Cybersecurity Management

T4 - Incident Response

marc.ruiz-ramirez@upc.edu

Objectives

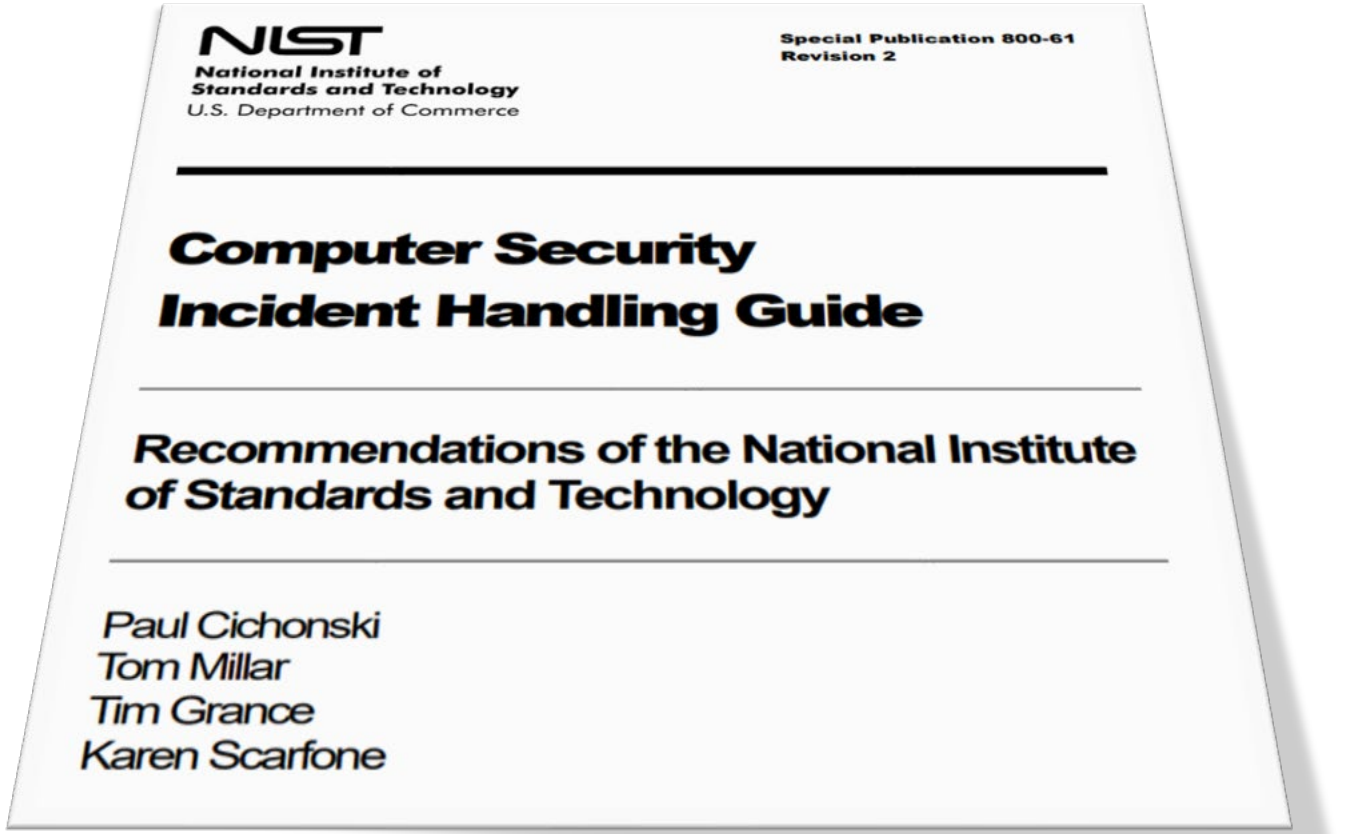
- To know the main concepts and definitions of IR.
- To know what a Computer Security Incident Response Team (CSIRT) is, how it is created, and what services it offers.
- To know the different phases of an incident response process.
- To know the primary forms to manage in an incident response process.
- To practice, using an example, a simulation of a IR.

Contents

- IR. Concepts & Definitions
- CSIRT
  - Creation
  - Services
- Incident Handling (or IR) Process
  - Preparation phase
  - Detection & Analysis phase
  - Containment, Eradication & Recovery (C,E&R) phase
  - Post-Incident Activity
- IR Forms
- Exercise: DDoS incident

IR. Concepts & Definitions

NIST Special Publication 800-61 Revision 2


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

For more information, please refer to Computer Security Incident Handling Guide by NIST.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Incident Response (IR). Definition

- Well-defined course of action whenever a computer or network security incident occurs.
- **NIST*** → only events with negative consequences are considered security incidents:
  - System crashes
  - Packet floods
  - Unauthorized use of system privileges
  - Unauthorized access to sensitive data
  - Execution of destructive malware
- IR. Scope
  - ***Incident handling is not only about intrusions!***
    - Malicious insiders, availability issues and loss of intellectual property all fall under the scope of incident handling as well.
- **Incident Response = Incident Handling**

**the Computer Security Incident Handling Guide by NIST*

Computer Security Incident Response Team (CSIRT)

CSIRT (CERT or IR Team). Definition

- NIST
  - *“An incident response team (IRT), also known as a Computer Security Incident Response Team (CSIRT) is responsible for providing incident response services to part or all of an organization.”*
- The IRT
  - Receives information on possible incidents
  - Investigates them
  - Takes action to ensure that the damage caused by the incidents is minimized.

CSIRT. Service Categories

Reactive Services	Proactive Services	Security Quality Management Services
• Alerts and Warnings • **Incident Handling** • Artifact Handling	• Announcements • Technology Watch • Security Audits or Assessments • Configuration and Maintenance of Security Tools, Applications, and Infrastructures • Development of Security Tools • Intrusion Detection Services • Security-Related Information Dis-semination	• Risk Analysis • Business Continuity and Disaster Recovery Planning • Security Consulting • Awareness Building • Education/Training • Product Evaluation or Certification
• *Are triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system.* • ***Core component** of CSIRT work.*	• *Provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events.* • *Performance of these services will directly reduce the number of incidents in the future.*	• *Augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organization such as the IT, audit, or training departments.*

CSIRT. Services.

