SANS 504

▼ What is incident handling ?

- **it's an action plan for dealing with the misuse of computer systems and networks like:**
  - Intrusion
  - Malicious code infection
  - Cyber theft
  - Denial of service
  - Other Security-related events
- **The incident handling plan must comply with your government policy**
- **Examples of incidents include:**
  - Unauthorized use of another user's account
  - Unauthorized use of system privileges
  - Execution of malicious code that destroys data
- **Examples for an event:**
  - The system boot sequence
  - Packet flooding within a network
  - A system crash
- **The observable events provide the bulk of your organization's and we should:**
  - Record it in notebooks and logs
  - Recording the same events in multiple phases helps improve evidence that's corroborating evidence.

> ***Incident handling is similar to first aid***

- **The Golden Six Stages**
  - Preparation
  - identification
  - containment
  - Eradication
  - Recovery
  - Lessons Learned
- **After an incident occured you don't need to act, but take to think so you don't ruin the evidence.**
- **ISC displays statistics from DSHEILD sensor network which has over 40.000 sensor around the planet gathering information about scans and attacks against various ports**

▼ First Phase: Preparation

- **The Goal of Preparation**
  - To get the team ready to handle incidents (people, software, policy, data, supplies communications, documentation).
  - People is One of the most overlooked aspects of our security posture, also it is the most easily attacked via phishing or social engineering
  - Policy is like warning banners to the users.
  - Warning banners are very important to incident handlers. They make the major difference in the amount of trouble you have to go through to collect and use evidence.
  - One of the warning banner that is really important "The use of the system may be monitored and recorded".
  - In the policy you must declare the Response strategies like :
    - Establish an organizational approach to incident handling
    - Decide generally how you will handle the "big issues" up front.

    - You must include the low inforcement to your company to make the hackers pay
    - One of the curcial notes in preparation phase is Remain calm and taking notes.
- I**f you are willing to create a team make sure it contains the following disciplines:**
    - Security: includes incident handler, forensics, malware ...
    - Operation (System Administrator)
    - Network Management
    - Legal Counsel
    - Human Resources
    - Public Affairs/ public relations
    - Disaster recovery
    - Union representation
- **Some Important Key Points for the Preparation Phase:**
    - Develop an emergency communication plan.
    - Getting access to systems & data, this phase it's like don't use root or admin privilege if you don't need it, and passwords, keys must be stored correctly with the right people.
    - Establish a primary point of contract and an incident command communication center
    - Reporting Facilities, as (system admins, help desk workers are the eyes and ears of any organization, you should put a bounty or reward if they get any malicious behavoir or something like that or even writing a small article with photo of him, these type of things pays off time and time again for the organization, also you need to make it easy to report:
        - well known voice or fax number
        - Email, Web address for an internal website devoted to incident handling

> *Also in this topic you should provide what it's called "War Room" which you can say, display anything without worrying about spying or recording or any other stuff like temprature to make the boys comfortable (incident handlers)*

    - Train the team, Here is some resources that your team can practice to know the things that they will go through, and it's fun counter hack challenges, holiday hack challenges

- Cultivate (it's like make it strong) Relationships, knowing your help desks and the relation between system administrators and network administrators
- Investing in your help desk, making sure they are trained to be part of the response process, is sound practice.
- System and Network Admin's are the wild cards in incident handling, you can't handle a large incident without system and network administrators, but they are likely to make those critical mistakes that happens in the first five minutes of an incident

> *There is a great tool that shared for performing large scale incident response and hunt teaming is called GRR, currently this project is maintained by google and it's free, This tool has the ability to store a wide selection of data that is relevant from a large number of hosts, even if this host is not on the network it has the ability to wait for it to connect to the network then pull this data from it*

> 💡 One way to use GRR is to create a flow, which is a script that runs on the GRR server, but makes calls to the clients to perform various tasks. For example, you could create a flow to look for a file with a specific hash (or other properties). You could run this flow across several clients, even an entire enterprise, using a Hunt.

- Get a duffle bag and keep it stocked with items for incident handling, duffle bag it's like the first aid kit that you need when something is happenening like:
    - Fresh media for holding file system images
    - Evidence collection software (e.g. FTK Imager Lite) etc..

The Second phase is Identification

• How do you detect an incident? The bulk of all detects will come from either sensor platforms or the things that just happens for the people to notice

• **Points to keep in mind**

. Be willing to alert early!

