Phases Of A Cyber Attack

Objectives

After completing this unit, you should be able to:

- Delve into basic concepts of Cybercrime & types of Cybercrime
- Understand phases & techniques of a typical Cyber Attack
- Appreciate the need of having an enterprise wide cyber security framework
- Get an overview of NIST Cyber Security Framework
- Understand basic concepts around Incident Response

Cyber – Crime

What Do You Mean By Cybercrime?

A criminal activity that involves computing devices such as computers, tablets, phones, IoT, networked devices or a network

Cybercrime Examples

Categories Of Cybercrime

Computer systems – Technology as a Target

- Computing systems, Networks and many more, act as primary business & personal enablers & carry lots of sensitive data and are critical in sustaining many practical life situations. Example: Pace makers, medical monitoring chips and so on
- Such key computing systems or networks are targeted with an aim of causing disruption
- Ex: Hacking & remotely controlling computers, endpoints, injecting malicious code & viruses to cause disruption, DOS attacks for shutting systems or services down

Computer systems – Technology as a Weapon

- As computing systems are part & parcel of real life situations & enablers – such systems can be used against businesses & individuals for committing real world crimes
- Ex: Banking frauds, Vendor Payment Frauds, Cyber terrorism, Cyber influencing and so on

Hacking

Hacking is an "art" of gaining unauthorized access to data in a system or computer!

- Usually the term is referred with a negative connotation, however may have two perspectives:

White Hat Hacking

Black Hat Hacking

- **White Hat Hacking** is carried out for planned, approved & ethical reasons
- **Black Hat Hacking** is carried out for unethical, unauthorized, damaging reasons – usually for fulfilling personal or a group's reasons
- Unethical or **Black Hat** hacking leads to Cybercrime & the perpetrators are usually known as Cybercriminals

Incentives Of Cybercriminals

Cyber Attacks Making News! “Not Without A Reason”

ERP applications are under cyber attack, research confirms

ERP applications are increasingly being targeted by cyber criminals, hacktivists and nation-state actors, a report reveals

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS

Hackers launched blistering ransomware attacks Tuesday against companies and agencies across the world, particularly targeting Ukrainian businesses.

WannaCry

The most infamous ransomware attack of 2017 was a strain of ransomware called WannaCry that spread all over the globe.

The ransomware targeted numerous public utilities and large corporations, most notably National Health Service hospitals and facilities in the United Kingdom, hobbling emergency rooms, delaying vital medical procedures, and creating chaos for many British patients.

ABC NEWS

Just In | Australia | World | Business | Sport | Science | Arts | Analysis | Fact Che

Print | Email | Facebook | Twitter | More

Ransomware cyberattack hits Australia as EU warns victims worldwide may grow

Updated 15 May 2017, 8:58am

More Australians could find they have become victims of a massive global cyber attack when they turn on their computers this morning, the Federal Government is warning.

The attack, which locks computers and holds users' files for ransom, hit 200,000 victims in 150 countries over the weekend.

The Telegraph HOME | NEWS | S

News

UK | World | Politics | Science | Education | Health | Brexit | Royals | Investigatio

News

Cyber attack on Singapore health database steals details of 1.5m including prime minister

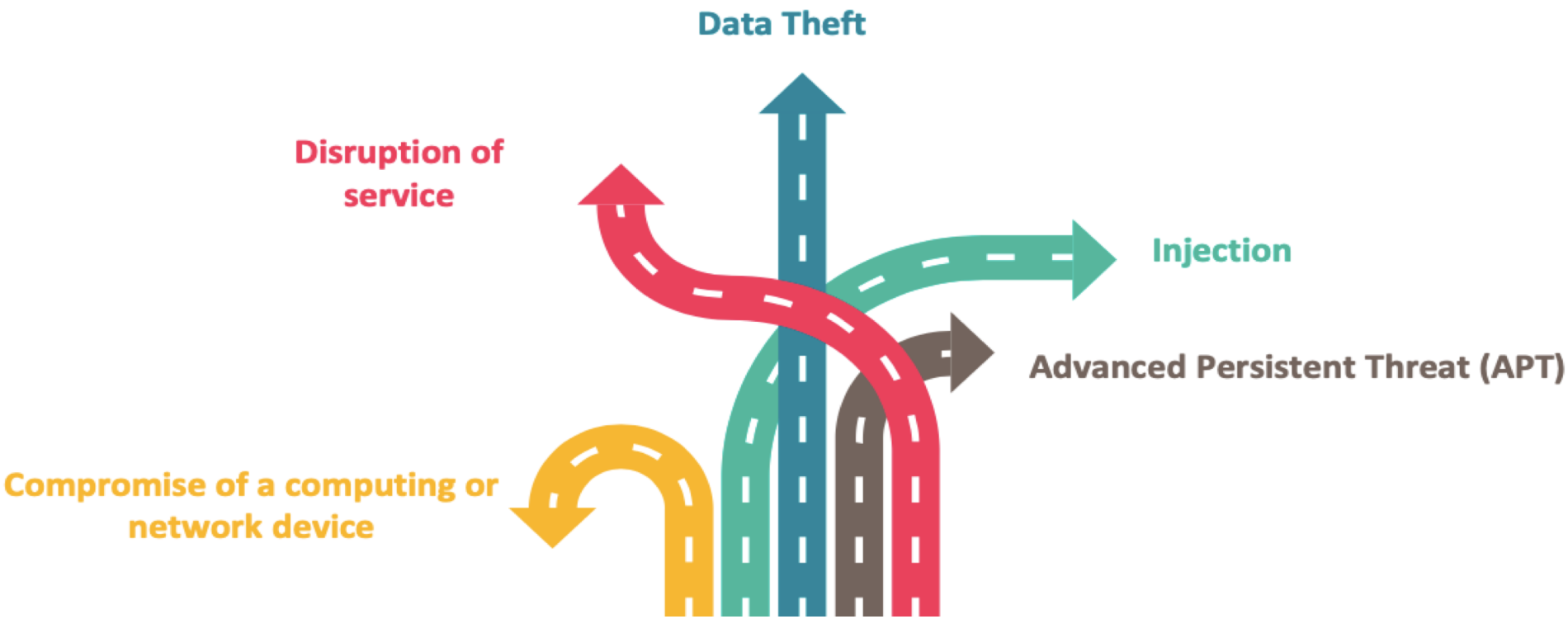
share | Save

FTVETI

ICT @ FTVETI

Cyber Attacks

Categories Of Cyber Attacks



Compromise Of A Device

Objective:

- Gaining full control of a computing device or endpoint - so as to remotely control it for hacker's requirements
- Running Malware on machine for damaging the normal operation of the endpoint
- Performing unauthorized transactions on behalf of someone else
- Spying

Requirements:

- Root, Admin, Power user credentials
- Exploit: EOP (Elevation Of Privilege) - Enter with Low privilege user (such as guest) & Transform into High privilege user (power, admin, root)

Outcome:

- Arbitrary execution on compromised device
- Network capture & control
- Once control is achieved, it gives a huge power to the hacker to carry out multitude of other cyber attacks

Disruption Of Service

Objective:

- Preventing a service, device, website, portal, application, server from performing its usually expected functions

Requirements:

- Huge computing (servers, networks, technology) resources

Outcomes:

- System failure
- Downtime
- Revenue loss
- Reputation loss

Data Theft

Objective:

- Stealing sensitive information from a target or group of targets

Requirements:

- Access to the storage media or computing device

Outcomes:

- Reconnaissance of target environment or user for launching further bigger attacks
- Arbitrary unauthorized operations and transactions using the stolen data
- Identity Theft
- IP (Intellectual Property): Patents, Trade secrets, business strategy theft
- Exposure of Private information/PII

Injection

Objective:

- Submission of incorrect data into a processing system which gets accepted without detection

Requirements:

- Access to device storing data, system and application

Outcomes:

- Determination of the current state of data driven services – for launching further attacks
- Attacks on other users of the system

APT

Objective:

- Gaining in-depth access to a computing environment for multiple malicious & unauthorized purposes

Requirements:

- Sophisticated knowledge about the target
- Resources (Time, Funds, Technology)

Outcomes:

- Long-term reconnaissance
- Ability to act on target quickly after establishment
- Complete and undetected control of systems
- Combination of outcomes of Injection, Exfiltration, Service Disruption & Remote control
- Potential high impacts on enterprises and government organizations

Categories Of Elementary Technical Attacks

Active Attacks

Comprise of intrusion, disruption into a victim's computing system and environment

Examples:

- Denial of Service
- Resource usage tracking
- Spoofing

Passive Attacks

These attacks may not always require a disruption or a major intrusion to the target systems. Usually Passive attacks are initially used for gaining grounds before launching Active attacks

Examples

- Sniffing
  - Passwords
  - Network Traffic
  - Sensitive Information
- Information Gathering (Recon)

Elementary Security Attacks

Spoofing

An attacker alters his identity & pretends to be someone else (usually a trusted individual) to the victim and the exploits this trust for his own benefit

Types Of Spoofing

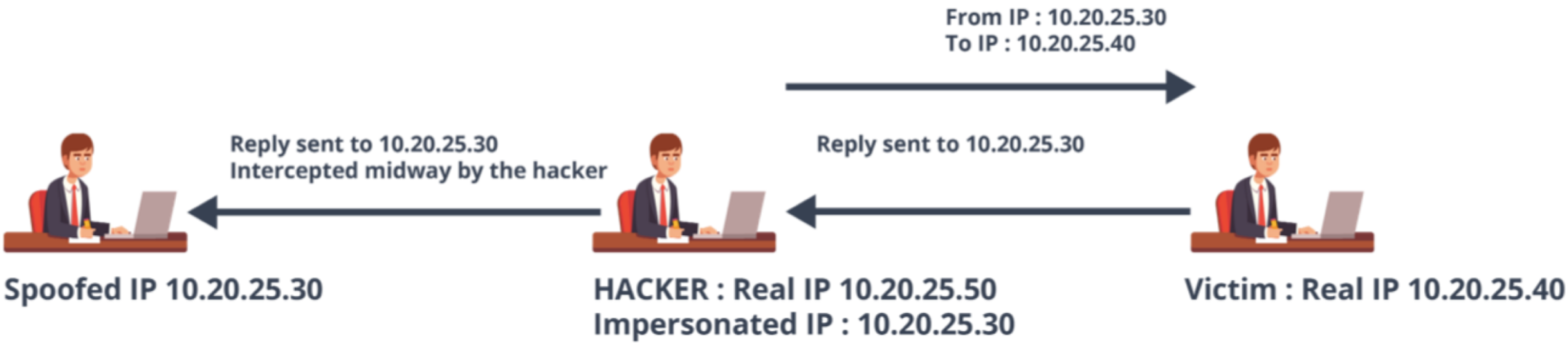
IP Spoofing

Email Spoofing

Web Spoofing

IP Spoofing: Source Routing Alteration

The hacker first spoofs the address of another machine. Then the attacker places himself in between the attacked machine & the spoofed machine so as to intercept replies. This is a kind of MITM (Man In The Middle) attack



IP Spoofing: Destination Alteration

The hacker impersonates himself with an IP address of another trusted computer, to gain unauthorized access or capture sensitive information

HACKER : Real IP 10.20.25.30

Receiver's Real IP : 10.20.25.40

Real IP : 10.20.25.50 (Victim)

Email Spoofing

The hacker sends messages pretending to be some other individual or organization who the victim would trust

Common techniques of email spoofing:

- Create a fake account with similar looking email address: Ex- Hacker sends an email to a victim an email from fake email created with name "ceo.rkm.organization@yahoo.com" instead of “ceo.rkm@organization.com”
- Modify an e-mail client: Attacker can put in "ANY" return address of his choice, in the mail he sends to a victim. This causes all the replies go to the set return address
- Abuse Port 25: Email servers usually use port 25 (SMTP). Attacker logs on to this port using basic attack techniques, and then composes a message for the user

Web Spoofing

- The hacker registers a new look-alike typo-squatted web address (domains) with an entity's existing web address
- **Example:**
  - funfair.com [original]
  - funfare.com [fake]
  - fumfair.com [fake]

Usage of fake look – alike web domains

- Man-in-the-Middle Attack
  - An attacker first allures a user to access the fake page & then acts as a silent proxy between the original web server and the client
  - Endgame: Interception of traffic, Credential theft
- URL Rewriting
  - The hacker may redirect web traffic to an another fake website controlled by the hacker for malicious purposes
  - The hacker may insert his own fake web site's address before the real legitimate link of the original website
  - Usually dynamic websites have variables in their URLs to instruct fetching instructions for the user - & such variables may be hacked as well

DOS – Denial Of Service

DOS Attack refers to a method through which an attacker can make a system useless or significantly slowing it down to be used by legitimate users by overloading or abusing them

Methodology

- An attacker sends a burst of data or packets which causes the victim system to crash, reboot, slow down or enter into an infinite loop
- When all critical resources are exhausted, users are either denied access or denied service

DDOS (Distributed DOS) Attacks

- DDOS is a set of coordinated DOS attacks involving multiple systems or machines to launch attacks against a given victim
- DDOS is much more powerful as the burst of data could become super huge to handle at server side
- **Examples:** Ping Of Death, Smurf, SYN Flood and so on

Session Hijacking

Session hijacking refers to the method of taking over an existing active user session on a specific website, for performing unauthorized activities

1. User makes a successful connection to the server, after authenticating using his user ID and password
2. After the user authenticates, it gets an access to the server until the session is active
3. An attacker first tries to steal the session details (session tokens, id and so on)
4. The attacker then somehow diverts the user out or offline via Denial Of Service attack
5. The attacker then gains access to the user's session by impersonating the user using the stolen session details

Buffer Overflow

01 Buffer Overflow Attack takes advantage of the way in which the information is stored by computer programs

02 An attacker tries to store more information on the stack than the size of the buffer

03 When data inserted by a program or process is more than the pre-allocated size, the excess data overflows out of that buffer