Service Categories. Reactive Services

- Designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems.
- Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Reactive Services

- **Alerts and Warnings**
- **Incident Handling**
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
  - Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- **Artifact Handling**
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

CSIRT. Services.

Service Categories. Proactive Services

- Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Proactive Services

- **Announcements**
- **Technology Watch**
- **Security Audits or Assessments**
- **Configuration and Maintenance of Security Tools, Applications, and Infrastructures**
- **Development of Security Tools**
- **Intrusion Detection Services**
- **Security-Related Information Dissemination**

CSIRT. Services.

Service Categories. Security Quality Management Services

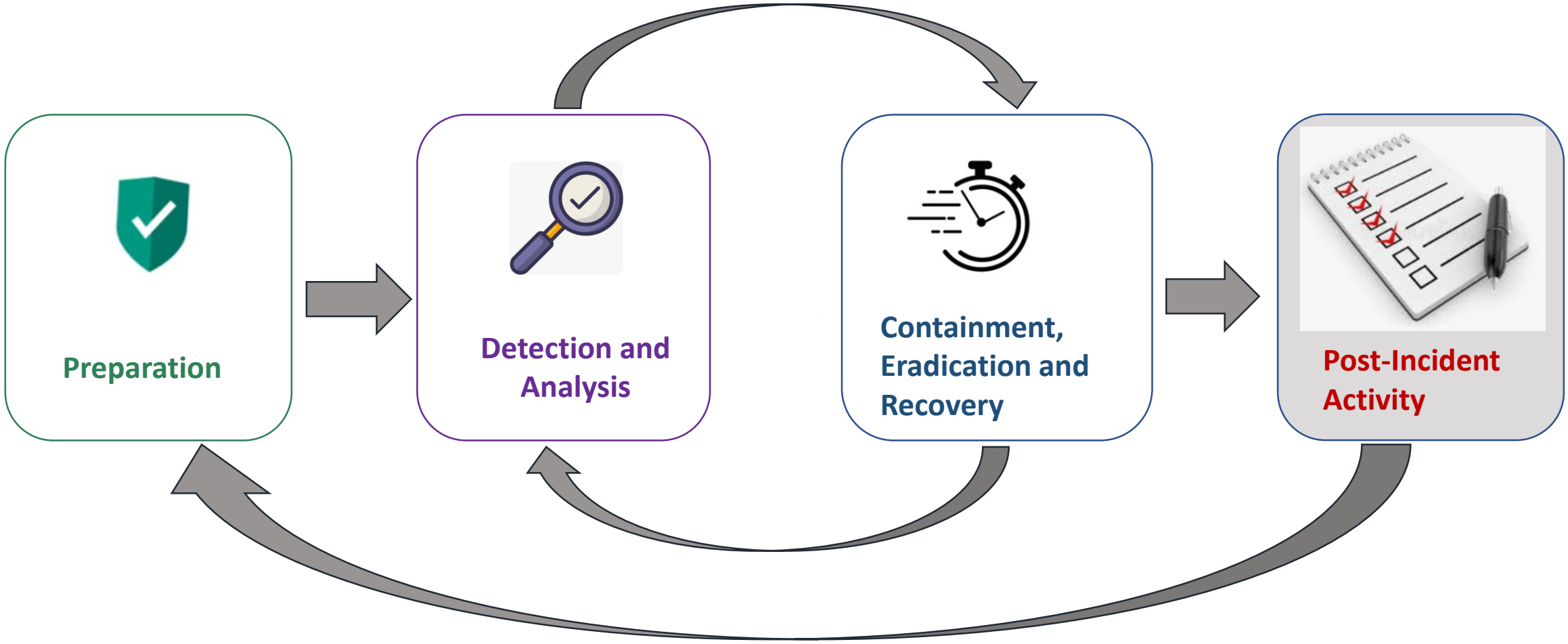
- Services designed to improve the overall security of an organization.
- By leveraging the experiences gained in providing the reactive and proactive services.
- These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks.

Security Quality Management Services
• **Risk Analysis** • **Business Continuity and Disaster Recovery Planning** • **Security Consulting** • **Awareness Building** • **Education/Training** • **Product Evaluation or Certification**

Incident Handling (or IR) Process

CSIRT Reactive Services

Incident response life cycle



NIST: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Incident response life cycle

- **Preparation**:
  - The organization prepares for potential incidents by creating an incident response plan, establishing incident response teams, and providing training to personnel.
  - Risk assessments and implementation of appropriate security controls.
- **Detection and Analysis**:
  - Incidents are detected and analyzed to determine the scope and nature of the incident.
    - Identification of the affected assets, evaluating the severity of the incident, and determining the root cause.
- **Containment, Eradication, and Recovery**:
  - The incident is contained to prevent further damage, eradicated to remove the threat, and the affected systems are recovered to normal operations.
  - Implementation of corrective actions to prevent similar incidents from occurring in the future.
- **Post-Incident Activity**:
  - A thorough review of the incident response process is conducted to identify areas for improvement.
  - Analyze the effectiveness of the incident response plan, evaluate the performance of incident response teams, and update policies and procedures based on lessons learned.

IRLC. Preparation phase

IRLC. Preparation phase

- Includes everything related to an organization's IR readiness.

Employees	Documentation	Defensive Measures
• A Skilled Response Team • IT Security Training • Security Awareness/ Social Engineering Exercises, etc.	• Well-defined policies • Well-defined response procedures • Maintaining a chain of custody of actions	• Antivirus, Intrusion Detection System (IDS), Data Loss Prevention (DLP), Endpoint Detection and Response (EDR), Security Patches • Security Information and Event Management (SIEM), Unified Threat Management (UTM), Threat Intelligence • Network Security Monitoring (NSM), Central Logging, Honeypots, etc.

