



Yesterday

Today

Tomorrow

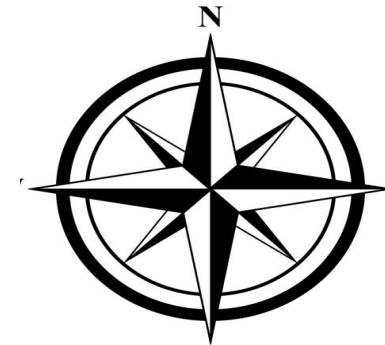
**PROF. DR. JUAN CARLOS BARRERA**

**CYBER-SECURITY (BC6)**

July 2020

Online Germany

Broadcasting from USA



**Preparation**

# **Vulnerability and Threat Management**

Agenda:

1) Incident Management & Security Vulnerability

2) Videos: Discussion & Reflection

3) Third Lab

4) Ahead of Cybersecurity

5) In Closing: Debriefing for Cases

# Safety & Security

- **Cyber Incident:** An occurrence that *actually* or *potentially* results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
- **Cyber Event:** any *actual* unauthorized, accidental or unlawful access, use, exfiltration, theft, disablement, destruction, loss, alteration, disclosure, transmission of any IT Assets owned or used by or on behalf of either party or any member of its Group, or any information or data (including any personally identifiable information) stored therein or transmitted thereby.

# 1) Incident Management

## Incident – Operational Definition

- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

## Examples

- Denial of service attack causes web server to crash
- Malware installed from a phishing attack infects user computers and establishes connections with an external host
- An attacker obtains sensitive data and demands ransom from your CEO to prevent release
- Sensitive information from your company is being disseminated through peer-to-peer file sharing services

# Incidents...

## Incidents would not happen if

- We had infinite security budgets, and
- We had infinitely capable security personnel

## However, things can go wrong

- In spite of your best attempts
- We call them incidents

## Useful to develop standard procedures to respond to incidents

- and to refine these procedures based on experience
- Typical business process improvement exercise

### Incident management cycle in NIST SP 800-61:

- ❖ Preparation.
- ❖ Detection and analysis.
- ❖ Containment, Eradication, and Recovery.
- ❖ Post-Incident Activity.

### Incident management cycle in ISO/IEC 27035:

- ❖ Plan and Prepare.
- ❖ Detection and Reporting.
- ❖ Assessment and Decision.
- ❖ Responses.
- ❖ Lessons Learnt.

# Incident Management

## Incident Handling

- Described in NIST 800-61 rev.2
- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery, and
- Post-Incident Analysis



# Preparation

- **PREPARATION:** is the first step in creating an incident response plan
- **Not an enumeration process**
- Listing all possible threat scenarios
- and adding the appropriate response to each of these scenarios
  
- **More productive**
- Identify basic steps common to all events
- Plan execution of each of these steps



# Incident Preparation Components

## Peacetime activity

- 1) Incident response policy
- 2) Incident response team
- 3) Supporting team
- 4) Incident communication
- 5) Compliance
- 6) Hardware and software
- 7) Training



# 1) Incident Response Policy

- Description of standard methods used by the organization for handling Information Security Incidents

## **Benefits of policy**

- Helps focus on incident as a whole, from start to finish
- Without getting diverted by media and organizational pressures
- Discussions provide management with understanding of issues they may have to deal with during an actual incident
- Impacts of planned controls can be assessed by stakeholders
- May not be anticipated by IT team
- Reassurance for users

## 2) Incident Response Team

### Staff designated to respond to incidents

- Develop experience over time about expectations of organization during incidents
- Often cross-departmental
- Managers have to spare IRT members when needed
- You may consider to conduct “Drill” exercises.



# Responsibilities

- Quickly identifying threats to the data infrastructure
- Assessing the level of risk
- Taking immediate steps to mitigate risks
- Notifying management of the event and associated risk
- Notifying local personnel of any incident involving their resources
- Issuing a final report as needed, including lessons learned
- Roles of each member of the IRT must be part of the incident response policy
- A large organization may need multiple IRTs and One within each division of the organization
- A central group decided when events start crossing boundaries of the affected division

# Incident Response Team IRT

## **The IRT will have one chair, usually a senior security analyst**

- Coordinates with external stakeholders
- Helps other IRT members to perform their functions
- Needs high credibility within the organization
- For competence
- Excellent communication skills, both oral and in writing
- Enough technical background to understand the situation
- Judgment to make split second, educated decisions based on the status updates

# IRT

## **Technical members of IRT selected depending on the threat action, e.g.**

- If an Oracle database was breached due to a compromised administrator account on the Operating System, the IRT may include the following members
- A person familiar with the OS to look at the OS system and logs
- A Database Administrator to examine Oracle database, contents, and logs
- Try to determine if anything was altered.
- A Network Engineer to review firewall and/or netflow logs observe any unusual traffic
- Desktop Services personnel if desktop machines facilitated the attack

# IRT Interactions with Stakeholders



### 3) Supporting Team

**Communication is an important aspect of the duties of the IRT**

- Extreme interest among different constituencies for information
- Potentially conflicting needs
- Often not enough information for satisfactory response

**Resist temptation of conveying speculation as informed “expert” opinion**

**Need-to-know principle**

- People only provided information necessary to perform their job



## Cont'd

### **In communication with general public, supporting team advisable**

- Media Relations has the know-how and experience on dealing with media
- Legal Counsel can verify federal or state disclosure laws
- Unintended disclosure may have severe financial and public relation consequences
- Law Enforcement for government cover and credibility

