CY5210 INFORMATION SYSTEM FORENSICS

Northeastern University

Module 9
Incident Response

Elton Booker | Part-Time Lecturer | e.booker@northeastern.edu

Incident Response

CY5210
Information System Forensics

Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7: Lessons Learned

Incident Handling

- Incident handling is an action plan for dealing with the misuse of computers systems and networks
  - Intrusions
  - Malicious code
  - Cyber-related theft
  - Denial of service
  - Other security-related events
- The goal is to return systems and networks to a normal state
- Policies and procedures should be in place to guide responders

Defining an Incident

- An "incident" is an adverse event in an information system or network…
- …or the threat of the occurrence of such an event
- Focus is on detecting deviations from the normal state of networks and systems
- Examples of incidents include
  - Unauthorized use of another's account
  - Unauthorized use of system privileges
  - Execution of malicious code

- An incident implies harm or the threat of harm

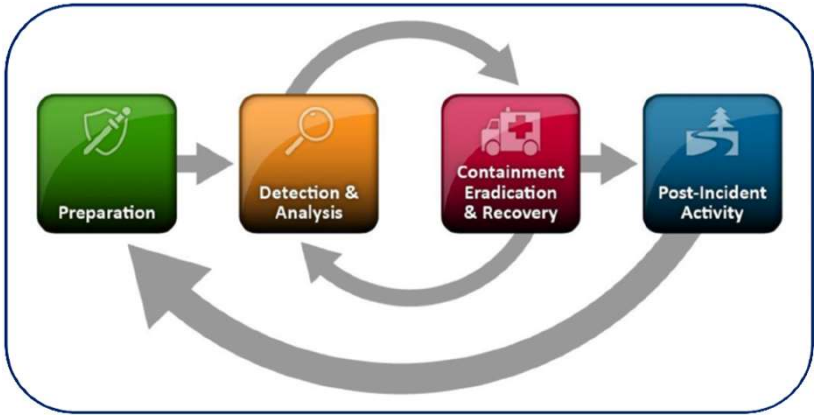
Defining an Event

- An “event” is any observable occurrence in a system and/or network
- Examples of events include
  - A system randomly booting
  - A system crash
  - Packet flooding on the network
  - Failed login

- These type of events will be the bulk of incident response activities
- These events provide the bulk of a potential policy violation
  - Must be recorded in notes and logs
  - A chain of custody must be completed
  - Reporting the same event in multiple ways improves evidence (corroborating evidence)

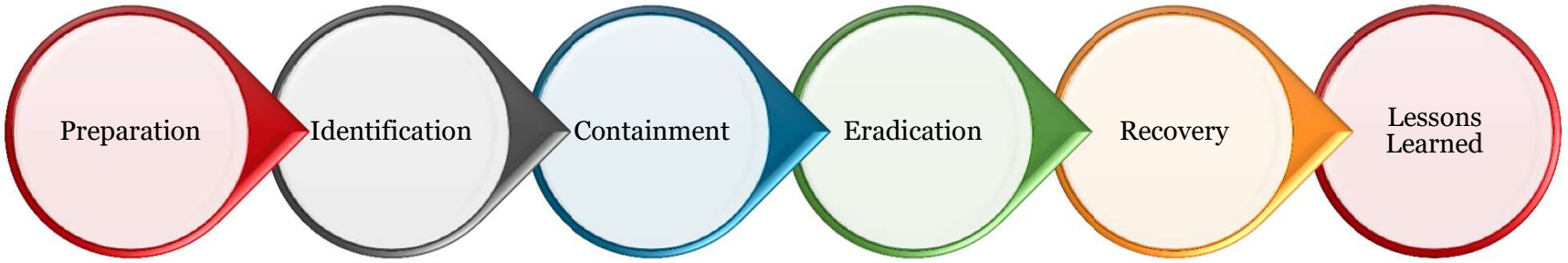
Incident Response Summary

- Incident handling is similar to first aid
- Mistakes can be costly and stress is high
- A simple, well understood, documented process is best
- Keep the six stages if incident handling in mind:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned



- Additional supporting material:
  - NIST's Computer Security Incident Handling Guide, Revision 2
    - *https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final or on Blackboard*