IRLC. Preparation phase.

Key Points

- Establish and train a multi-disciplinary team
- Risk assessments to limit the number of incidents that will occur.
- Determine minimum time to respond.
- Access to systems capabilities.
- Establish a Single Point Of Contact for Information Security(SPOC) & reporting capabilities.

Incident Prevention

- Vulnerability Testing Tools
- Static techniques:
  - Static vulnerability analysis tools: Interact with assets, typically via network scanning, to identify information about available systems and based on databases of known vulnerabilities, produce reports highlighting important findings in terms of vulnerable assets, misconfigurations, etc.
- Dynamic techniques:
  - Dynamic vulnerability analysis tools
  - Penetration testing tools: More active in the scanning, compared to vulnerability analyser tools by, for instance, offering the option to try to exploit identified vulnerabilities. More specialised to specific types of assets.

Vulnerability analysis tools - Static

- SonarQube: Measure the source code quality of a web app and identify vulnerabilities
- Cppcheck: Code analysis tool to detect bugs and dangerous coding constructs. Static analysis tool for C/C++ code.
- OWASP Dependency Check: Detect publicly disclosed vulnerabilities contained within a project's dependencies.
- nvd-clojure (National Vulnerability Database dependency checker library): Detect vulnerabilities contained within project dependencies.

Vulnerability analysis tools - Dynamic

- OpenVAS: Vulnerability scanner and vulnerability management tool.
- Burp Suite: Tool for performingsecurity testing of web applications.
- Wapiti: WebApp vulnerability scanner. Scan web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data.
- Nikto Web server scanner: Vulnerability scanner that scans webservers for dangerous files/CGIs, and outdated server software.
- Grabber Vulnerability scanner: Black box web application vulnerability scanner that looks for SQL Injection, Blind SQL injection, XSS vulnerability and File include injection.

Penetration testing tools

Web Application testing

- W3af - Web Application Attack and Audit Framework: Web application security scanner which helps developers and penetration testers identify and exploit vulnerabilities in their web applications.
- SQLMap: Detection and exploitation of SQL injection flaws.
- Wfuzz: Automate web applications security assessments.
- OWASP Zed Attack Proxy (ZAP): Find vulnerabilities in web applications.

Penetration testing tools

Network Security Testing

- T50: Mixed packet injector for stress testing.
- Aircrack-ng: Tools suite to assess WiFi network security.
- Btljuice: Implements Man-in-the-Middle attacks on Bluetooth Low Energy devices.
- Spooftooph: Automated tool for spoofing or cloning Bluetooth device information.
- Nogotofail: To test TLS/SSL connections.

Penetration testing tools

Security Control Testing for specific security controls (e.g., antivirus)

- Veil: Tool designed to generate Metasploit payloads that bypass common anti-virus solutions.
- Hyperion: Runtime encrypter for 32-bit portable executables.
- Phantom Evasion: For polymorphic code and antivirus sandbox detection techniques to evade Antivirus software.

Social Engineering

- Social Engineering Toolkit (SET): Social engineering penetration testing framework.
- KingPhisher: Phishing campaign toolkit to run user awareness training campaigns.

IRLC. Detection & Analysis phase

IRLC. Detection & Analysis phase

- IR most challenging part: Detect and assess accurately a possible incident
  - Determining whether an incident has occurred
  - Type, extent, and magnitude of the problem
- Combination of three factors:
  - Different means to detect incidents:
    - Automated detection: IDPSs, antivirus software, and log analyzers.
    - Manual detection: Problems reported by users.
  - The volume of potential signs of incidents is typically high
    - Organizations can receive thousands or even millions of intrusion detection sensor alerts per day.
  - Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

Incidents

- Organizations should be generally prepared to handle any incident
  - Specially incidents that use common attack vectors.
- Response strategies defined according to the type of incident
- Common attack vectors:
  - **External/Removable Media**: An attack executed from removable media or a peripheral device
    - Ex: Malicious code spreading onto a system from an infected USB flash drive.
  - **Attrition**: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services
    - Ex: DDoS intended to impair or deny access to a service or application; A brute force attack against an authentication mechanism (passwords).
  - **Web**: An attack executed from a website or web-based application
    - Ex: A cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
  - **Email**: An attack executed via an email message or attachment
    - Ex: Link to a malicious website in the body of an email message.
  - **Impersonation**: An attack involving replacement of something benign with something malicious
    - Ex: Man in the middle or SQL injection attacks.
  - **Improper Usage**: Any incident resulting from violation of an organization's usage policies by an authorized user.
  - **Loss or Theft of Equipment**: The loss or theft of a computing device or media used by the organization (laptop, smartphone, etc.)

Detection of incidents

- Signs of an incident fall into two categories:
  - Precursor: is a sign that an incident may occur in the future
  - Indicator is a sign that an incident may have occurred or may be occurring now
- Precursors and indicators are identified using many different sources:
  - Computer security software alerts
  - Logs
  - Publicly available information
  - People

Precursors and Indicators

- Intrusion Detection and Prevention System (IDPS): Identify suspicious events and record pertinent data regarding them.
- Security Information and Event Management (SIEM): Similar to IDPS, but generate alerts based on analysis of log data.
- Antivirus and antispam software: Detects various forms of malware, generates alerts, and prevents the malware from infecting hosts.
- File integrity checking software : Detect changes made to important files during incidents using hashing algorithms.
- Third-party monitoring services: Offer a variety of subscription-based and free monitoring services.
  - Ex: Fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations.

IDPS

- Monitor network traffic, analyze it and provide remediation tactics when malicious behavior is detected.
- Functionalities:
  - Detection: Identify malicious behaviors and log and send alerts.
  - Prevention: Response based on predetermined criteria of types of attacks to block or drop malicious traffic or processes when are detected.
- IDPS tools detect malware, web-based threats (e.g., DDoS) and socially engineered attacks.