### **Minimize rumor-mongering, ill-informed publicity and general disorder**

# 4) Incident Communications

## Inbound communications

- Information about occurrence of incident

## Outbound communications

- Notifications to affected people



# Inbound Communications:

## **Direct Report**

- Asset owner or custodian may report the incident
- E.g. observing unusual computer behavior

## **Anonymous Report**

- Web forms to report an issue anonymously without fear of reprisal
- E.g. Allegations that a high ranking University official is printing pornographic material on University printers
- Public relations risk, sexual harassment lawsuits

## Inbound Communications (cont'd):

### **Help Desk**

- Problem resolution may reveal problems
- E.g. misconfiguration of shared network drives

### **Self-Audit**

- Periodical vulnerability assessment and log analysis may identify breaches
- Stress Testing
- Other

## Outbound communications:

### **Affected people are curious**

### **IT Personnel and the IT Help Desk**

- Users quickly overwhelm Help Desk when essential assets are affected
- Immediate updates to remove exploited vulnerability

### **Inform managers and other executives periodically**

- Even if nothing has changed
- Prevents distracting phone calls to engineers working on containment and eradication of the problem
- Quick text messages and brief email messages with status updates are adequate

## Outbound communications (cont'd):

### **End Users and Customers**

- Get very edgy when they don't know what is going on
- 2 questions
- When will the system be back?
- What happened?

## 5) Compliance

**Act of following applicable laws, regulations, rules, industry codes and contractual obligations**

- Ideally, best-practices developed to avoid well-known past mistakes
- In practice, often important mainly because non-compliance leads to avoidable penalties

**Need to comply with incident response requirements applicable to your context**

**Example:**

*Federal Information Security Management Act (FISMA)*

*Requires Federal agencies to establish incident response capabilities*

*Each Federal civilian agency must designate a primary and secondary point of contact with US-CERT United States Computer Emergency Readiness Team*

## 6) Hardware and Software

**To be effective, IRT needs appropriate tools**

**Sampling of the hardware and software recommended by NIST 800-61 rev.2 for incident response includes**

- Backup devices to create disk images or other incident data
- Laptops for gathering, analyzing data, and writing reports
- Spare computer hardware for “crash and burn” purposes, such as trying out malware and other payload found and considered “unknown.”
- Packet analyzers to capture and analyze network traffic
- Digital forensics software to recover erased data, etc.



## 7) Training

**Awareness of a baseline set of information on all aspects of security, e.g.**

- Access Control / Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Cryptography
- Security Architecture and Design / Security Operations
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance / Physical (Environmental) Security
- **Other facets of training**
- Media Relations

# Incident Documentation

## **NIST recommendations for minimal information**

- Current status of the incident / Summary of the incident
- Indicators related to the incident / Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable / Impact assessments related to the incident
- Contact information for other involved parties
- List of evidence gathered during the incident investigation
- Comments from incident handlers / Next steps to be taken

# Security Vulnerability

**Vulnerability:** refers to the inability of a system to withstand the effects of a hostile environment.

**In a Computer system:** a vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

**Exploit:** means to take advantage of something for one's end, specially unethically or unjustifiably. An exploit is a piece of software that takes advantage of a bug or vulnerability in order to cause unintended behaviour to occur on computer software or hardware.

**OWASP** ▫ Open Web Application Security Project ▫ Not-for-profit charitable organisation ▫ Focused on improving the security of software ▫ All materials are available under a FOSS license ▫ Currently has over 142 active projects 12

<https://www.owasp.org>

# Top 10 Web Application Security Risks

**Injection.** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

**Broken Authentication.** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

**Sensitive Data Exposure.** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, etc. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes..

**XML External Entities (XXE).** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

**Broken Access Control.** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

**Security Misconfiguration.** Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.

**Cross-Site Scripting XSS.** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

**Insecure Deserialization.** leads to remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

**Using Components with Known Vulnerabilities.** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

**Insufficient Logging & Monitoring** coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data.

# SANS Top 20 Security Vulnerabilities [www.sans.org](http://www.sans.org)

## *The Top 20 Most Critical Internet Security Vulnerabilities (Updated) - The Experts Consensus*



### Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Microsoft Office and Outlook Express
- W5. Windows Configuration Weaknesses

### Top Vulnerabilities in Cross-Platform Applications

- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. File Sharing Applications
- C6. DNS Software
- C7. Media Players
- C8. Instant Messaging Applications
- C9. Mozilla and Firefox Browsers
- C10. Other Cross-platform Applications