SANS Incident Handling Process



Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7: Lessons Learned

Preparation Overview

The primary goal of this step is to ensure the environment, processes, and capabilities

- People
- Policy
- Procedures
- Data
- Software/Hardware
- Communications
- Supplies
- Secure Baselines
- Transportation
- Space
- Power and Environmental Controls
- Documentation
- Training
- Network Configurations
- Security Tool Configurations

People

- One of the most overlooked infection vectors
- The most easily targeted
  - Targeted e-mail (Spear phishing)
  - Phone calls (social engineering)
  - Text messages (smishing)
- Frequent, ongoing training required
  - Annual training often ineffective
  - Constant reinforcement
  - Phishing education platforms

- Regularly train employees with social-engineering tests

Phishing Frameworks

FEATURE	PHISHME	KNOWBE4	WOMBAT
AWS Instance	X	X	X
Voice phishing (Vishing)		X	
SMS / Text phishing (Smishing)		X	X
Fax phishing			
External device (USB) dead drops		X	X
Comprehensive User Training	X	X	X
Infographic / HTML	X	X	X
Videos	X	X	X
Redirect	X	X	X
Game / Quiz	X	X	X
Active Directory Integration	X	X	X
Reporting and Analytics	X	X	X
Vulnerable Plugin Check		X	X
Phishing Button	X	X	X
Benchmarking Comparison Against Sector	X		X
Weak Data Egress Control Test			X
Email Exposure Check		X	

Policy – Warning Banners

- Establish policy including warning banners
  - Limit the presumption of privacy

- Banners must advise the user community:
  - Access to the system is limited to company authorized activity
  - Any unauthorized access, use or modification is prohibited
  - Unauthorized users may face civil/criminal penalties
  - The use of the system may be monitored and recorded
  - If criminal activity is identified, evidence may be submitted to LE

Crucial

- Have your legal department approve the language
- Pay attention to local privacy laws (e.g. EU)

Policy – Response Strategies

- Establish an incident response plan
  - Include ancillary procedures (COOP, DRP, BCP, other DFIR policies)

- Decide how to handle important issues ahead of time
  - Remain covert or notify law enforcement
  - Contain or watch and learn
  - When will systems be contained
  - Roles and responsibilities
  - Definitions of events and incidents

- Obtain executive buy-in and written approval
- Perform tabletop exercises to prepare teams

Notifying Law Enforcement

- Reasons you **must**
  - Threat to public health
  - Threat to public safety
  - Legal industry requirement
- You **may** need to notify if PII/PHI breached
  - Most states have breach disclosure laws
  - If you business in a specific state with these laws, you may need to report
  - Most states and the U.S. Federal Government are working on similar laws
- **Optional** reasons
  - Benefit from discovery
  - Assist other companies

Not Notifying Law Enforcement

- Common reasons not to report
  - Loss of control
    - Investigation and recovery goals are different
  - Negative publicity
  - Risk of continued attacks or loss of data
  - Risk of equipment seizure as a result of the investigation
  - Become an agent acting on behalf of LE
    - Legal protections apply

Developing LE Contacts

- Make use of SANS “Interfacing with LE” FAQ
- Develop relationships with LE
- Know the cases that warrant LE investigation
- Join various associations
  - High Technology Crime Investigation Association (HTCIA)
  - FBI Infragard
  - Electronic Crime Task Force (ECTF)
  - Local threat sharing groups (e.g. ND-ISAC)
- Report to local, state, and federal departments

Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7: Lessons Learned

Identification Overview

- Prevention ideal, but detection is a must
- Do your best to alert early
  - Don't be afraid to declare an incident
  - The organization wins even if an attack hasn't happene
- Maintain situational awareness
- Provide indications and warning
- Provide up-to-date "intelligence" to handlers
- Fuse or correlate information

Assigning Responders

- Assign a primary incident responder
  - One person to handle identification and assessment
  - Assign specific events and systems
- Empower the primary analyst
  - Decision making
  - Identifying resources
- Assign a secondary responder
  - If resources available
  - Second analyst can take notes

Control Information Flow

- Abide by the “need to know” policy
- Share details with the minimum amount of people
- Receive written permission to extend the scope
  - Human resources
  - Legal department
  - External attorneys

- Constantly remind parties of the need for discretion
- Remind them that they may need to testify

Communication Best Practices

- Avoid using potentially compromised systems (e-mail or chat)
- Rely on out-of-band communications
  - Telephones and faxes
  - Be careful with VOIP (Wireshark, CAIN, and VOMIT)

- Make sure the team(s) can share encrypted emails
- Exchange keys early
  - GnuPGP
  - PGP
  - S/MIME

- Use encrypted cloud storage

Where Might Identification Occur?