IDPS

- Trend Micro TippingPoint Next-Generation Intrusion Prevention System (NGIPS)
- Cisco Firepower Next-Generation IPS (NGIPS)
- Trellix Network Security
- NSFOCUS
- OSSEC HIDS
- Snort
- ThreatBlockr

SIEM

- Monitor and analyze security related events and activities of organizations
- Functionalities: Collection, aggregation, normalization, correlation and analysis of real-time and historical security events.
- Objectives:
  - Provide security professionals with valuable insights into potential security threats.
  - Allow to identify, prioritize, and respond to security incidents effectively.

SIEM

- OSSIM: SIEM platform that combines event collection, processing, normalization, and correlation. It includes open-source projects, as OSSEC, Snort, Suricata and OpenVAS tools.
- ELK stack: SIEM platform comprising Elasticsearch (search and analytics engine), Logstash (server-side data processing pipeline that ingests data from multiple sources) and Kibana (visualisation layer).
- Prelude OSS: SIEM for collecting, normalising, sorting, aggregating, visualising, and reporting security-related events aggregated from various types of logs using the unified format IDMEF (defined in IETF's RFC4765).
- SIEMonster: SIEM framework consisting on open -source tools (e.g., ELK, Wazuh, and threat intelligence solutions). Support for cloud deployment (through Docker containers or VMs).
- Wazuh: Open-source platform that provides prevention, detection, and response capabilities. It has its own multi-platform agent that runs on the endpoints to be monitored.
- OSSEC: Host-based Intrusion detection system that performs integrity checking, windows registry monitoring, rootkit detection, time-based alerting, and active response. It has a centralized architecture for logs' analysis and correlation from multiple devices and formats.

IRLC. Detection & Analysis phase.

Damage-estimation questions

- Have we identified the impact of vulnerability exploitation?
- Are there any crown jewels that can be affected?
- What are the minimum requirements for effective exploitation?
- Is this being actively exploited in the wild?
- Is there a proposed remediation strategy?
- Is there threat intel/evidence that suggests increased spreading capabilities?

IRLC. Containment, Eradication & Recovery (C,E&R) phase

IRLC. C,E&R phase

- Includes everything related to

Containment	Eradication	Recovery

• Preventing an incident from getting worse
• Subphases
  • Short-Term Containment
  • System Back-Up
  • Long-Term Containment
	• Eliminating intruder artifacts
	• Understanding the root cause
	• Attack vectors and tactics, techniques & procedures (TTPs)
		• Restoring
		• Monitoring

IRLC. C,E&R phase.

Before Containment. Very first steps

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:

IRLC. C,E&R phase.

Before Containment. Incident Classification

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:
  - **Type**

Denial of Service
External Exploitation
Internal Exploitation
Information Leakage
Malware
Malicious Email

IRLC. C,E&R phase.

Before Containment. Incident Classification

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:
  - Type
  - **Impact**

Incident affecting critical system(s)
Incident affecting non-critical system(s)
Incident affecting asset that requires no immediate investigation

***Impact is tightly connected with the Response Time*.**

IRLC. C,E&R phase.

Before Containment. Incident Classification

- Identify if we are dealing with a malicious insider or not.
- Isolate the area under investigation.
- Utilize incident casualty forms.
- Classify it based on:
  - Type
  - Impact
  - **Extend**

- Extensive compromise, including sensitive customer information
- Manageable intrusion and spreading
- Immediately detected or easily contained intrusion

Extent is tightly connected with the escalation level. For example, should the CISO's office or upper management be informed?

IRLC. C,E&R phase.

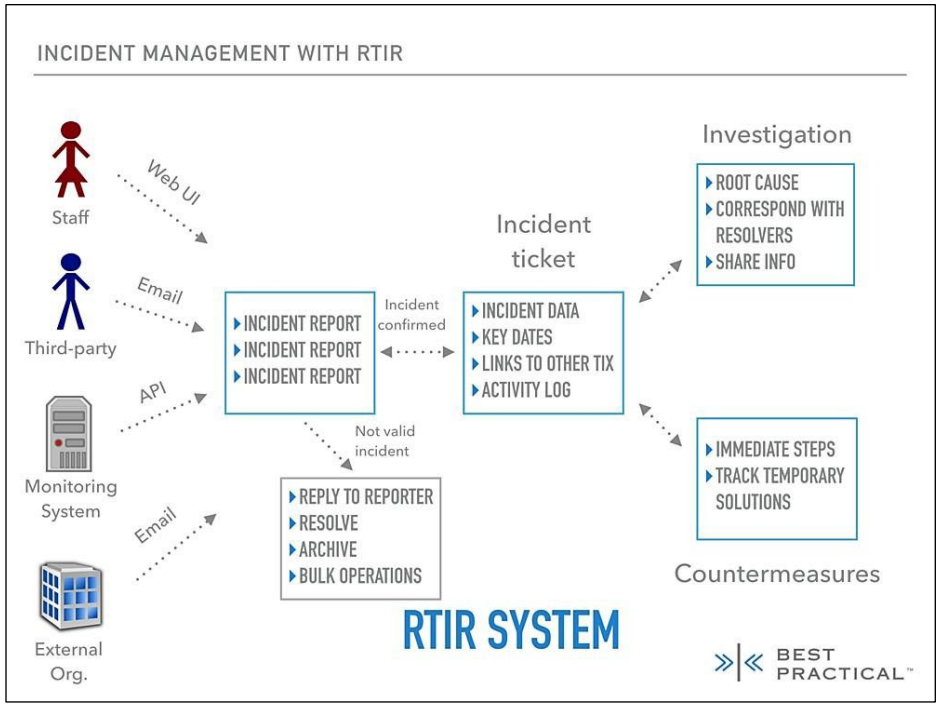
Before Containment. Incident Communication

- Senior management member
  - CIO/CISO/head of the legal dept., etc.
  - Escalating or help
  - Should be the first upper management individual who will be informed of an incident and provided with notes from the first responder.
- The communication flow should include
  - Security + Management (people) → affected business units will be informed

IRLC. C,E&R phase.

