- Hash functions have a fixed output size, like 256 bits for SHA-256.
- They are used for data integrity verification, password hashing, digital signatures, and more.
- Cryptographic hash functions should be irreversible, meaning it's hard to get the original input from the hash value.
- They should be resistant to finding another input that produces the same hash value
- Common hash functions include SHA-256, SHA-3, MD5 and SHA-1
- MD5 and SHA-1 are considered broken and insecure due to vulnerabilities.

OWSAP TOP 10 2021

OWASP stands for the Open Web Application Security Project, an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

Broken Access Control

Broken Access Control moved up from the fifth most severe risk in 2017 to the top risk in 2021. There were more instances of Common Weakness Enumerators (CWE) for this than any other category.

Cryptographic Failures

Previously known as “Sensitive Data Exposure”, it was renamed to better reflect the root cause of the issue. It moves up from number three to runner-up in widespread vulnerabilities on the OWASP list. It consists of a failure to protect sensitive data that should not have been publicly accessible.

Injection

A code injection happens when an attacker sends invalid data to the web application with the intention of making it do something that the application is not designed/programmed to do.

Insecure Design

A new addition to the OWASP Top Ten, clocking in at number four on the list, is insecure design. This focuses on the ground-up development of web applications from the very beginning of its life cycle.

Security Misconfigurations

This category moves up one notch from the previous top 10 list published in 2017. The previous category for XML External Entities (XXE) has been rolled into this one.

Vulnerable and Outdated Components

Even simple websites such as personal blogs have a lot of dependencies, plugins, extensions and third party code. Failing to update every piece of software on the backend and frontend of a website will introduce heavy security risks sooner rather than later.

Identification and Authentication Failures

Previously number two on the OWASP list, “broken authentication” has been renamed to this and now ranked at number seven. A broken authentication vulnerability can allow an attacker to use manual and/or automatic methods to try to gain control over any account they want in a system – or even worse – to gain complete control over the system.

Software and Data Integrity Failures

Another new addition to the 2021 roster is software and data integrity failures. These failures can take many forms, particularly since as the web evolves it is more and more common to use third party code and services within web applications.

Security Logging & Monitoring Failures

The importance of securing a website cannot be understated. While 100% security is not a realistic goal, there are ways to **keep your website monitored** on a regular basis.

Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

THANK

YOU