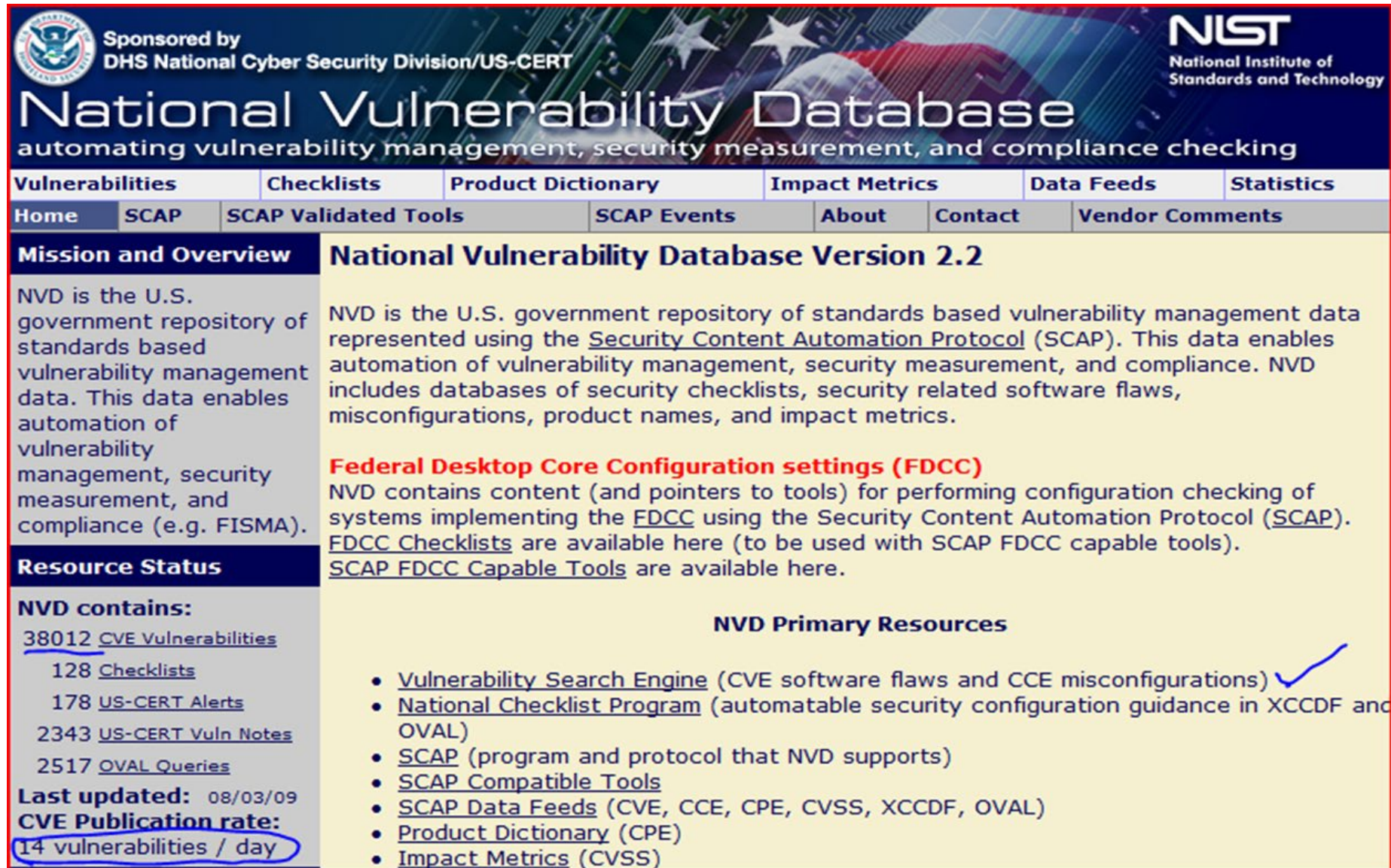
### Top Vulnerabilities in UNIX Systems

- U1. UNIX Configuration Weaknesses
- U2. Mac OS X

### Top Vulnerabilities in Networking Products

- N1. Cisco IOS and non-IOS Products
- N2. Juniper, CheckPoint and Symantec Products
- N3. Cisco Devices Configuration Weaknesses

# National Vulnerability Database <https://nvd.nist.gov/>



Sponsored by  
DHS National Cyber Security Division/US-CERT

NIST  
National Institute of  
Standards and Technology

## National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

### Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

### National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

### Federal Desktop Core Configuration settings (FDCC)

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

### Resource Status

**NVD contains:**

- [38012 CVE Vulnerabilities](#)
- [128 Checklists](#)
- [178 US-CERT Alerts](#)
- [2343 US-CERT Vuln Notes](#)
- [2517 OVAL Queries](#)

**Last updated:** 08/03/09  
**CVE Publication rate:**  
[14 vulnerabilities / day](#)

### NVD Primary Resources

- [Vulnerability Search Engine](#) (CVE software flaws and CCE misconfigurations) ✓
- [National Checklist Program](#) (automatable security configuration guidance in XCCDF and OVAL)
- [SCAP](#) (program and protocol that NVD supports)
- [SCAP Compatible Tools](#)
- [SCAP Data Feeds](#) (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- [Product Dictionary](#) (CPE)
- [Impact Metrics](#) (CVSS)



# Vulnerability Scanner Software <https://www.tenable.com/products/nessus>

The screenshot displays the Nessus Scan Templates interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' tabs, along with a notification bell and a user profile icon. The left sidebar contains navigation options under 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Scanners). The main content area is titled 'Scan Templates' and includes a 'Back to Scans' link and a search bar labeled 'Search Library'. A grid of 20 scan templates is shown, each with an icon, title, and brief description. Some templates have 'UPGRADE' or 'UNOFFICIAL' banners. The templates include:

- Advanced Scan**: Configure a scan without using any recommendations.
- Audit Cloud Infrastructure**: Audit the configuration of third-party cloud services.
- Badlock Detection**: Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
- Bash Shellshock Detection**: Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
- Basic Network Scan**: A full system scan suitable for any host.
- Credentialed Patch Audit**: Authenticate to hosts and enumerate missing updates.
- DROWN Detection**: Remote checks for CVE-2016-0800.
- Host Discovery**: A simple scan to discover live hosts and open ports.
- Intel AMT Security Bypass**: Remote and local checks for CVE-2017-5689.
- Internal PCI Network Scan**: Perform an internal PCI DSS (11.2.1) vulnerability scan.
- Malware Scan**: Scan for malware on Windows and Unix systems.
- MDM Config Audit** (UPGRADE): Audit the configuration of mobile device managers.
- Mobile Device Scan** (UPGRADE): Assess mobile devices via Microsoft Exchange or an MDM.
- Offline Config Audit**: Audit the configuration of network devices.
- PCI Quarterly External Scan** (UNOFFICIAL): Approved for quarterly external scanning as required by PCI.
- Policy Compliance Auditing**: Audit system configurations against a known baseline.
- SCAP and OVAL Auditing**: Audit systems using SCAP and OVAL definitions.
- Shadow Brokers Scan**: Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
- Spectre and Meltdown**: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware**: Remote and local checks for MS17-010.

# AWS Approach



# Other Vulnerabilities

**Code Mistakes**

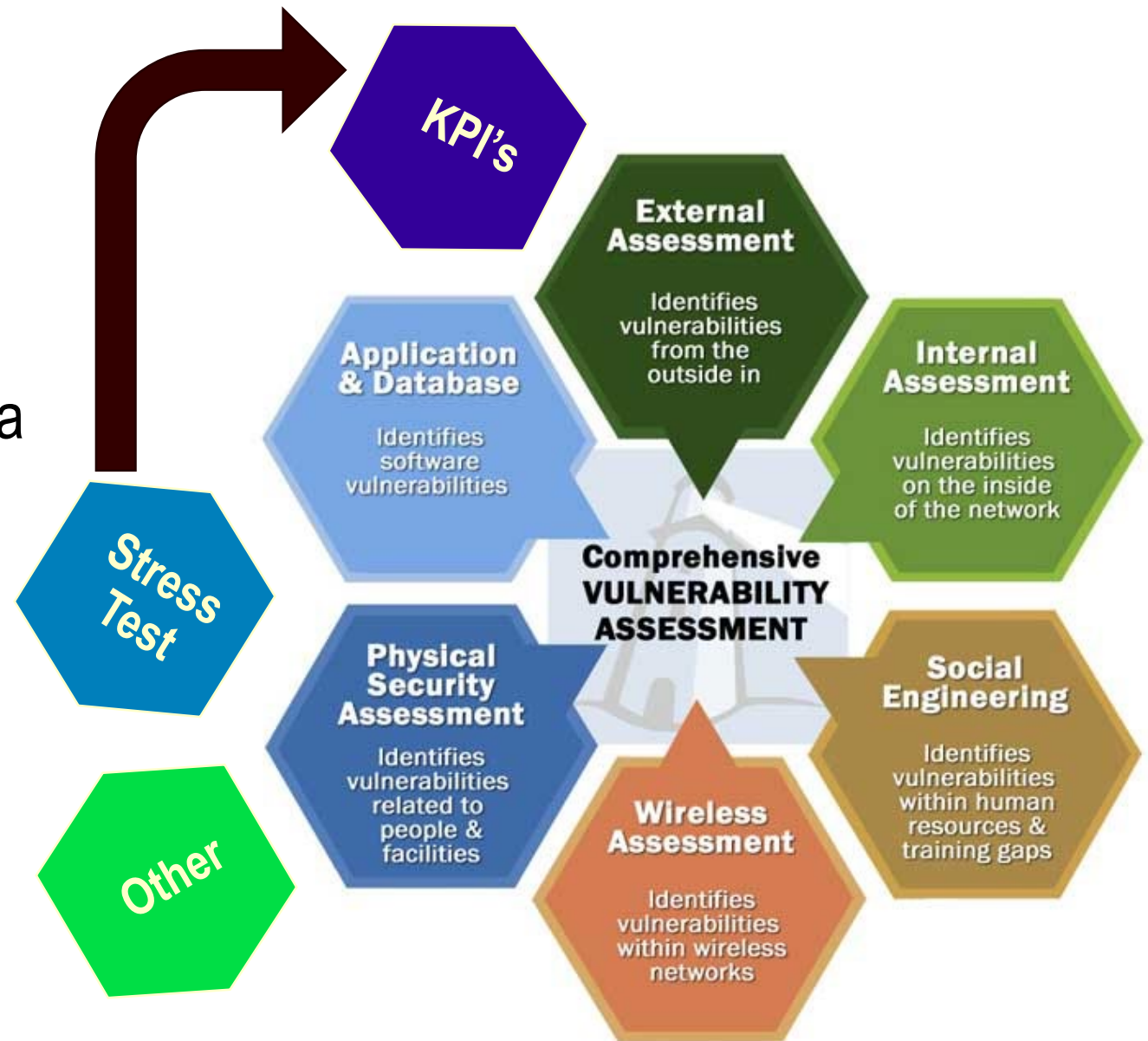
**Untrained Users:**

Security ignorance compromises data

Provide the training

Rules of Behavior

Annual refresher training



## 2) Videos: Discussion & Reflection

- Vulnerability Scanner
- Is your cyber security strategy keeping pace with today's threats?



Go to the virtual room, and complete the activity thread.

### 3) Third Lab

Please go to the Virtual Room for Instructions\\



## 4) Ahead of Cybersecurity



### Crime Theories:

- 1. Classical Theory:** crime is a result of the risk-reward ratio leaning favorably towards “reward.” In other words, if the reward outweighs the risk, crime occurs.
- 2. Strain Theory:** crime is more likely to occur when a person is strained. However, this theory specifically cites an inability to achieve one’s goals or success as the source of crime.
- 3. Social Control / Power Control Theory:** This theory states that it is up to society to prevent crime, to enforce rules, to provide stable environments, etc.
- 4. Routine Activity Theory:** Crime “wants” to happen and that routine helps keep crime at bay, but when routine changes, we are exposed to new circumstances that re-ignite the desire for crime, especially when the new circumstances are not as well protected by law.
- 5. Critical Theory:** Even democracy is too imbalanced; that a very small number of law-makers and power-holders make the laws and, thus, the definition of crime. The people who commit crimes do not necessarily clash with the laws themselves, but with the law makers.

# The Cyber World: Areas of concern: <https://cybermap.kaspersky.com/>

- Cyber Espionage
- Cyber Warfare – Terrorism
- Cyber Crime
- <https://norse-corp.com/map/>

## Defense Goals

- Cyber Knowledge
- Cyber Protection
- Recognition and Mitigation of attacks



# Goals of Cyber – attacks

- Money
- Power
- Control
- Publicity
- Revenge
- Crackers
- Learning
- Future protection/Penetration testing
- Or Just to do it!





# Data and data sources

- Intelligence is lots of data – small pieces add up:
- Male/female
- Initials to real name
- Address
- Residence
- Work history
- Type of system used
- Weaknesses

## **Where do you get data:**

- ✓ Social networks.
- ✓ Stolen items –RFID's, laptops, wallets.
- ✓ Papers (trash).
- ✓ Shoulder surfing – looking over someone's back.
- ✓ Phishing.
- ✓ Personally from employee or target person. internal mole.

# Elements of an Attack

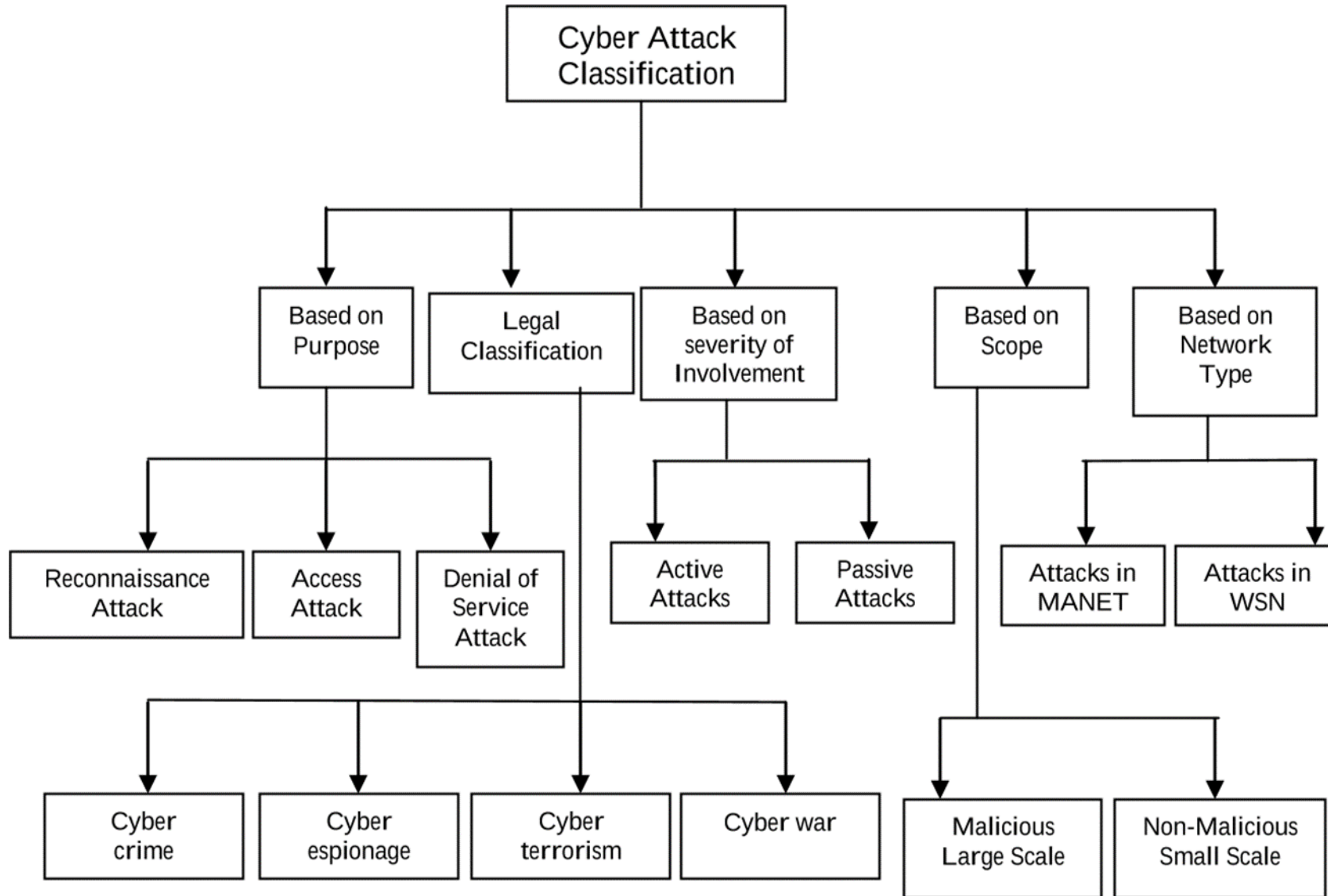
What is needed for a cyber attack?

- Goal – Reason for attack – end desire
- Intelligence
- Lots of data
- Information

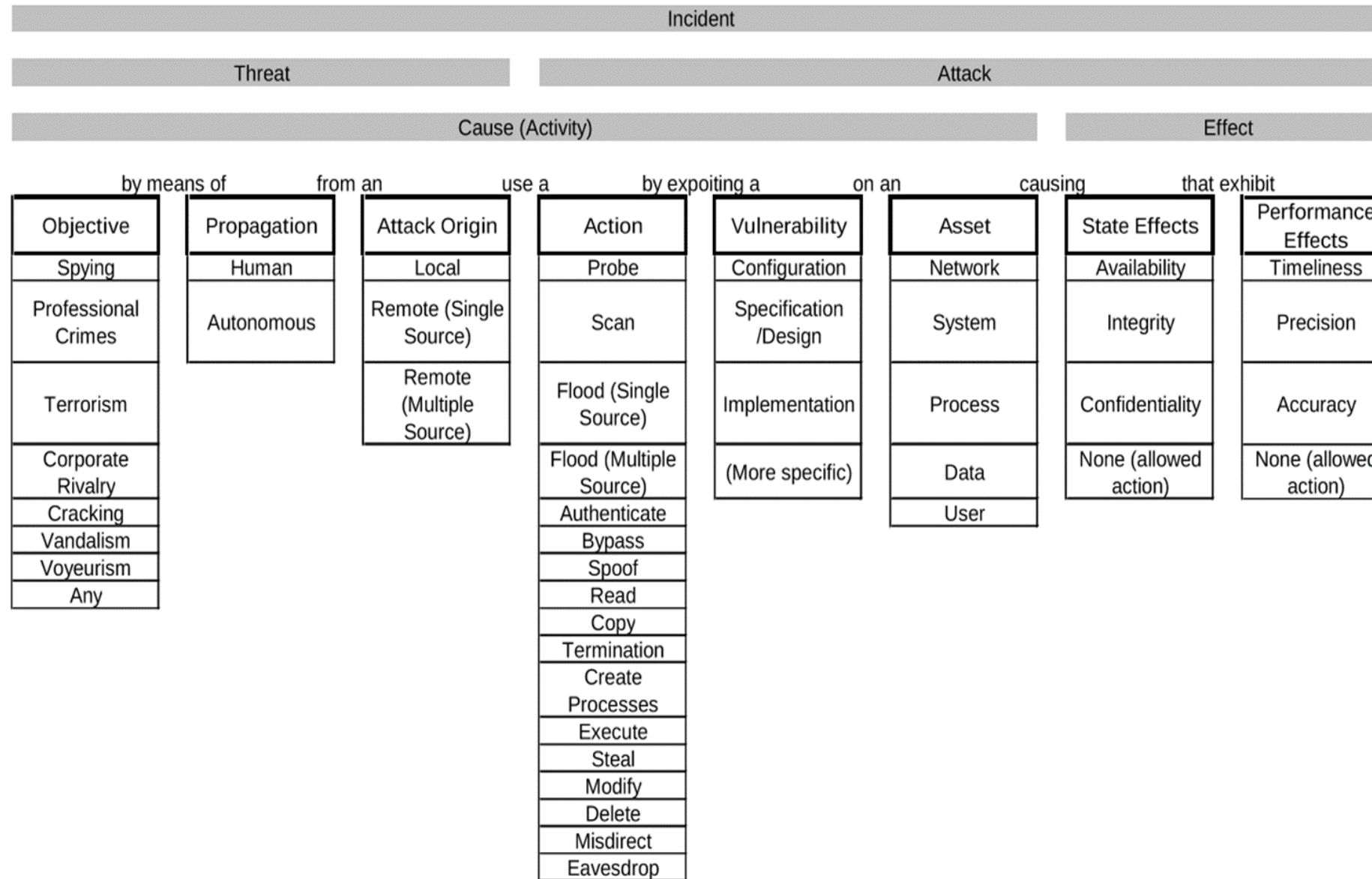
Five common steps in an attack

- 1. Reconnaissance
- 2. Probing
- 3. Actual attack
- 4. Maintaining presence
  - To continue original attack desired effect
  - To allow for future attacks
  - continued surveillance
  - Light footing
- 5. Covering attack track
  - How it was done
  - Access point
  - Residual for future or continued access

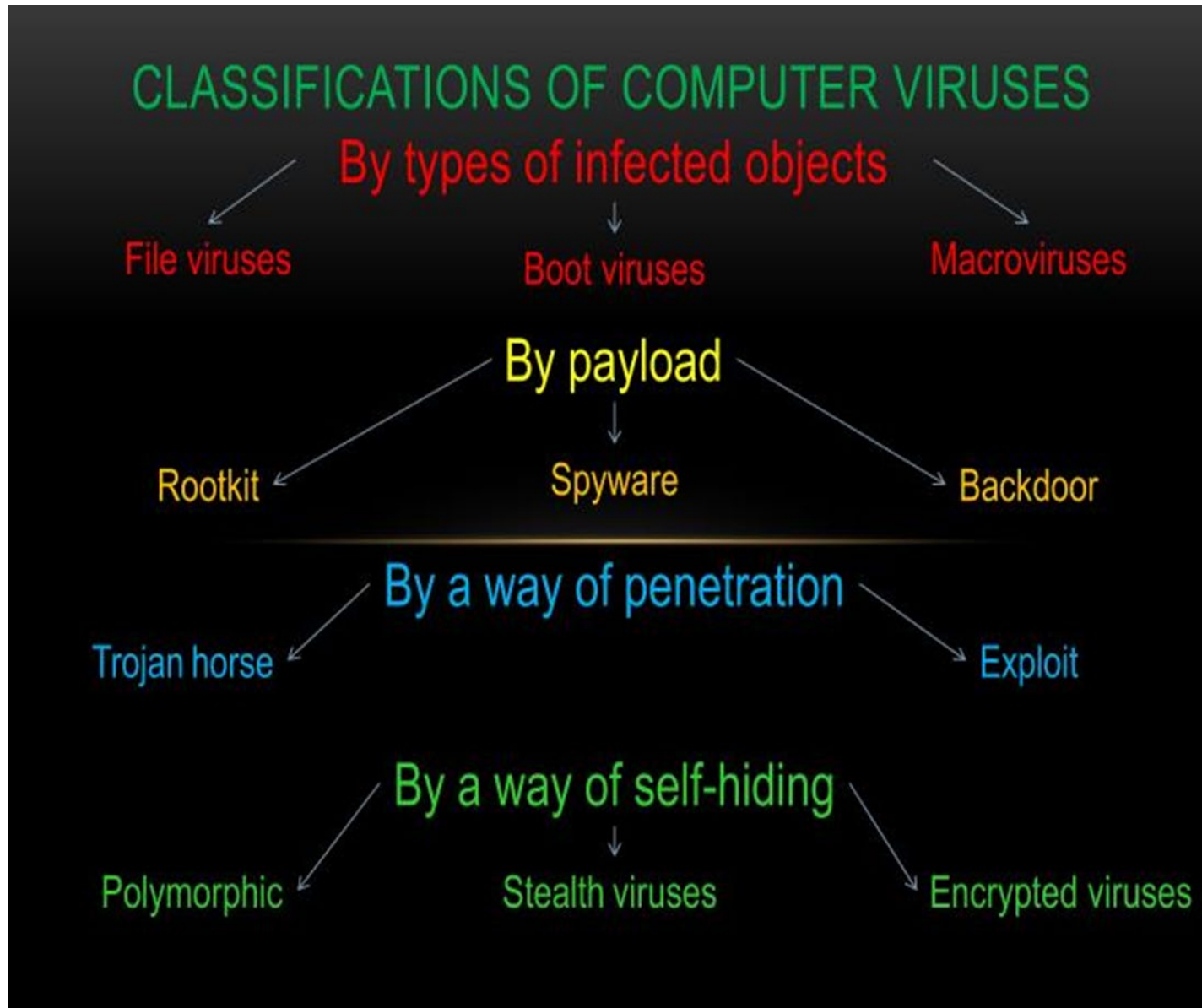
# Cyber-Attack classifications



# SFR Framework of Cyber Attack Classification



# Classification of Computer Viruses



# A special note on DOS

## What is a denial-of-service (DoS) attack?

- In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.
- The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request.

## A special note (cont'd)

### **What is a distributed denial-of-service (DDoS) attack?**

- In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

# How do you know if an attack is happening?

- Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack:
  - unusually slow network performance (opening files or accessing websites)
  - unavailability of a particular website
  - inability to access any website
  - dramatic increase in the amount of spam you receive in your account



# 2019 Attack Threats Overview

- **JSEcoin:** Web-based cryptominer that performs online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources to mine coins, thus impacting the machine's performance.
- **Lotoor** is a hack tool that exploits vulnerabilities on the Android operating system to gain root privileges on compromised mobile devices.
- **Mirai** is an Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. Mirai botnet first appeared in September 2016 and quickly made headlines for largescale attacks, including a massive DDoS attack used to knock the entire country of Liberia offline.

## 2019 Attack Threats (cont'd)

- **Nivdort** is a Trojan family which targets the Windows platform. It gathers passwords and system information or settings such as the Windows version, IP address, software configuration and approximate location.
- **NotPetya** is a ransomware which was spread in a worldwide attack with a high concentration of hits in Ukraine, including the Ukrainian central bank, government offices and private companies.
- **OilRigAPT** Also known as APT34, OilRig is an Iranian APT group active since 2016, and is believed to be a state-sponsored group under the guidance of the Iranian Intelligence Agency and the Iran Revolutionary Guard Corps (IRGC). The group attacks various targets and organizations across the Middle East, and its primary goal is espionage and sensitive data theft.

# TWO Events to Discuss!

- Check this out! <https://docs.broadcom.com/doc/istr-24-2019-en>

## 1) Ransomware in the cloud

- The past 12 months have seen a plague of ransomware attacks, with targets including Britain's National Health Service, San Francisco's light-rail network, and big companies such as FedEx.

## 2) The weaponization of AI

- This year will see the emergence of an AI-driven arms race. Security firms and researchers have been using machine-learning models, neural networks, and other AI technologies for a while to better anticipate attacks, and to spot ones already under way. Hackers are adopting the same technology to strike back.

# Top 5 Most Destructive Computer Viruses

- **1) Stuxnet (2009-2010)** Stuxnet was unique in that it targeted software that controls industrial systems. Specifically, Stuxnet was designed to damage machinery at Iran's uranium enrichment facility in Natanz
- **2) Conficker Virus (2009)** In 2009, a new computer worm crawled its way into millions of Windows-based PCs around the world, creating a massive botnet army of remotely controlled computers capable of stealing financial data and other information.
- **3) agent.btz (2008)** This piece of malware's claim to fame is that it temporarily forced the Pentagon to issue a blanket ban on thumb drives and even contributed to the creation of an entirely new military department, U.S. Cyber Command. Agent.btz spreads through infected thumb drives, installing malware that steals data.

## Top 5 (cont'd)

- **4) Zeus (2007)** There is no shortage of malware kits that target personal information, but Zeus has become the go-to tool for many of today's cyber criminals and is readily available for sale in the cyber crime underworld. It can be used to pilfer passwords as well as files, helping to create a literal underground economy for compromised identities that can be bought and sold for as little as 50 cents.
- **5) PoisonIvy (2005)** it allows the attacker to secretly control the infected user's computer. Malware like PoisonIvy is known as a "remote access trojan," because it provides full control to the perpetrator through a backdoor. Once the virus is installed, the perpetrator can activate the controls of the targeted computer to record or manipulate its content or even use the computer's speaker and webcam to record audio and video.

# Active Computer Viruses as of 2019-20

- ILOVEYOU: Originated in the Philippines – Spread through social media and direct email attachments.
- CODE RED: Originated in China – Spread into the US government systems.
- MELISSA: Originated in the US – as corrupted word document.
- ZEUS: Trojan horse targeting windows programs.
- CONFICKER: Targeted computers using windows.
- STUXNET: Attributed to US & Israel governments, as cyber-warfare.
- MYDOOM: Unknown origin, still active.
- CRYPTOLOCKER: Ransomware targeting windows programs – spread via email.
- FLASHBACK – Unknown origin, still active, no protection develop against it yet.

# Worm Classification

- **1. Stealth worms** do not spread in a very rapid fashion but instead they spread in a stealthy, very hard to detect way by masking their traffic patterns amongst common traffic.
- **2. Polymorph worms** can change themselves during propagation in order to make signature-based detection more complicated. In some cases, two strains of the same polymorph worm will not have a single coinciding element. This is achieved by encoding the main body of the worm and by modifying the program-decoder.
- **3. File worms** are a modified form of viruses, but unlike viruses they do not connect their presence with any executable file. When they multiply, they simply copy their code to some other disk or directory hoping that these new copies will someday be executed by the user.

## Worms (cont'd)

- **4. Multi-vector worms** use different propagation methods in order to make more hosts vulnerable for attack and effectively propagate behind firewalls.
- **5. Email worms** email themselves to other email addresses and make the user execute email attachments with malicious code or use bugs in the email programs to get attachments executed automatically.



# Phases of a Worm

- **1. Information Gathering Phase** The worm selects hosts that will be targeted for infection during this phase. This is the mechanism by which the worm extends its view of the world around itself, determines information about the systems and networks around the machine, and discovers new targets to infect. Before a worm can infect a machine, it needs to identify and locate it. The worm sends stimuli to a possible target, and based upon the responses received, it determines what hosts are active and listening, what ports are open and accessible, and the configuration of the host.
- **2. Infecting Target Machines Phase** The worm enters the host and, if required escalates privileges on other systems. After selecting the target in the first phase, the worm transmits itself into target machines. The privileges include exploitation of vulnerabilities, such as buffer overflows, cgi-bin errors etc. Attack capabilities of worms are limited to one platform or to the method used to find vulnerable hosts.

## Phases (cont'd)

- **3. Payload Phase** Any action programmed other than spreading itself will take place in this phase. Payload is what the worm delivers to an infected host. The worm can create backdoors in the host machine, alter or destroy files, transmit passwords it cracked, or leave copies of itself or other programs into memory to be executed at a later time as a time bomb. Worms use operating system facilities that are often automatic and invisible to the user. Often, worm activity remains invisible until their uncontrolled replication consumes system resources, slowing or halting other tasks. Worm attack can lead to Denial of service by flooding the network with useless packets. Worms can also send sensitive information to cause confusion.
- **4. Network Propagation Phase** Selecting the targets and infecting these targets is accomplished during this phase using random number generators which generate random host addresses to be attacked next. Because the copies of the worm reside on different machines, some form of communication allows for the transfer of network vulnerability and mapping information which can be used in an attack. Worms can also keep track of the systems they attacked if all the copies of the worm know about each other.

# Future Key Design Characteristics of a Worm:



# Building a worm – Reverse engineer the cyber-attack!

- **1: Portability** – worm must be architecture-independent, and work on different operating systems
- **2: Invisibility** – stealth/masquerading techniques to hide itself in live system and stay undetected.
- **3: Independence** – spread autonomically, with no user interaction, using built-in exploit database.
- **4: Learning** – learn new exploits and techniques instantly; by launching one instance of updated worm, all other worms, using special communication channels (wormnet), should download updated version.
- **5: Integrity** – single worms and wormnet structure difficult to trace and modify/intrude/kill.
- **6: Polymorphism** – with no constant portion of (specific) code, to avoid detection.
- **7: Usability** – worm should be able to realize chosen mission objectives – eg. infect chosen system, then download instructions, and, when mission is completed, simply disappear from all systems

# 5) In Closing: Debriefings for Cases

- Debriefing for Cases 01 – 02 – 03 – 04
- Please go to the *Virtual Room* for Instructions
- Prepare your answers accordingly!



**Thank you**

Day 03

**CLOSED**  
**FOR BUSINESS**