Before Containment. Incident Tracking Mechanism

- Handle multiple incidents
- Incident reporting mechanism
  - All tickets for the same incident.
- Example Tool
  - Request Tracker for Incident Response (RTIR)

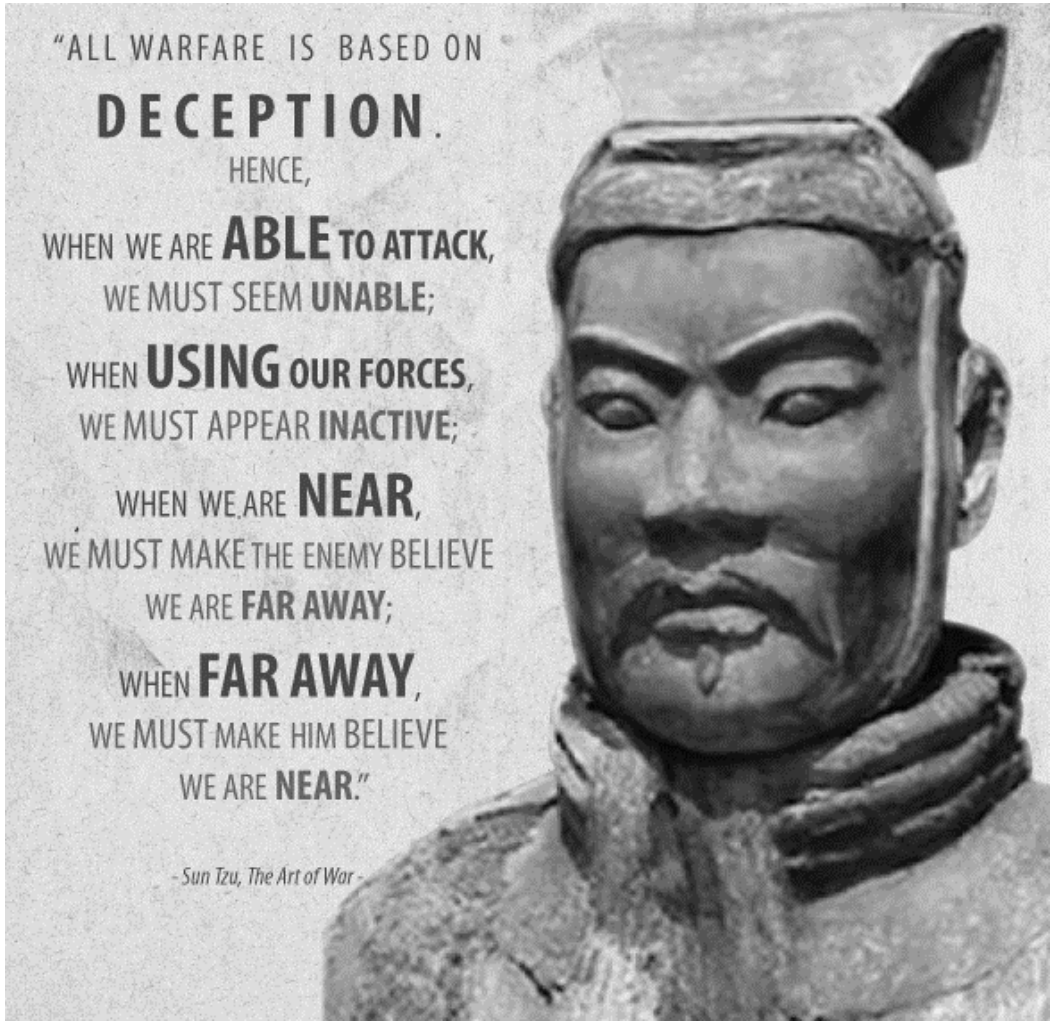


IRLC. C,E&R phase.

Before Containment. Low profile

- We should be
  - extremely careful
  - not to let the adversaries now our operations
  - no uploading binaries to cloud
  - no interacting infrastructures

- Act normally…



IRLC. C,E&R phase.

Containment

- Important before an incident overwhelms resources or increases damage.
- Provide time for developing a tailored remediation strategy.
- An essential part of containment is decision-making:
  - Ex: shut down a system, disconnect it from a network, disable certain functions.
- Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident.
- Organizations shall define containment strategies for each major incident type:
  - With criteria documented clearly to facilitate decision-making.

IRLC. C,E&R phase.

Containment

- Criteria for determining the appropriate containment strategy:
  - Potential damage to and theft of resources
  - Need for evidence preservation
  - Service availability (e.g., network connectivity, services provided to external parties)
  - Time and resources needed to implement the strategy
  - Effectiveness of the strategy
  - Duration of the solution
    - Ex: Emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution.

IRLC. C,E&R phase.

Containment. Subphases

- Containment is divided into the following subphases:
  - Short-term Containment
  - System Back-up
  - Long-term Containment

IRLC. C,E&R phase.

Containment. Short-term Containment

- Objective: Limit damage before the incident gets worse
- Eliminate intrusion → without erasing tracks
- Actions
  - Isolating network segments
  - Isolate the machine
  - Taking down hacked production server

IRLC. C,E&R phase.