- Anywhere in your environment, but there are some specific locations
- Network perimeter detection
  - Firewalls, routers, external-facing network-based IDS, IPS, DMZ systems, etc
- Host perimeter detection
  - Data enters/leaves host
  - Personal firewall/IPS, local firewall, port sentry tools
- System-level (host) detection
  - Antivirus tools, endpoint security suites,
  - file integrity tools, user-reported behavior
- Application-level detection
  - Application logs (web app, app server, cloud services, etc)

Limitations

- No one tool or alert can detect every attack
  - The most dangerous attackers are more stealthy
  - The generic attackers are easier to detect
  - The attacker's may make mistakes

- Typically security analysts must understand "normal" behavior
  - Spot abnormal events
  - Procedures and processes show how to identify outliers

Initial Assessment

- Determine whether an event is an actual incident
  - Check for mistakes made by users, admins, etc
  - Assess the evidence in detail
  - Identify the scope!!!
  - Determine other possibilities
  - Incident response accounts for common methods
  - Report to executive leadership

Handling mistakes and errors effectively is part of the process

Assessment Questions

- Determine the extent of the damage
  - What is the scope of the incident?
  - How can the incident be contained?
  - How widely deployed is the OS, application, vulnerability?
  - What is the impact of exploitation, if one exists?
  - What is the value of systems impacted and risk?
  - What is the value or criticality of data on the systems?
  - Can the vulnerability be exploited remotely – increased risk
  - Is there a public exploit available?
  - Is the exploit being used in the wild?

Additional Questions

- Also determine:
  - What level of skill or training is required to exploit the vulnerability?
  - What is the risk, threat, and impact?
  - Is the vulnerability wide-spread in a default configuration?
  - Is there a fix available for the vulnerability?
  - Are there existing mitigations that reduce the risk?

- Initial Security Incident Questionnaire for Responders
  - https://zeltser.com/security-incident-survey-cheat-sheet/

Chain of Custody

- Maintain a valid chain of custody!!
  - DO NOT delete any files until the case is closed
  - There should be a document retention policy
  - Identify every piece of evidence
  - Hash all files and evidence
  - Control access to evidence
- All evidence must be under the control of one person at any time
  - Record date/time
  - Person turning over and receiving evidence
- Have LE sign for evidence when they confiscate items

Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7: Lessons Learned

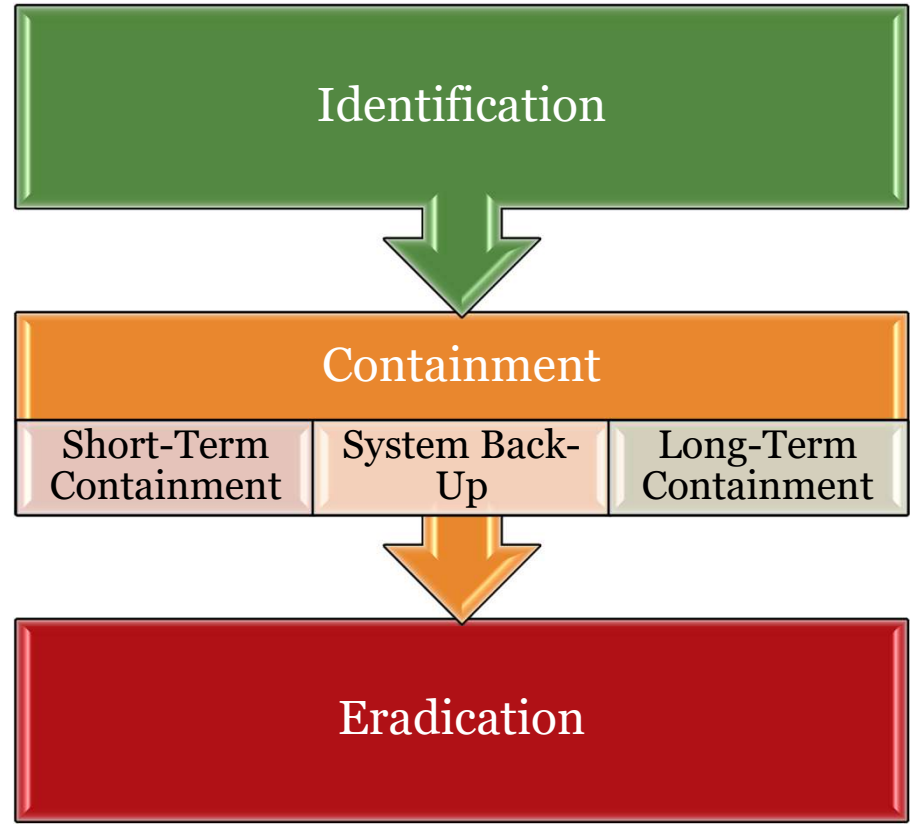
Containment Overview

- The goal is to stop the bleeding
  - Prevent the attacker from getting any deeper into the network

- We'll discuss
  - The sub-phases of Containment
  - Methods for short-term Containment
  - System back-up
  - Methods for long-term Containment

Containment Sub-Phases

Containment actually has several components



Deployment

- Deploy a small team to scope the incident
  - Typically same as identification team
  - Secure the area
  - Use pre-designed and printed forms
  - Review and verify the information from the Identification phase

Characterize Incident

After declaring an incident, record the category (might be more than one), criticality, and sensitivity…

- **Category**
  - Denial of Service
  - Compromised Info
  - Compromised Asset
  - Unlawful Activity
  - Internal Hacking
  - External Hacking
  - Malware
  - E-mail
  - Policy Violations

- **Criticality**
  1. Incident impacts critical systems: 60 min
  2. Incident impacts non-critical systems: 4 hrs
  3. Possible incident, non-critical: 24 hrs

- **Sensitivity**
  1. Extremely sensitive (CSIRT, mgmt)
  2. Sensitive (CSIRT, mgmt, sys owners, Ops)
  3. Less sensitive (isolated virus infection)

Notifying Management and Track Incident

- Notify your organizational incident response team
- Notify your manager and security officer
- Vertical and horizontal reporting may be necessary
  - Inform management
  - Inform affected business unit

- Create entry in incident tracking solution
  - The free RTIR Incident Response tracking tool
  - BMC Footprints for tracking
  - ServiceNow Incident Response module

Short-Term

- Prevent the attacker from causing more damage
- Create images to avoid contaminating evidence
- Short-term containment actions:
  - Disconnect network cable
  - Pull the power cable (caveats)
  - Use network management tools and place system(s) on infected VLAN
  - Apply filters to routers and/or firewalls
  - Change host name in DNS to point to a different IP address
- If the system must be disabled, notify the business unit
  - Information or application owner
  - Advise them in writing or email
  - They may disagree

ISP Coordination

- For external attacks, coordinate closely with you ISP
  - It may be able to assist in identification, containment, and recovery
    - Large packet floods, botnets, worms, and spam
  - It may be able to throttle the attack (DoS/DDoS)

- You may need to work with another ISP to get a bot-infected system taken offline

Creating Forensic Images

- Make images of affected system(s) ASAP
- Grab an image of memory and the file system
  - Mandiant Redline and the Volatility Framework
- Use sterilized media and make a bit-by-bit image
- Not all incidents allow for a full backup or analysis
- Create a hash of the original and all images
  - Chain of custody
  - Use write-blocking hardware
  - Destination larger than source
  - Drive duplicator hardware

Long-Term

- After imaging, changes can be made to the system
- Longer-term containment strategies can be implemented

- **Ideal**: If the system can be kept offline, move to the eradication phase
  - Get rid of the attacker from the environment

- **Less-than-ideal**: If the system must be kept in production, perform long-term containment actions
  - This may be a business decision
  - Document your recommendation in writing and have the business unit agree

Long-Term Actions

- Numerous possible actions:
  - Patch affected and nearby systems
  - Insert Intrusion Prevention System (IPS) or in-line Snort
  - Null routing
  - Change passwords
  - Alter trust relationships
  - Apply firewall and router rules
  - Remove accounts used by attacker
  - Shutdown backdoor processes used by attacker

- Eradication must be performed
- The goal here is to provide a temporary solution and stay in production while re-building the system during **Eradication**

Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7: Lessons Learned

Eradication Overview

- Goal is to get rid of the attacker's artifacts and prevent re-infection
- Determine cause and symptoms of the incident
  - Use info gathered during identification and containment
  - Try to isolate the attack and determine how it was executed

- Remove traces of attackers
- Ensure they cannot return and continue to affect systems
- May need to restore from backups
- System will need to be rebuilt
- Business unit could face downtime

Removing Malicious Software

- Remove malware inserted by the attack
  - Virus infestations
  - Backdoor
  - RootKits or Kernel-level RootKits

- If a RootKit exists, rebuild from scratch
  - Format the drive
  - Operating system (and all patches)
  - Applications (and patches)
  - Data (after the dataset has been scanned*)

- Encourage business unit to rebuild and a review by the CSIRT
- The attacker may not have used malware (SSH or RDP)

Improving Defenses

- Implement appropriate protection techniques
  - Applying firewall and/or router filters
  - Moving the system to a new name/IP address
  - Null routing particular IP addresses
  - Changing DNS names
  - Appling patches and hardening the system

Vulnerability Analysis

- Perform vulnerability analysis
  - System vulnerability analysis
  - Network vulnerability analysis
  - Search for related vulnerabilities
  - Scan network with a port scanner
  - Use a vulnerability scanner
    - Tenable's Nessus, OpenVAS, Qualys, etc
- Attackers often use the same exploit and backdoors on multiple machines
  - Look for these iOCs throughout your environment

Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7 Lessons Learned

Validation

- Goal is to put impacted systems back into production
- Validate the system
  - After restoration, verify the operation was successful and the system normal
  - Ask for test plans and baseline documentation
  - Run through the tests, or have the business unit test

Restore Operations

- Decide when to restore operations
  - Try an off-hours timeslot
    - It's easier to monitor carefully
    - You may be overruled, since the business unit wants to restore service
  - Put the final decision on the system owner(s)
  - Provide advice, but the owner makes the call
    - Document advice in signed memo

Monitor

- Monitor the systems
  - Once the system is back online, continue to monitor for backdoors that were undetected
  - Utilize network and host-based intrusion detection systems and Intrusion Prevention Systems
    - If possible, create a custom signature to trigger on the original attack vector because the attacker may try the same thing
  - Carefully check operating system and application logs

Return of Artifacts

- Incident handlers should check regularly for re-compromise
- Attackers may use normal mechanisms instead of malware
  - Look for changes to configuration via registry keys and values

- Write a script to check for similar artifacts returning (daily)
  - Windows reg command
    - Look for unusual processes
  - Windows wmic or tasklist commands, or Linux ps command
    - Look for accounts used by the attacker
  - Windows wmic useraccount or net user commands, or Linux cat /etc/password
    - Look for simulataneous logins

- Utilize the cheat sheet techniques looking for specific indicators

Incident Response

- Module 1.1: Introduction to Incident Response
- Module 1.2: Preparation
- Module 1.3: Identification
- Module 1.4: Containment
- Module 1.5: Eradication
- Module 1.6: Recovery
- Module 1.7: Lessons Learned

Report Writing

- Goal of Lessons Learned is to document what happened and improve
- Develop a follow-up report
  - Start this process right after Recovery (two weeks is too late)
  - Assign task to on-site team with a team lead
  - Encourage all participants to review the draft
  - Attempt to reach consensus and get sgn off
  - If someone doesn't agree have them submit their version

- Determine the report formats required
  - Forensic reports, malware reports, intermittent updates
  - Ensure the report is signed and submitted in a timely manner

Final Meeting

- Meet within two weeks of completing the incident
- Review the report
- Subject the report to peer review
- Finalize the Executive Summary
- Keep the meeting short and simple
- Take notes and track meeting minutes
  - Recommendations for improvement
  - Configuration changes
  - Improved process flows
  - Policies and procedures
- Request approval and funding
  - People, processes, and technology
  - Improve incident handling capabilities

Northeastern University

Instructor Demo: Introduction to Wireshark

Become familiar with the basic review functions of Wireshark