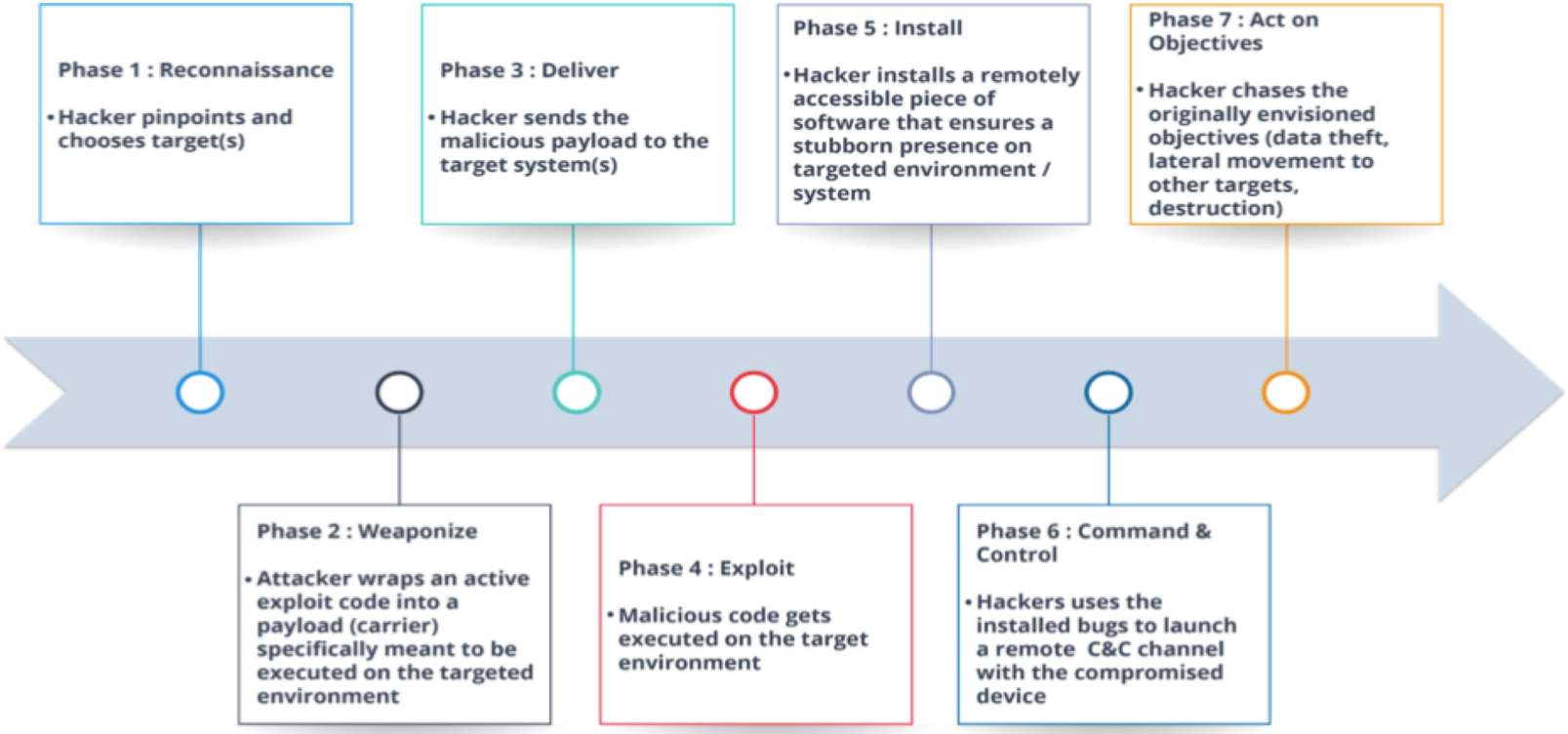
04 Such overflown data tends to leak into other adjacent buffers (being used by other processes on the system) and may corrupt or overwrite the data of those impacted buffers

05 In a buffer-overflow attack, the overflowing data sometimes contains planted specific CPU instructions that the hacker wants to execute which could in turn damage files, alter data or reveals private information held by one process into an another hacker controlled process

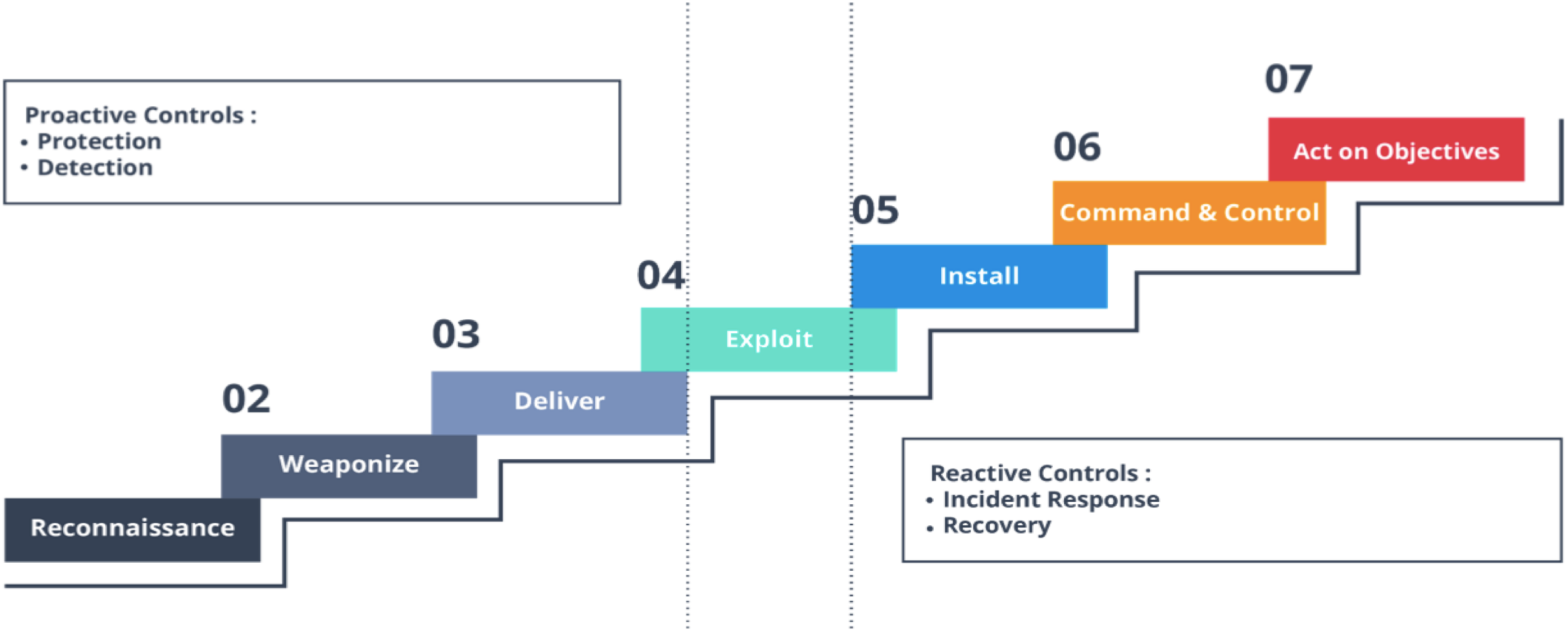
Cyber Attack Lifecycle

Cyber Attack Progression

- Multitude of cyber – attack life cycles exist, including Lockheed Martin's "Cyber Kill-Chain", penetration steps proposed in NIST SP 800-115 & many more
- In general there are 7 distinct phases of a cyber attack as defined in NIST SP 800-150:



Cyber Kill Chain (Lockheed Martin®)



Phase1: Reconnaissance

Overview

- Efforts of an attacker towards gathering maximum information about a target in terms of network, architecture, operating systems & other specifications
- Recon attack is performed using publicly available information about the target

Objectives

- Find who are the high privilege or power users in the target environment which will yield the most to the hacker if compromised
- Recon phase usually focuses on maximal enumeration of the attack surface of the target

Types

- Active: Intrusive in nature (performed by penetrating, accessing and moving around the target network)
- Passive: Non intrusive in nature (performed usually with externally available information)

Tools

- Apart from Physical human intelligence, a variety of free available resources are used for gathering and correlating information about the target
- Example: Google tricks, Shodan, ZoomEye & Censys, give a picture of open & vulnerable assets. DarkWeb marketplaces for gathering leaked credentials of servers & users

Mitigation

- Best mitigation to Recon is achieved using Detection & Preventive Controls on all layers of information exit
- Basic System Hardening , Vulnerability management, Patching & Configuration management are the key inevitable controls
- Streamlined security policies, Governance & Information Flow control is an added advantage.
- Technical measures help a long way to detect technical reconnaissance being carried out against an organization (detecting usage of port, vulnerability scanning, injection)
- Deception (Deploying Honeypots) is a great way of early detection of such attempts being carried out

Phase2: Weaponization

Overview

- Hacker's goal is to create cyber "weapons" such as botnets, trojans, malwares & so on, which will cause a security hole in the victim's system
- Usually the attacker modifies or plants something in a system, which a user will encounter & react so as to create malicious results
- Weapons are usually maliciously repackaged tools, utilities, documents etc
- Remember - in this phase the weapon has NOT reached the victim yet & this phase is typically executed OUT of the victim's boundary (if the attacker is an external entity)

Objectives

- Preparation of a cyber weapon which will be run by the user unknowingly
- To allure the user enough to make him run a maliciously packaged binary or document that will reach him in the next phase

Mitigation

- Cyber Threat Intelligence
- Updated Detection
- Process monitoring

Tools

- Metasploit – heavily used by hackers to develop & execute exploit-code against a specific remote target
- Veil Framework – used by hackers to generate binaries or executables that will typically not be detected by common anti-malware solution
- Luckystrike – PowerShell based tool used by attackers to create malicious office documents with encrypted code pieces for infecting a network

Phase3: Delivery

Overview

- Trick User to click, interact with a cyber weapon created in the previous phase - yielding malicious results that favour hacker's intention

Types

- Hacker controlled delivery: by directly hacking into a known vulnerability or an open port (gathered while Recon phase)
- Hacker released deliver: by sending the packaged weapon to the victim through phishing emails, social media & so on

Mitigation

- Security Training & Awareness campaigns,
- Network security controls (IDS , IPS , Firewalls, WAF and so on)

Objectives

- Efforts towards Delivery of the cyber weapon created previously to the targeted victim

Tools

- Social Engineering methods
- Distributing Alluring free USB devices
- Mal-advertisements

Phase4: Exploitation

Overview

- First opportunity to the hacker for making an actual intrusion into the target victim's system

Types

- Placement of malware (dropper), backdoor for RCE (Remote Command Execution)
- Integer, Buffer overflow - system crash & memory leak

Objectives

- Exploitation of a known or expected vulnerability (not necessarily technical)
- This exploit may not be always visible but does create a hole or backdoor in the system which is used

Mitigation

- Process monitoring, HIDS, Anti-malware
- System hardening
- Security Awareness

Phase5: Installation

Overview

- With successfully exploited vulnerability in previous phase, the attacker's weapon installs a malware or backdoor onto the victim's system in installation phase

Objectives

- Installation of the Payload (malicious code) victim's system
- Such malicious piece of code installed helps the attacker then to remote control the victim's system for achieving endgoals
- Such malwares may (usually silently) begin harvesting further user information such as passwords, credentials for EOP etc. that helps it to move laterally and persistently into the environment & keep searching the sweet spots of target

Mitigation

- Earliest possible detection of such malwares is the key
- Network Security Controls
- Endpoint Security Controls
- Server Hardening
- Security Monitoring
- User Behaviour analysis
- Swift Incident Response is very important if any such attempt is found

Phase6: Command & Control

Overview

- The installed backdoors or malwares in the previous stage usually need to be controlled by the hacker in its due course of hunting, destruction & achieving its malicious intents. Hence such installed malwares make seemingly legitimate connections from inside to externally hosted C&C (Command & Control) servers where it not only dumps collected information to the hacker but also gains next commands from the hacker

Objectives

- Establishing covert connections by the malware to externally hosted C&C servers
- Such connections are typically custom encrypted and go via normal https ports
- Many a times the C&C communication takes places in small un – noticeable chunks hence the communication is not made often & also the communication runs in small amounts
- For complex APT attacks – The C&C servers are usually moved frequently from one IP or domain to another so as to counter any security detection or monitoring attempts within the victim organization

Mitigation

- Advanced Network Security Controls based on Machine learning & Data Analytics
- Correlation with Endpoint Security Controls
- User Behaviour analysis
- Swift Incident Response is very important if any such attempt is found

Phase7: Action On Objectives

Overview

- This is the final stage where the attacker tries to actually accomplish the real objective of launching this hacking attempt

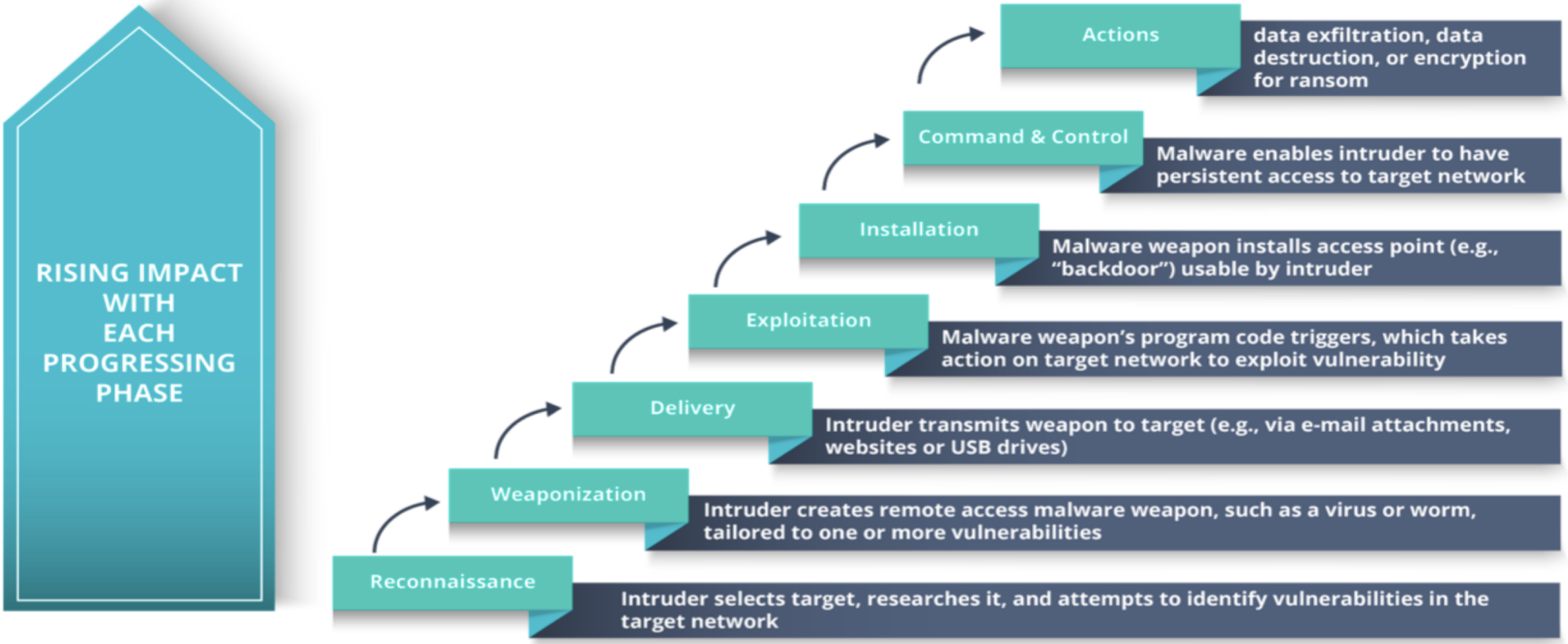
Objectives

- Endgame of the attack!
- The final goal could include anything from ransom extortion, data theft, critical server or system damage, targeting enterprise Production (SCADA) or IOT systems for causing loss in production, revenue, cyber terrorism towards military, nuclear, public welfare operations and so on

Mitigation

- Often it is too late to detect such a phase without any damage. However, in proportion to the complexity of attack and the end goal - it may take the hacker a significantly long time for moving from C&C stage to the Action phase due to many hurdles that he may face in the course
- It is essential to detect the presence of a bug or malware & potential C&C communication as early as possible within this advancement window
- Swift incident response & recovery is the key
- Thus strongly developed and well tested BCP/ DR plans are must for any organization that relies on IT

Cyber Kill Chain – Summary



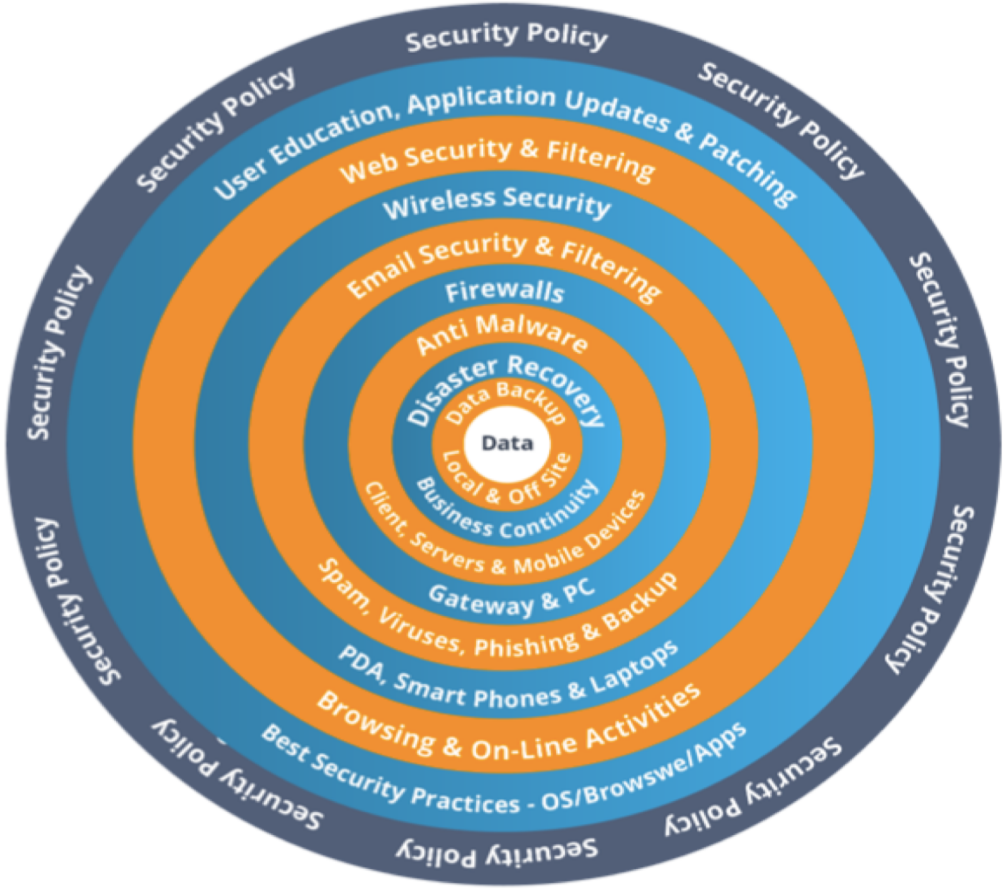
Security Approach

Layered Security Approach (Defence In Depth)

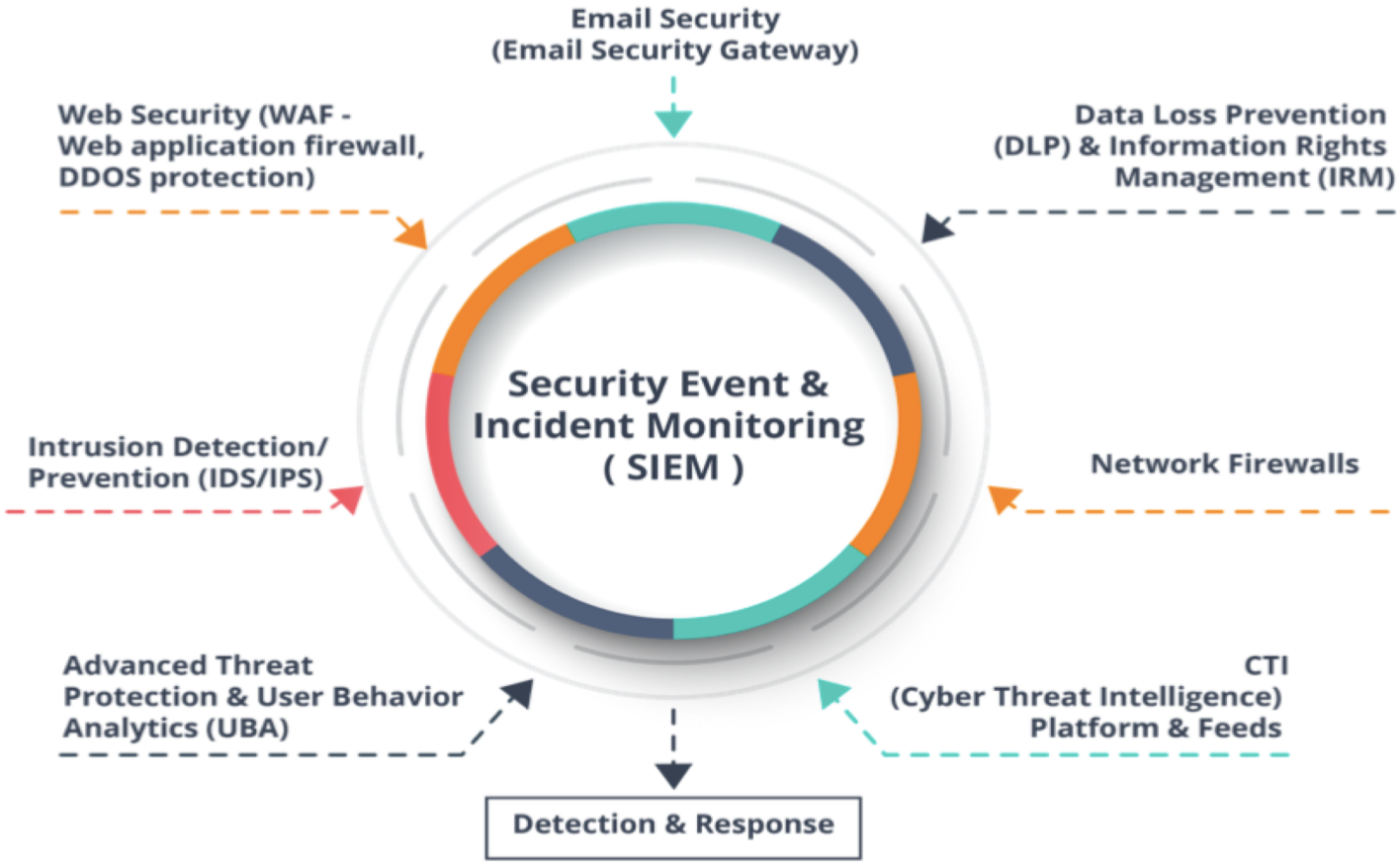
Enterprise Data & Applications are core assets to be protected

More Layers = More and complicated attacking effort

More Layers = More chances of attack being early detected



Layered Security Controls



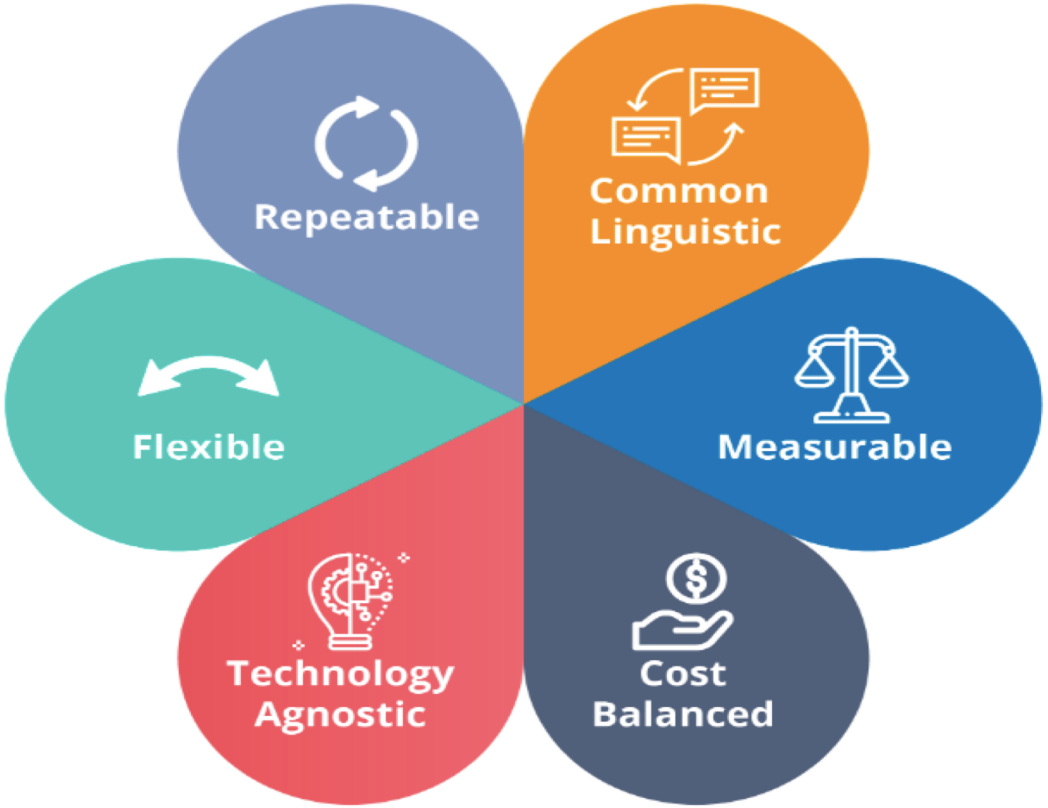
Essential Practices – Cyber Defense In Depth

Cyber Security Frameworks

Cyber Security Frameworks

- An enterprise needs to essentially categorize and prioritize the areas & key assets to be secured
- A Cyber Security Framework is a high level guidance, based on existing guidelines and best practices for enterprises to efficiently & effectively manage and minimize the security risk in cyber world

Characteristics Of A Cyber Security Framework



Objectives Of A Cyber Security Framework – NIST CSF

Source: https://www.nist.gov/cyberframework

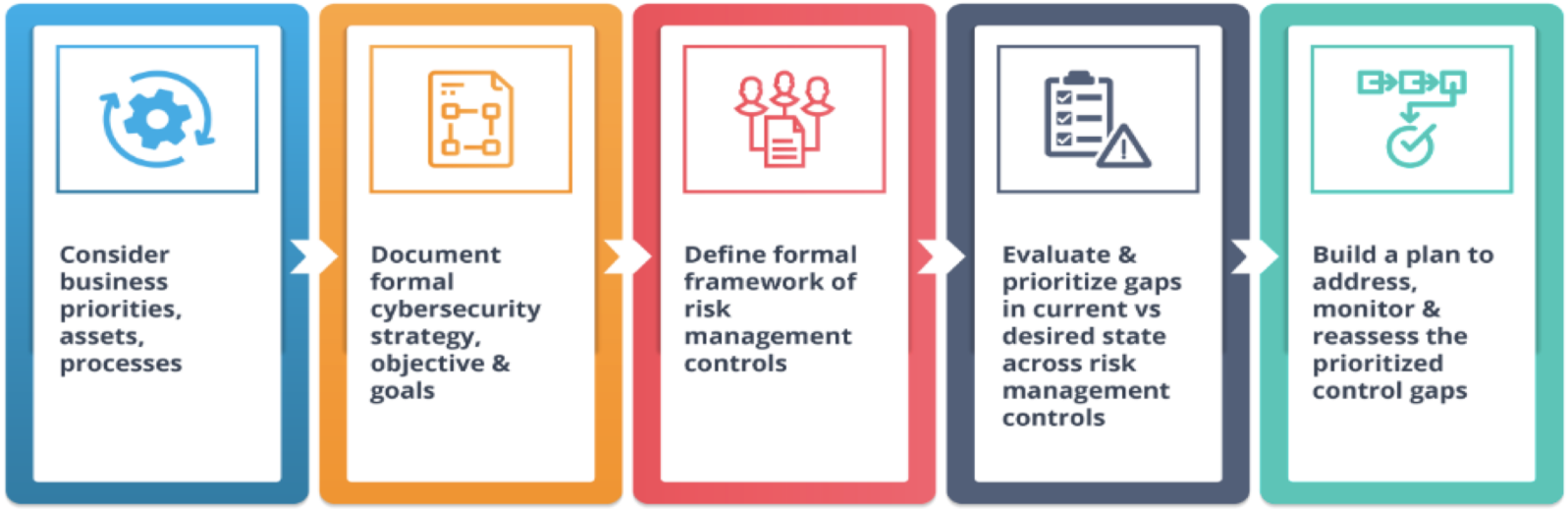
Examples Of Well Known Cyber Security Frameworks

- **HITRUST (Health Information Trust Alliance):** Set of guidelines for information security designed specifically for the healthcare sector
- **PCI DSS (Payment Card Industry Data Security Standard):** Set of security controls designed to protect payments, account security around credit, debit, and cash card data
- **ISO (International Organization for Standardization):**
  - ISO 27001 specifies generic requirements for information security for an organization
  - ISO 27002 specifies the security controls to support the requirements stated in ISO 27001
- **CIS Critical Security Controls:** Previously known as SANS Top 20 security controls – CIS Critical controls enlists 20 assorted security controls in the order of priority, prescribed to stop the most commonly occurring cyber attacks
- **NIST Framework**
  - Another holistic framework aimed towards improving organization's readiness for managing cyber security risk by leveraging standard methodologies and processes. Being business vertical agnostic , NIST & ISO frameworks are considered as gold security standards
  - Example: NIST SP 800-53 (Security Control Catalog) NIST SP 800-30 (Risk Assessments) & NIST-CSF (NIST Cyber Security Framework)

Cyber Security Program

At a high level, the comprehensive collection of security controls that an enterprise needs to have in place so as to protect & secure its key assets and help business run smoothly - is collectively called as cyber security program

Key Elements of a Cybersecurity Program:



NIST Cyber Security Framework

FTVETI

ICT @ FTVETI

NIST CSF – Components Overview

NIST CSF – Implementation Guidance Steps

Step 1: Prioritize & Scope

Strategic decisions and scoping for cyber security based on the organization's mission , vision & business priorities

Step 2: Orient

Identification of related systems and assets, regulatory requirements, & overall risk approach. Identification of threats & vulnerabilities pertaining to the identified assets & systems

Step 3: Create a Current Profile

Creation of a security profile of current levels with reference to the prescribed categories in the CSF

Step 4: Conduct a Risk Assessment

Analysis of operational environment in order to derive the likelihood of a cybersecurity event & the impact that the event could have on the organization

Step 5: Create a Target Profile

Creation of a security profile of desirec levels with reference to the prescribed categories in the CSF

Step 6: Determine, Analyze, & Prioritize Gaps

Gap analysis between the Target Vs Current profile Assessment of resources, cost, funding etc to bridge the identified gaps

Step 7: Implement Action Plan

Actions to be taken for bridging the prioritized gaps & moving towards the desired Target Profile

Incident Response

Incident Response

Incident Response – Handling an event of Cyber Attack

Incident response refers to a process by which an enterprise copes up with a cyber attack

Aim is to effectively manage the incident, in order to minimize the damage in terms of cost, business reputation, critical data and so on

Organizations must have a clearly drafted & tested incident response plan in place

Incident Response Lifecycle

Pre-Incident Phase

PREPARATION

- preparing for an unavoidable security breach.
- Development of incident response plan , security strategy, breach management strategy etc.

IDENTIFICATION

- Detection via log files, monitoring tools, error messages, intrusion detection systems, and firewalls to detect and determine incidents and their scope.

Incident Phase

TRIAGE

- Prioritize by level of impact (usually when there are multiple incidents detected)

CONTAINMENT

- Control the situation so as to curtail the damage usually by containing the affected processes / systems.
- Preserve evidences if required for compliance audit and/or legal matters

ERADICATION

- Threat removal (Technical activities around cleanup/removal/restaging of the malicious components)
- Restoring systems to previous working state as much as possible
- Ensure adjacent & linked systems are rendered clean

Recovery Phase

Validating the systems being restored are clean through testing & monitoring before placing them into production environment.

Post-Incident Phase

LESSONS LEARNED

- Detailed RCA (Root Cause Analysis) of the incident
- Derivation of improvement plan in order to avoid the incident to recur in the future
- Updation of Incident Response plan & Awareness Training as required
- Communication with stakeholders
- Resetting benchmarks for future comparison of Incident thresholds
- Feedback to CTI / Threat hunting group

Quiz #1

- What is the prime objective of a DOS (Denial of Service) attack?
  a. Exploiting a vulnerability in the ISO/OSI Layers
  b. Executing a Malware on a target computer system
  c. Overloading a system to make it sluggish or not available for normal operations
  d. Shutting down the target services by turning them off via social engineering

Answer #1

- What is the prime objective of a DOS (Denial of Service) attack?
  a. Exploiting a vulnerability in the ISO/OSI Layers
  b. Executing a Malware on a target computer system
  c. **Overloading a system to make it sluggish or not available for normal operations**
  d. Shutting down the target services by turning them off via social engineering

Answer c:
Explanation: DOS attack is aimed at overloading the target system with an unmanageable burst of requests so as to make it dysfunctional

Quiz #2

- Phishing attacks are primarily based on which technique?
  a. Identity Theft
  b. Impersonation
  c. Dumpster Diving
  d. Covering the tracks

Answer #2

- Phishing attacks are primarily based on which technique?
  a. Identity Theft
  b. Impersonation
  c. Dumpster Diving
  d. Covering the tracks

Answer b:
Explanation: Phishing works on the basis of the attacker pretending to be someone who is more trust worthy to the victim. This is nothing but impersonation for malicious reasons

Quiz #3

- A public internet zone (cyber café / internet kiosk) in a college, has multiple visitors visiting throughout the day for their personal and educational internet surfing purposes. It has been noted by many students that most of the students' emails got compromised of late after visiting such kiosks. The students had been accessing their personal emails using the public shared computers available in the kiosks. What could be a potential reason for this breach?

  a. IP Spoofing

  b. Presence of a Ransomware on the public computers

  c. Presence of a Keylogger on the public computers

  d. Presence of a botnet on the public computers

Answer #3

- A public internet zone (cyber café / internet kiosk) in a college, has multiple visitors visiting throughout the day for their personal and educational internet surfing purposes. It has been noted by many students that most of the students' emails got compromised of late after visiting such kiosks. The students had been accessing their personal emails using the public shared computers available in the kiosks. What could be a potential reason for this breach?

  a. IP Spoofing

  b. Presence of a Ransomware on the public computers

  c. Presence of a Keylogger on the public computers

  d. Presence of a botnet on the public computers

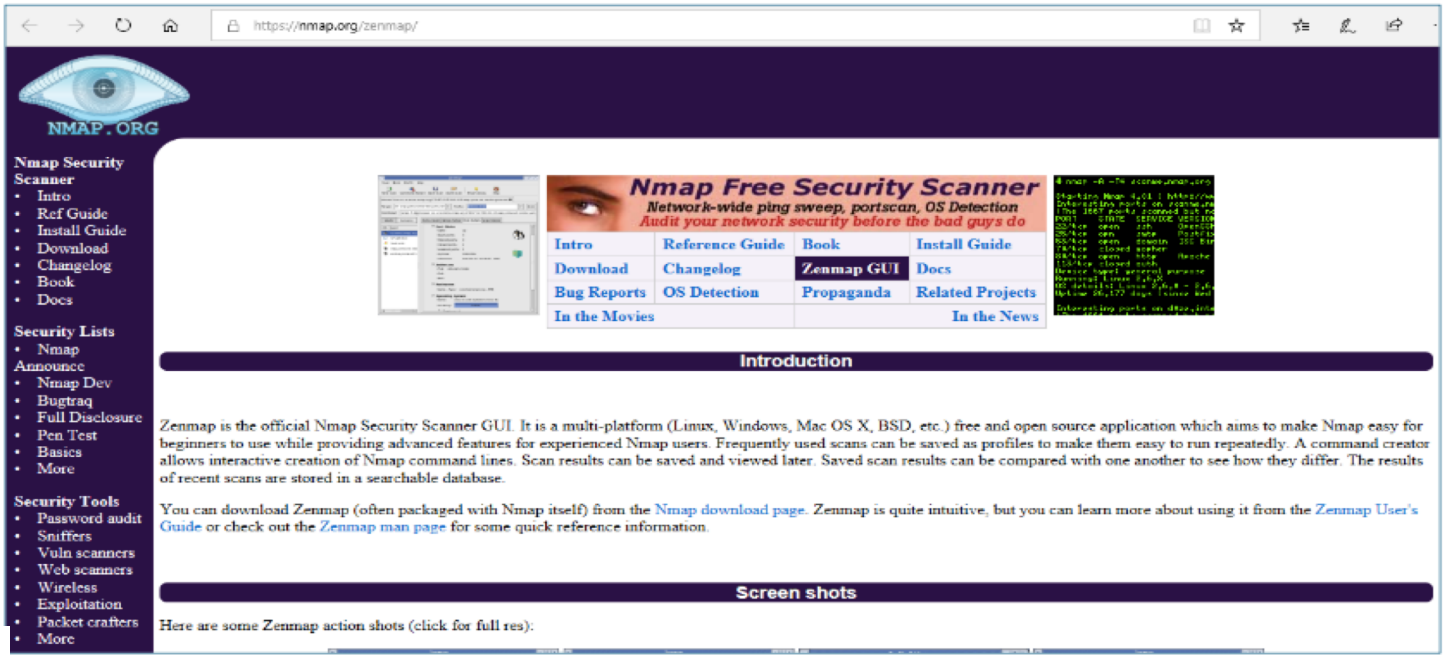
Answer c:
Explanation: A keylogger is a malware which records all the keyboard activity & sends back to the hacker. Such recorded activity may contain URL, User Names, Passwords and so on. Which makes it easy for an attacker to use this information against the victims

Demo 1: Footprinting

- As a part of information gathering or foot-printing phase gather the OS (operating system) version of the target web server
- Use **ID Serve** tool to gather the details of the web server
- Download and install **ID Serve** tool from the following location: https://www.grc.com/id/idserve.htm

Demo 2: Scanning And Enumerating

- Scan the target system to identify the various active services
- Enumerate the target to gather more information
- Use **Nmap/ Zenmap** tool to scan and enumerate
- Download and install **Zenmap** tool from the following location: https://nmap.org/zenmap/

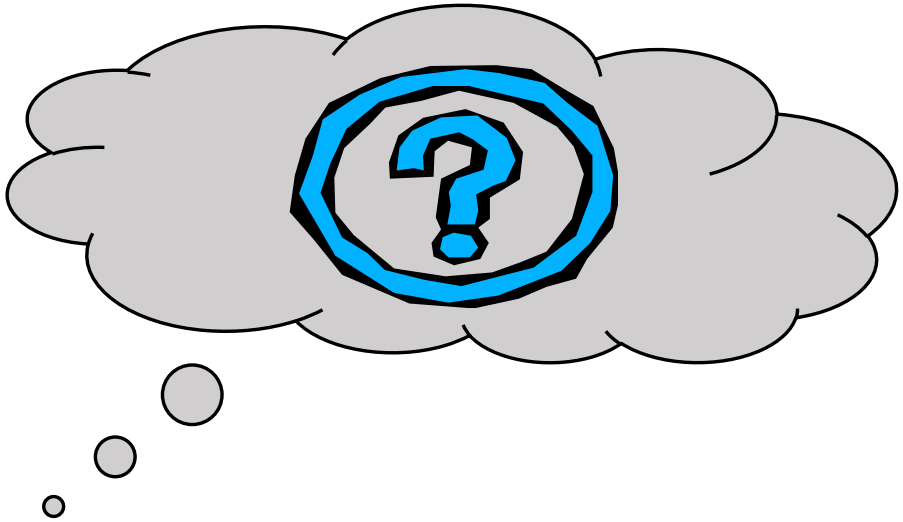


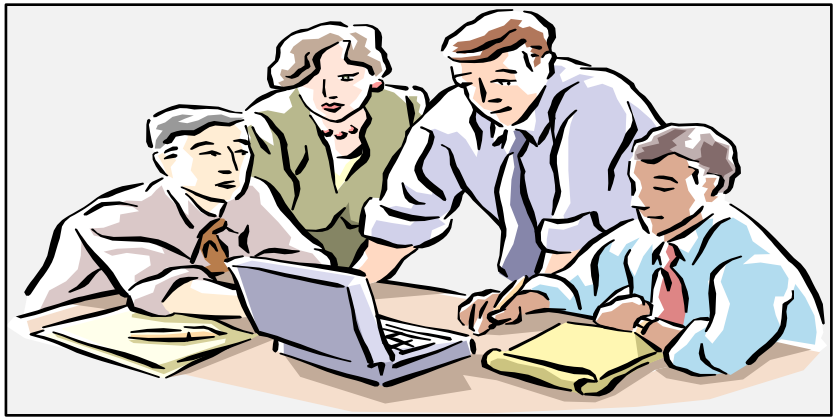
Summary

In this unit, you should have learnt:

- Cybercrime & types of Cybercrime
- Phases & Techniques of a typical Cyber Attack
- Cyber Security Framework
- Basic concepts of NIST Cyber Security Framework
- Incident Response

QUESTIONS PLEASE ☺





FTVETI

ICT @ FTVETI