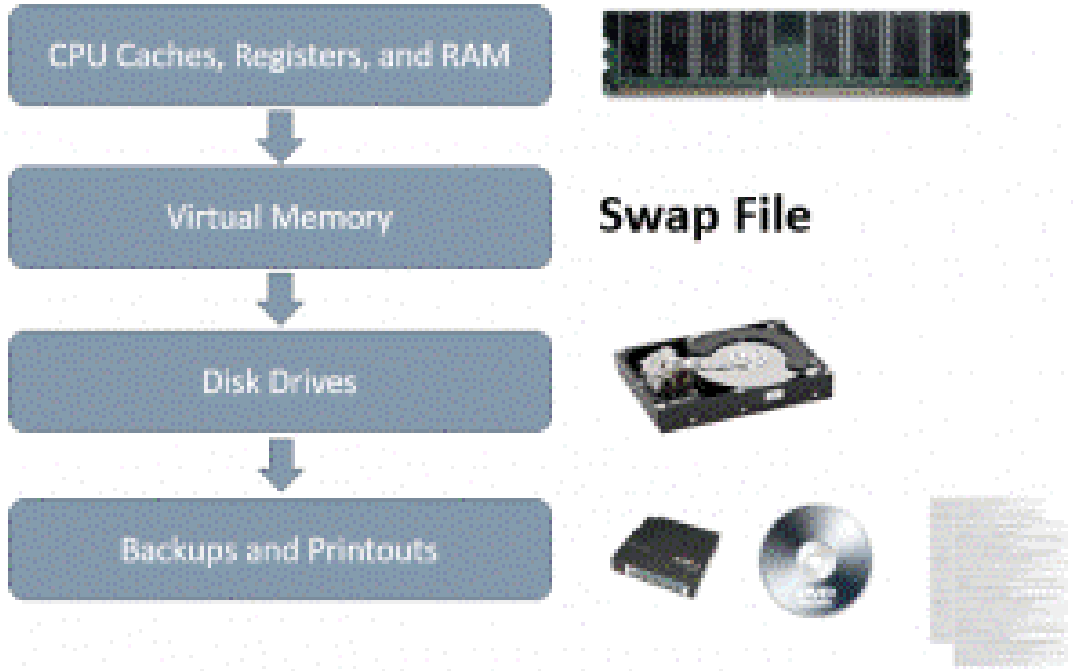
Containment. System Back-Up

- The next step is to take forensic image of the affected system(s) for forensics activities.
  - Forensic Tool Kit (FTK)
  - EnCase
- The, wipe and reimage the systems.
- Objective: Preserve evidence from the attack that can be used in court, and also for further investigation of the incident and lessons learned.

IRLC. C,E&R phase.

Containment. System Back-Up. Data Acquisition (DA)

- Preservation of evidence
  - → working with images
- Original image (oi)
  - saved
  - work with copies of the oi
- Data acquisition
  - → **order of volatility**
    - RAM → VMEm → ..



IRLC. C,E&R phase.

Containment. System Back-Up. DA. Types

- **Static Acquisition**
  - No volatile data (hard disks, flash disks).
- **Dynamic / Live Acquisition**
  - Volatile data.
  - Performed while a system is still powered on
  - RAM → find stored passwords, messages, domain names and IP address, etc …
  - Can also exist on disk → paging, temporary files, and even log files.
  - OS cannot be entirely trusted → rootkits
- Choosing which technique to apply depends on data volatility and the incident

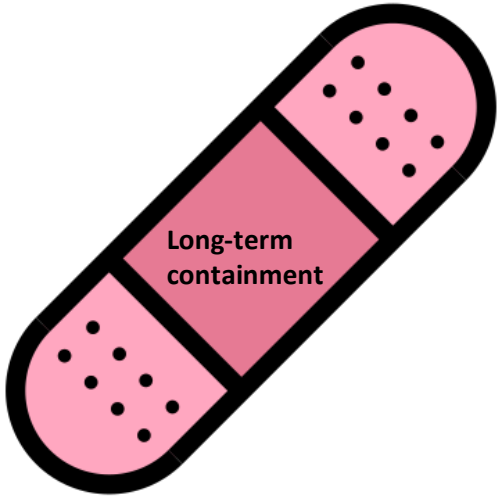
IRLC. C,E&R phase.

Containment. Long-term Containment

- Long-term containment by applying temporary fixes to make it possible to bring production systems back up.
- The primary focus is removing accounts or backdoors left by attackers on the systems, and addressing the root cause
  - Ex: Fixing a broken authentication mechanism or patching a vulnerability that led to the attack.

IRLC. C,E&R phase.
Eradication.

- After an incident has been contained, eradication may be necessary to eliminate components of the incident
  - Ex: Deleting malware and disabling breached user accounts
- Eradication
  - to make sure the attacker is locked out
  - to identify the root cause and indicators of the incident.
    - Use information from the **Detection & Analysis** and **Containment**
  - to isolate the intrusion and identify the **attack vector**.
  - Drive-wiping before doing anything else.
    - ***Reformatting and reinstalling the OS or identifying a clean backup and reloading the data ONLY is a bad strategy!***



IRLC. C,E&R phase.
Eradication.Important phases

- Eliminating attacker residuals
  - Removing malware (backdoors, rootkits, malicious kernel-mode drivers, etc.)
  - Identify credential reuse (Remote Desktop, SSH, VNC, etc.)
- Improving defenses
  - Configuring additional router & firewall rules
  - Obscuring the affected system’s position
  - Null routing (DDoS)
  - System hardening, patching, and vulnerability assessment procedures, etc.

IRLC. C,E&R phase.

Recovery.

- Recovery → we will bring the affected systems back to production.
- Key points to consider are:
  - Process System Recovery
  - Restore of Operations
  - Monitoring

IRLC. C,E&R phase.

Recovery. Process System Recovery

- Once the affected system is restored, ask **the business unit** to
  - perform QA activities to ensure the system's running condition.
  - ensure the system includes everything needed for their operations.

IRLC. C,E&R phase.