. Don't be afraid to declare an incident

. Maintain situational awareness

. Fuse or corrulete information

• **Assigning handlers**

. *Ideally it's best to assign a primary handler a set of events to analyze and Empower him to escalate if needed, also you need to assign a helper to the handler to speed up the process of collecting evidence*

• **Control The flow of information**

• **Communications channels**

. Maybe the computers gotton compromised during the attack, so you want to avoid using them for incident handling discussion (email or chat), So you need to relay on out-of-band communications like telephones and faxes, also make share the team can send encrypted email using GnuPG, PGP ...

• **Where does Identification Occur?**

So you can identify it in multipel layers like:

. Network Perimeter detection, using IDS, IPS, routers....

. Host Perimeter detection, using personal firewalls/ IPS..

. System-level (HOST) detection, gets detected using endpoints security, antivirus tools etc.

. Application perimeter detection, Application logs

. talked about tcpdump (used for capture packets) and netstat (current process)

. Port 4444 is the default port for many metasploit payloads.

• The official port list is mainted by IANA you can search it

• In the application level of detection, you get the data from the logs either web app, cloud based services, and the data that you should be looking for is :

. Dates

. Time Stamps

. Actions and transactions, including User Input variable value

. Users (specially admins)

• **Identification Across all levels**

. Unfortunatly, some attacks are stealthy and detected only on the filtration process, That's why we need the identification capabilities across all four levels: **Network, Host perimeter, host level and Application level**

• There is a intrusion discovery Cheat sheet, that a SANS has released out for free, There is a page for Linux and page for windows, The purpose of this cheat sheet is to help administrators to detect intrusion or at least know the normal behavior and the malicious one.

• This cheat sheet will have the administrators look for unusual:

. Processes and services

. Files

. Network usage

. Scheduled tasks

. Accounts

. Log entries

. Other unusual items

. Third Party tools

Windows Cheat Sheet Lab

1. Some commands Here

```
>netstat -naob          //show owning process id and associated executables
>netsh advfirewall show currentprofile  //Examine built-in firewall settings
>tasklist /v       //examine processes at the command line with details
```

2. after you examined the processes with command line you can open task manager and look for unusual processes

While the ‘tasklist’ command is good, the ‘wmic’ command provides access to very detailed information about running processes

```
>wmic process list brief    // brief information
>wmic process list full     // full information
>wmic process get name, parentprocessid, processid  //get specific field
>wmic process where processid=pid get commandline   //Focus on a specific process
```

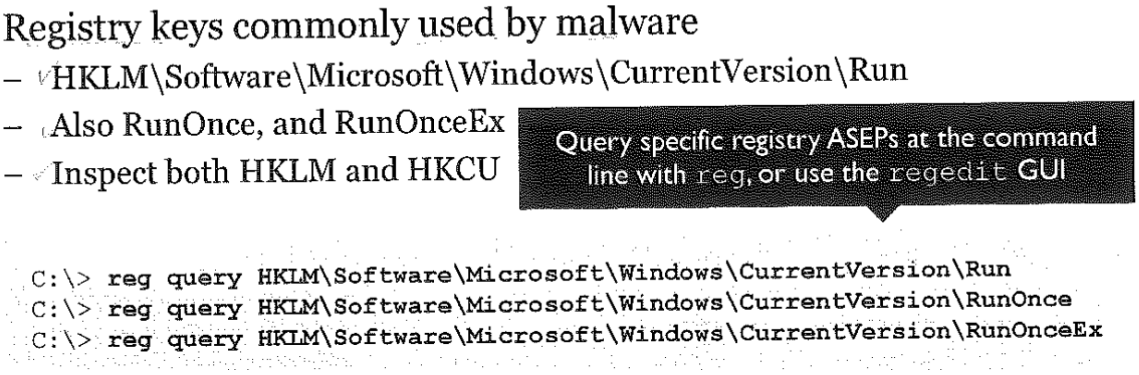
Pay close attention to any running processes that have base64-encoded command line options

3. **Examining services**

```
>services.msc  //examine services using the service control panel
>net start     //Examine running services
>sc query | more  //get more detail about each service
>tasklist /svc    //Map running processes to services
```

4. There is something called Registry ASEPs (AutoStart Extensibility Points), it contains numerous registry and file locations that start software automatically

Registry Keys commonly used by malware



```
>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
```

Additional Ways to Examine ASEPs

```
>dir /s /b "C:\Users\username\Start Menu"  //Check user autostart folder
  //YOU may use a tool to summarize ASEP Information
>start msconfig.exe
>wmic startup list full
```

5. Unusual Accounts, unexpected accounts in the administrators group

The commands That you can use it here

```
>lusrmgr.msc                    // GUI for viewing users and groups
>net user                       // List Users
>net localgroup administrators   // Shows who is in the administrator group
```

6. Check file space for sudden major decreases in space

```
>dir C:\
  // Search for file larger than 10 MB at the command line
>FOR /R C:\ %i in (*) do @if %~zi gtr 10000000 echo %i %~zi
```

7. **Look for unusual scheduled tasks**

Especially those that run as SYSTEM, as a user in the administrator group, or have a blank user name

```
>schtasks
>at //This command used to create tasks and display them
```

`'at'` command is limited, it only displays those tasks created using the at command itself, and not the scheduled tasks created using 'schtasks', So it's preferable using 'schtasks', There is a GUI for this Just search **Task Scheduler**

8. **Unusual log Entries**, Review the event log for suspicious events

a. Event log service was stopped

b. Windows file protection is not activated

c. The MS Telnet Service has started successfully

d. Look for a large login failed attempt or locked-out accounts

```
>wevtutil qe security /f:text  // view all the logs
```

9. **Other unusual items**, The Cheat sheet tell administrators to check performance monitor, and look for unusual crashes

Additional Supporting Tools

The Sys internals tools are great (and Free!)

- The Sysinternals tools are *excellent* (and free!)
  - Process Explorer gives in-depth information about running processes
  - Process Monitor shows file system, registry, network, and process activity in real-time
  - TCPView shows listening ports (TCP and UDP) and maps them back to the owning process
- Center for Internet Security has templates and scoring tools

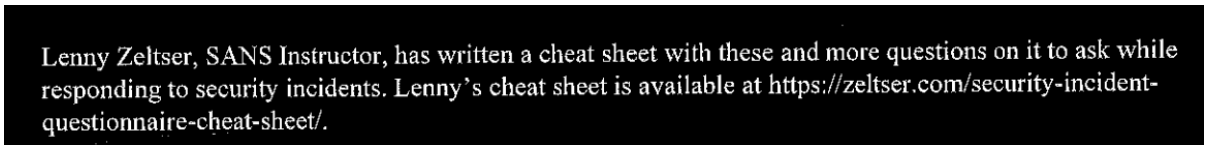
Assessment Questions

- How much damage could be caused ?
- How widely deployed is the affected platform or application ?
- What is the effect of vulnerability exploitation if a vulnerability is present ?
- What is the value of the systems impacted so far ? What is the value of the data on those systems?
- can the vulnerability be exploited remotely ?
- Is a public exploit available ?

- What level of skill are required by an attacker to exploit the vulnerability ?

- Is the vulnerability present in a default configuration ?
- Is a fix available for the vulnerability ?
- Do other factors exist that reduce or increase the vulnerability's risk or potential impact ?

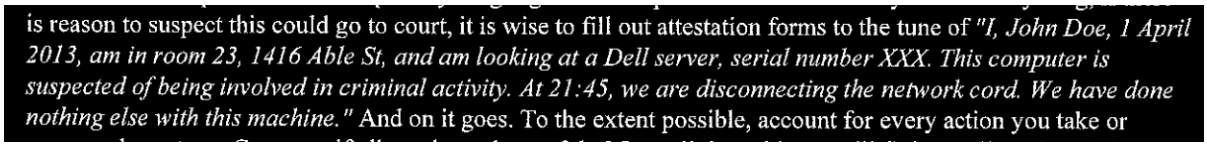
> *One of the most effective tools to assist in incident response released in the last few in the MITRE ATT&CK matrix, This is a collection of techniques used by actual malicious attack groups over the past few years, it breaks the technique up into phases attackers go through, you can found it here: "https://attack.mitre.org/wiki/Technique_Matrix"*



💡 One of the Main points also in identification is Establishing a **Chain Of Custody**

- Do not delete any files until the case is closed out, and if you have the storage do not delete them.
- Identify every piece of evidence in your notebook.
- Control access to evidence
- Every piece of evidence must be under the control of one identified person all the times
- When turning over evicdence to law enforcement, have them sign for it

Example of how you should store you evidence


is reason to suspect this could go to court, it is wise to fill out attestation forms to the tune of *"I, John Doe, 1 April 2013, am in room 23, 1416 Able St, and am looking at a Dell server, serial number XXX. This computer is suspected of being involved in criminal activity. At 21:45, we are disconnecting the network cord. We have done nothing else with this machine."* And on it goes. To the extent possible, account for every action you take or

Containment

> *The goal of containment is to keep the problem from getting worse. Before we fire, we should take the time to aim! Try to do a decent survey and review of the situation before alerting the system*

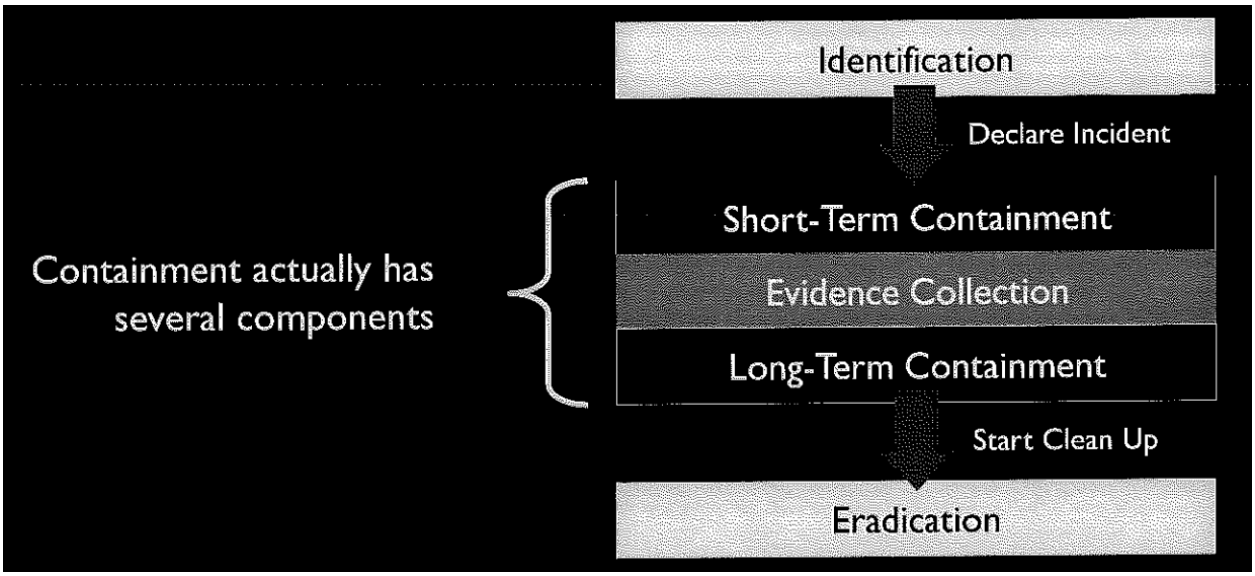
The containment phase is to stop the bleeding, prevent the attacker from getting any deeper or spreading to other systems

We discuss:

1. The sub-phases of containment
2. Methods for short-term containment
3. Evidence Collection
4. Methods for long term containment

First: Sub Phases Continued to long-term containment

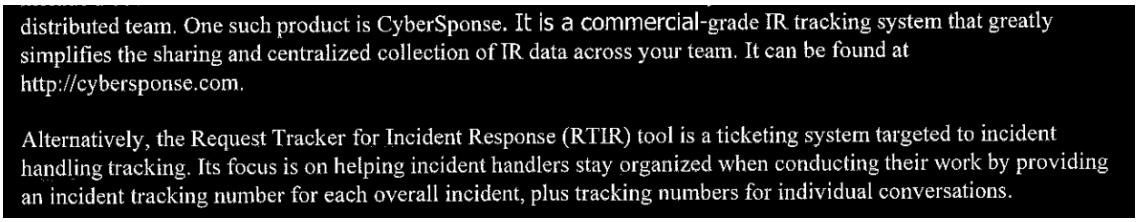
Containment includes the three sub phases: **short-term containment** to contain the damage at first followed by **collecting evidence** then **Long-term containment** to make sure the bad guy is denied access



- **Deployment**
  - Deploy a small in site team to survey the situation, to review the information that was provided to you from the identification phase etc…
- **Characterize incident**
  - Once an incidence has been declared, document various characteristics:
    - **First Case Classification**
      - incident category
      - Criticality (affects response time)
      - Sensitivity (affects who should be notified)
- **Inform Management**
  - you should identify a senior management sponsor for your team, CISO, CIO, Legal counsel etc.
  - When you declare an incident, notify your management sponsor either from E-mail or phone call and if it's critical pay him a visit.
  - assign an incident at least two people, handler and helper, and make sure they taking the right notes and observations for the incident
- **Notification and incident tracking**
  - Notify you local organization or your management sponsor

- Remember vertical and horizontal reporting
  - Inform management
  - Inform impacted business unit
- Create entry in incident **tracking system**
  - **CyberSponse** is a commercial IR tracking system
  - There's the free **RTIR** Incident Response tracking Tool

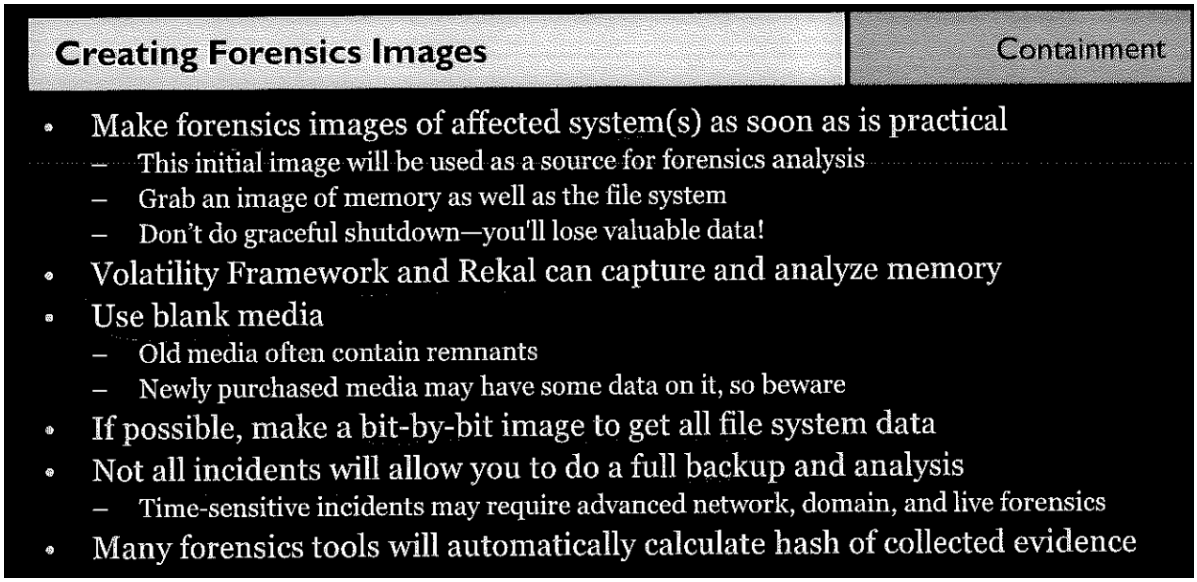
  The Next two tools helps you incident handling team to keep track of the incident in a way of assigning a tracking number for each overall incident, simplifies the sharing and centralized collection of IR data across your team



- Another option is **CyberCPR (Free tool)**, Created by SANS Instructor called Steve Armstrong, And it's a **web app** that tracks incidents, system and evidence
  - Enforces kneed to know on incidents
  - All files are hashed or encrypted upon upload
  - Tracks user tasks and activity
  - Tracks attacker campaigns
  - automates key analysis
  - Secure real-time out-of-band chat

- **Initial Analysis**
  - Keep a low profile
    - Avoid looking for the intruder with obvious ways like `ping, tracroute, nslookup`
    - Don't tip you hand to the attacker

        - Maintain standard procedure
    - Local handlers should keep reporting to command center, management sponsor or the sharing center as they gather and analyze evidence
- **Short-Term**
    - To prevent the attacker from causing even more damage, by any possible action like Disconnect the network cable, Change a name in DNS to point to a different IP address, You should also use WordWebBugs to track the attacker
- **Notifying Affected Business unit**
- **ISP Coordination**
    - For external attacks, coordinate closely with you internet provider they might help you in multiple phased like identification, containment and recovery
- **Creating Forensics Images**
    - If you don’t make a good forensics of the system before you doing detailed analysis, you are reducing the chance of that system information being usable in court, The other attorney could claim that you modified the system.



- **Write Blockers and Drive Duplicators**
    - Software write blockers runs on the host directly
    - Usually can’t use a write blocker on live systems

    - you should also consider getting a hardware live duplicator if you frequently use images, And it's much faster than using a laptop with two external hard disks.
    - The drive you store on your evidence should be 10% larger than the original drive
- **Determine the risk of continuing operations**
    - Remember, The ultimate decision for downing the machine is a business call. Make recommendations, which should documented in a signed memo to the business owner of the machine
- **Long-Term containment**
    - If the system can be kept offline (after we created forensics images), move to the eradication phase, get rid of the attacker's stuff
    - But sometime it's necessary to keep things in production, therefor you should perform long-term containment actions
- **Long-Term Actions**
    - Patch the system, and possibly neighboring systems
    - Insert IPS or in line snort
    - Null routing
    - change passwords
    - Alter trust relations between assets
    - Apply new filter rules based on the attack
    - Shut down any backup door, or accounts used by the attackers

> 💡 *The Idea of long-term containment is to apply a **temporary Band-Aid** to stay in production While you are building a clean system during **Eradication***

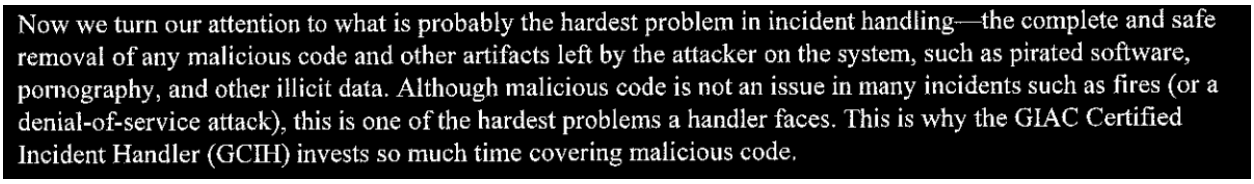
> 💡 *Don’t think you are done with the incident handling process here, just because you applied a **patch!** you have still got Eradication, Recovery and lessons learned*

> Keep system owners and administrators **briefed** on progress, Also Don’t play **the blame game,** Assigning fault now closes down important avenues of an investigation, if fault absolutely must be assigned, leave that to the **lessons learned phase**, not containment phase

Eradication

> Probably The hardest problem in incident handling process, The complete and safe removal of any malicious code and other artifacts left by the attacker on the system.

Read the next image and pay attention closely


Now we turn our attention to what is probably the hardest problem in incident handling—the complete and safe removal of any malicious code and other artifacts left by the attacker on the system, such as pirated software, pornography, and other illicit data. Although malicious code is not an issue in many incidents such as fires (or a denial-of-service attack), this is one of the hardest problems a handler faces. This is why the GIAC Certified Incident Handler (GCIH) invests so much time covering malicious code.

Why We need Eradication?

The goal is to get rid of attacker’s artifacts on the machine, You should know the **cause of the problem,** so you can solve it completely and not finding the same machine got compromised again

Some Key Points

- **Restoring from Backups**
  - In case of rootkit-style attack, wipe the drive, rebuild the system from the original install media and

    - don’t keep doing business exactly like before you got compromised, apply the patches first.
- **Removing Malicious software**
    - Remove the malware installed by the attacker.
    - As Said, if rootkit installed you should rebuild the system from the original media, rebuild the applications and Don’t forget the fkn Patches.
    - Not every attack accompanied with malware, maybe they just used legitimate service like RCE, SSH, etc..
- **Improving Defenses**
    - Like Updating the filters of The firewalls, immigrate to a New IP address, Changing DNS name, Applying patches
- **Vulnerability Analysis**
    - you should run vulnerability scanner like NESSUS (Free), There is a lot more but it’s paid, and for discovering open ports you can use Nmap (Free)
    - If you found something in one asset, there is a high chance that you find the same vulnerability in The other assets that you own.

Recovery

> The goal of the recovery phase is to put the impacted system back into production in a safe manner

- Decide when to restore operation like off-hour time slot
- Give the owners your advise, but let them give the final call
- You have to make scripts that looks for artifacts of coming back

💡 One way to improve is to learn from our mistakes and move on to **make new mistakes** instead on repeating the old ones. That’s how much **lessons learned** phase is **important**

Lessons Learned

Reporting

The goal of this phase is to document what happened to improve our capabilities

Assign all affected parties to review the draft

Meeting

After the report has reviewed, schedule a lessons learned meeting.

This meeting should occur within two weeks of resuming production

Apply Fixes

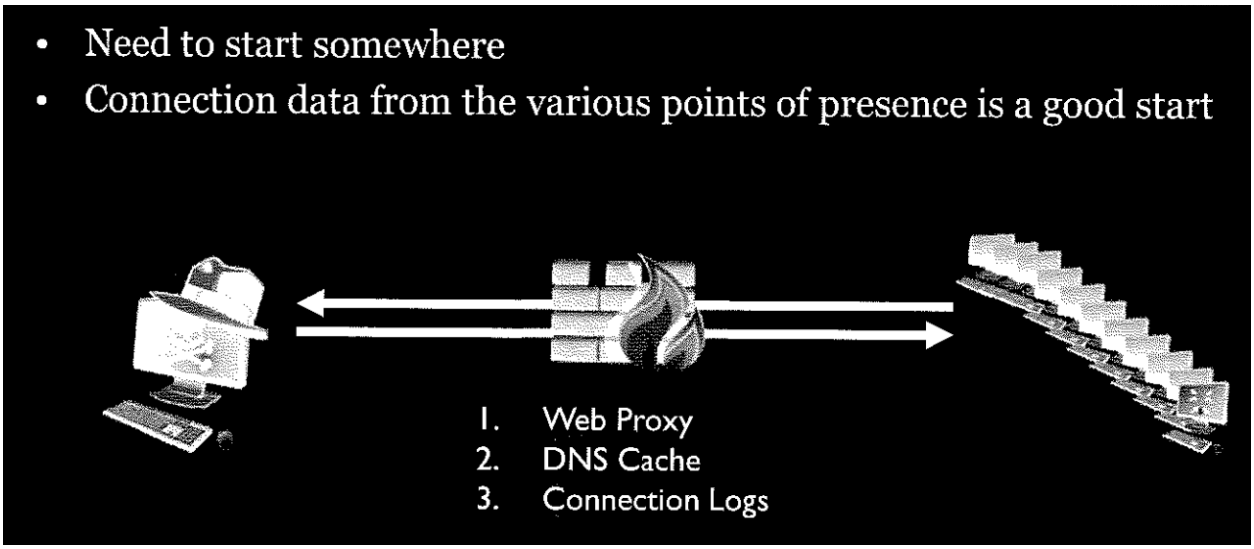
Based on what you learned, get appropriate approval and funding to fix your process, your technology and improve incident handling capabilities.

Do a root cause analysis. Like if the attack that happened, it happened because lack of policies or just a mistake.

Enterprise IR (Incident Response)

Determining if system is compromised can be difficult, doing this at **scale** across thousands of systems seems i**mpossible.** But with the **right tools** and technologies it is actually **possible.**

Many of the data point **(logs)** already being collected in your environment, you just need to know **where to look.**



- DNS logs can be very powerful, There is a tool for comparing your DNS logs with evil IP's `dns-blacklists.py`
- For the web proxy data, You can focus on the length of the URL, and strings on User-Agent

Pulling data from multiple systems

```
//Using WMIC TO PULL data from the enterprise
>wmic product get name,version,vendor
// The next command will let you run the same command on the entire enterprise.
>wmic /node:@systems.txt product get name,version,vendor /format:csv > SoftwareInventory.txt
```

You can use a tool named KANSA slide (133)

Applied Incident Handling

💡 Now we look at several incidents types and apply our six-phased process on them. We start with espionage

Espionage

- Many cases of unauthorized access to corporate systems are for espionage purposes.
- Most recent high-profile are espionage.
- In the identification phase, Google searches can be useful if attacker is sorting information on publicly accessible website
- Collect as much data as possible
- If you suspect the information is being collected and distributed by an insider, you can do this:
  1. Make up a fake activity called "Project XYX"
  2. Configure a network based IDS and/or antivirus tool with custome signature to look for the fake data.

Unauthorized Use

- The user is allowed normal access but is abusing it.
- The incident handlers frequently called upon to support:
  1. Email problems.
  2. Inappropriate web surfing

Phishing

- The attacker can do this in the email

  `<a href="http://wwe.evilwebsite.com">www.goodwebsite.com</a></p>`
- So it will appear as a good link but when you press it will direct you to another website.

Inappropriate web access

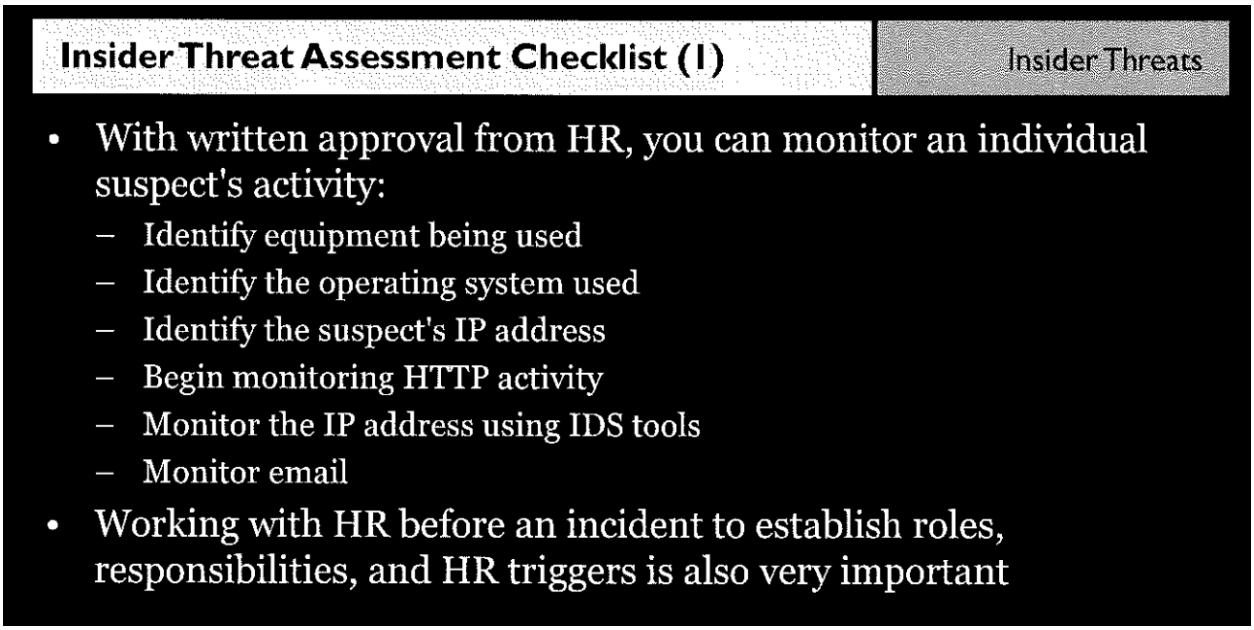
- If the manager or the HR requested you to gather some information on an employee or something like that, you don't have to say no, just make sure you get the **request in writing.**
- Sexually explicit web access can be a major problem for your organization, as incident handler your job involves helping your org minimize damage from the misuse of the computer systems
- We sometimes are called to get involved with this type of situations

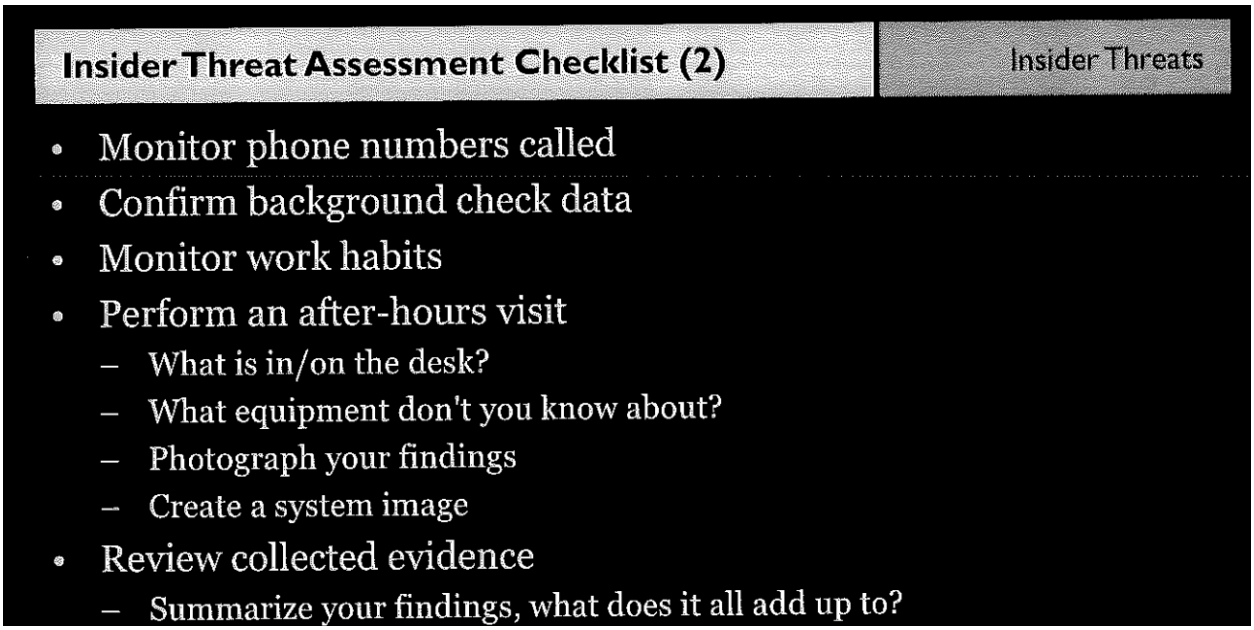
- You can filter the websites that you don’t want manually using proxies, or using tools (**GREAT TOOLS)** such as **Forcepoint**, **Blue coat** or others

Insider Threats

it doesn’t have to be, That a spy or an employee getting payed from another company to that, Maybe it’s just a leak of information (credentials or whatever).

- Since Insider threats activity can involve employees, make sure they are aware of your monitoring (Warning banners)
- With written approval from HR, you can monitor an individual suspect’s activity





Legal Issues and Cyber-Crime Laws

Computer crimes falls into two categories:

1. Traditional crimes facilitated by a computer
2. Crimes in which the computer is the target.