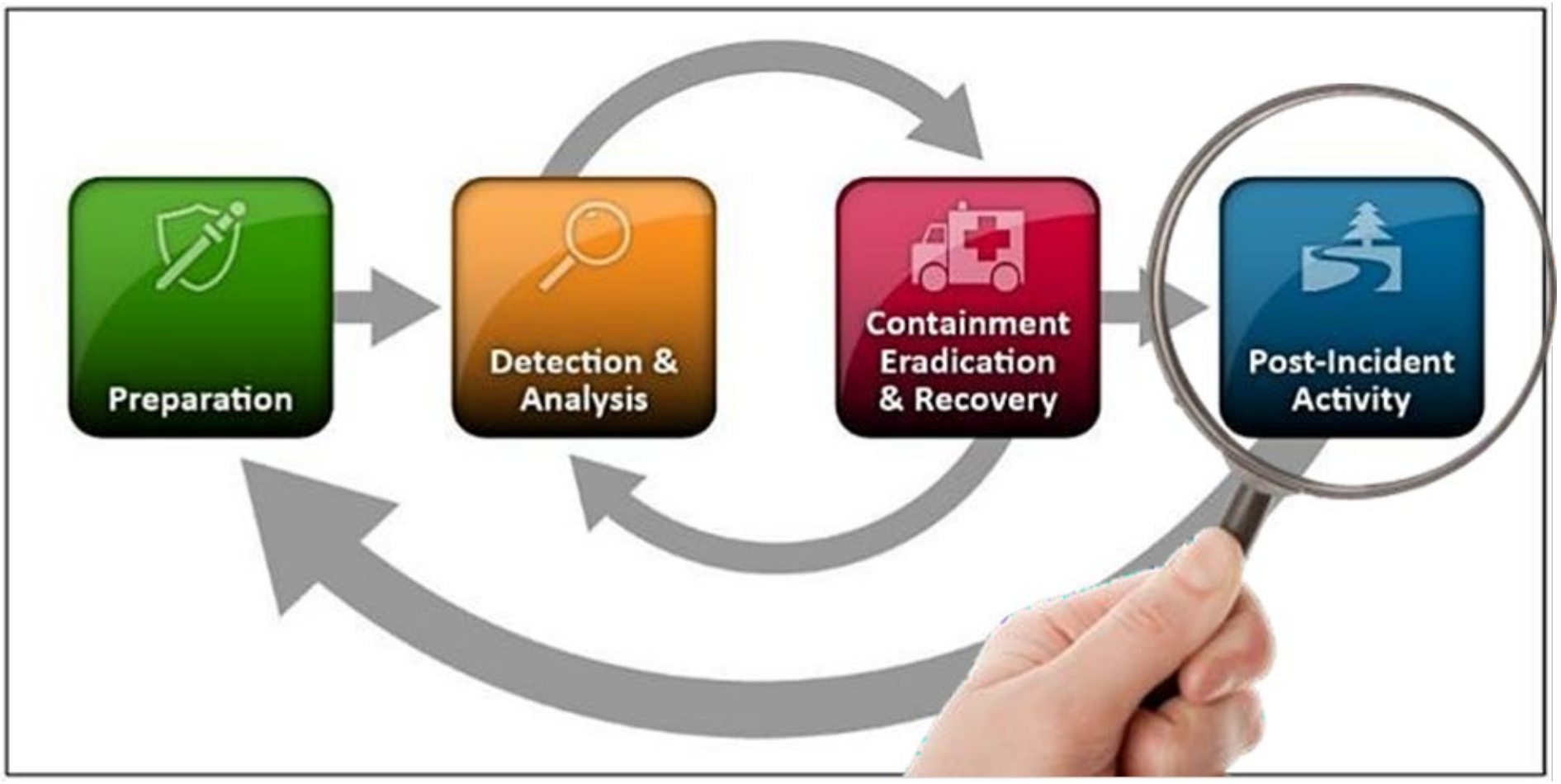
Recovery. Restore of Operations

- A decision has to be made regarding when the restored system will enter production again.
- Consult/coordinate with the business unit for this matter.

IRLC. C,E&R phase.
Recovery. Monitoring

- Once the restored system is back to production:
  - Backdoors may still exist!
  - IDPS → signs/patterns/signatures related to the original attack.
  - Analyze critical logs and events → signs of re-infection or re-compromise.
  - What to look for during the weeks (or even months) to come:
    - Changes to registry keys and values.
    - Abnormal processes
    - Abnormal user accounts.

IRLC. Post-Incident Activity



IRLC. Post-Incident Activity

- Right after recovery, the IRT should start constructing an objective, accurate and thorough **report** regarding the **lessons learned** from IR.
  - Identified weaknesses, oversights, and blind spots
  - Working processes and successful detection methods should also be included.
  - Don’t be afraid to mention how effective you were against specific stages of the attack.
- Schedule a meeting to discuss this report with all involved parties
  - System administrators, affected business unit representatives, IT security team, etc.
- Focus your energy on improving your processes, technological measures and **visibility**.

IR Forms

IR Forms

- There are IR Forms, which will come in handy during incident handling. Let’s look at some important forms you should preprint and use.
  - **Incident Contact List**
  - **Incident Detection**
  - **Incident Casualties**
  - **Incident Containment**
  - **Incident Eradication**

IR Forms.

Incident Contact List

- This form should contain the contact details of the organization’s:
  - CISO / CIO
  - SPOC of the incident handling or CSIRT team
  - Legal department contact
  - Public relations contact
  - ISP SPOC
  - Local cybercrime unit etc.

IR Forms.

Incident Detection

- This form should contain information such as:
  - The first person who detected the incident
  - The incident’s summary (type of incident, incident location, incident detection details, etc.)

IR Forms.
Incident Casualties

- This form should contain information such as:
  - Location of affected systems
  - Date and time incident handlers arrived
  - Affected system details (one form per affected system is advised)
    - Hardware vendor
    - Serial number
    - Network connectivity details
    - o Host Name | IP Address | MAC Address

IR Forms.
Incident Containment

- This form should contain information such as:
  - Isolation activities per affected system
    - Was the affected system isolated?
      - Date and time the system was isolated
      - Way of system's isolation
  - Back-up activities per affected system
    - Handler who performed the restoration
    - Back-up details etc.

IR Forms.
Incident Eradication.

- This form should contain information such as: (one form per affected system is advised)
  - Handler(s) performing investigation on the system
  - Was the incident’s root cause discovered?
    - Incident root cause analysis
  - Actions taken to ensure the incident’s root cause was remediated and the possibility of a new incident eliminated

Exercise: DDoS incident

IR. DDoS

What is a DDoS attack?

https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

DDoS

- Disrupt the normal traffic of a server, service or network
  - Overwhelming the target or its surrounding infrastructure with a flood of Internet traffic
- Carried out by networks of Internet-connected machines (bots)
  - Infected with malware and controlled remotely by an attacker.
  - Bots send requests to the to the target's IP address → Causing the server or network to become overwhelmed.
- Each bot is a legitimate Internet device:
  - Separating the malicious traffic from legitimate traffic is difficult.

Layer 7 DDoS – Application layer attacks

- Goal: Exhaust the target's resources to create a DoS.
- The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests.
  - A HTTP request is computationally cheap to execute (client side)
  - It can be expensive to generate the response (server often loads multiple files and runs database queries in order to create a web page) (server side)
- Example: **HTTP flood**
- Large numbers of HTTP requests flood the server resulting in DoS.
  - This attack is similar to pressing refresh in a web browser over and over on many different computers at once
- Simpler version: Access one URL with the same range of attacking IP addresses referrers and user agents.
- Complex versions: Use a large number of attacking IP addresses and target random urls using random referrers and user agents.

DDoS - Protocol attacks

- Goal: Cause a service disruption by over-consuming server resources and/or the resources of network equipment (firewalls and load balancers).
- Exploit weaknesses in layers 3 and 4 of the protocol stack to render the target inaccessible.
- Example: **SYN flood**
- This attack exploits the TCP handshake (the sequence of communications by which two computers initiate a network connection)
  - by sending a target a large number of TCP “Initial Connection Request” SYN packets
    - with spoofed source IP addresses.
- The target machine responds to each connection request and then waits for the final step in the handshake which never occurs.

DDoS - Volumetric attacks

- Goal: Create congestion by consuming all available bandwidth between the target and the larger Internet.
  - Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.
- Example: **DNS amplification**
- By making a request to an open DNS server with a spoofed IP address (the IP address of the victim), the target IP address then receives a response from the server.

IR. DDoS.

Preparation

- **Objective**: Establish contacts, define procedures, and gather information to save time during an attack.
- **Actions**
  - ISP
  - Network infrastructure
  - Internal contacts

The "preparation" phase is to be considered as the most important element of a successful DDoS incident response!

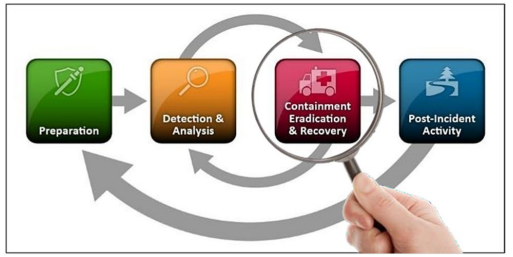
IR. DDoS.

Detection & Analysis

- **Objective**: Detect the incident, determine its scope, and involve the appropriate parties.
- **Actions**
  - Analyze the attack
  - Involve internal and external actors
  - Check the background

IR. DDoS.

Containment, Eradication & Recovery



Containment	Eradication	Recovery

• **Objective**
  • Mitigate the attack's effects on the targeted environment.
• **Actions**
  • Block DDoS traffic?
  • Alternate communication channel between you and your users/customers
	• **Objective**
	  • Take actions to stop the Denial of Service condition.
	• **Actions**
	  • Filtering Traffic
	  • Blackhole Routing
		• **Objective**:
		  • Come back to the previous functional state.
		• **Actions**
		  • Assess the end of the DDoS condition
		  • Rollback the mitigation measures

IR. DDoS.

Post-Incident Activity

- **Objective**
  - Document the incident's details, discuss lessons learned, and adjust plans and defenses.
- **Actions**
  - Consider what preparation steps you could have taken to respond to the incident faster or more effectively.
  - If necessary, adjust assumptions that affected the decisions made during DDoS incident preparation.
  - Assess the effectiveness of your DDoS response process, involving people and communications.
  - Consider what relationships inside and outside your organizations could help you with future incidents.
  - Collaborate with legal teams if a legal action is in process.

References

Links

- *https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/software*
- *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*
- *RFC-2350: http: //escert.upc.edu/rfc-2350*
- *https://www.trusted- introducer.org/directory/teams/escert-upc.html*
- *https://first.org/members/teams/escert-upc*
- *https://www.csirt.es/index.php/es/objetivos*
- *https://ciberseguretat.gencat.cat/ca/funcio-i- serveis/resposta-incidents/*
- *https://www.ccn-cert.cni.es/gestion-de- incidentes/directrices-para-la-gestion-de- incidentes.html*
- *https://www.misp-project.org/*

Links

- *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*
- *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*
- *https://www.wireshark.org/*
- *http://www.dmi.unipg.it/bista/didattica/sicurezza-pg/seminari2008-09/seminario_neri/seminario_neri.pdf*
- *http://www.iana.org/assignments/service-names-port-numbers/service-names-port- numbers.xhtml*
- *https://www.speedguide.net/ports.php*
- *https://docs.microsoft.com/en-us/azure/security/azure-log-audit*
- *https://www.first.org/resources/guides/csirt_case_classification.html*
- *https://bestpractical.com/rtir/*
- *https://github.com/meirwah/awesome-incident-response#incident-management*

Links

- *http://canarytokens.org/generate*
- *https://docs.microsoft.com/en-us/sysinternals/downloads/procmon*
- *http://www.chkrootkit.org/*
- *https://github.com/Tripwire/tripwire-open-source*
- *https://sourceforge.net/projects/aide/*
- *https://medium.com/@esmerycornielle/memory-management-paging-43b85abe6d2f*
- *https://www.heficed.com/kb/security/what-is-a-null-route/*
- *https://www.commandlinefu.com/commands/browse*
- *https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns*
- *https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer*