SIMPLE BLUETEAM PLAYBOOK

Ivan V S.

Incident Handling

- Incident handling is an action plan for dealing with the misuse of computer systems and network, such as
    - Intrusions
    - Malicious code infection
    - Cyber theft
    - Denial of service
    - Other security related events
- You are going to be hacked at some point!
    - Not a matter of if you'll get hacked, but a matter of when
    - Need to be prepared when this does happen

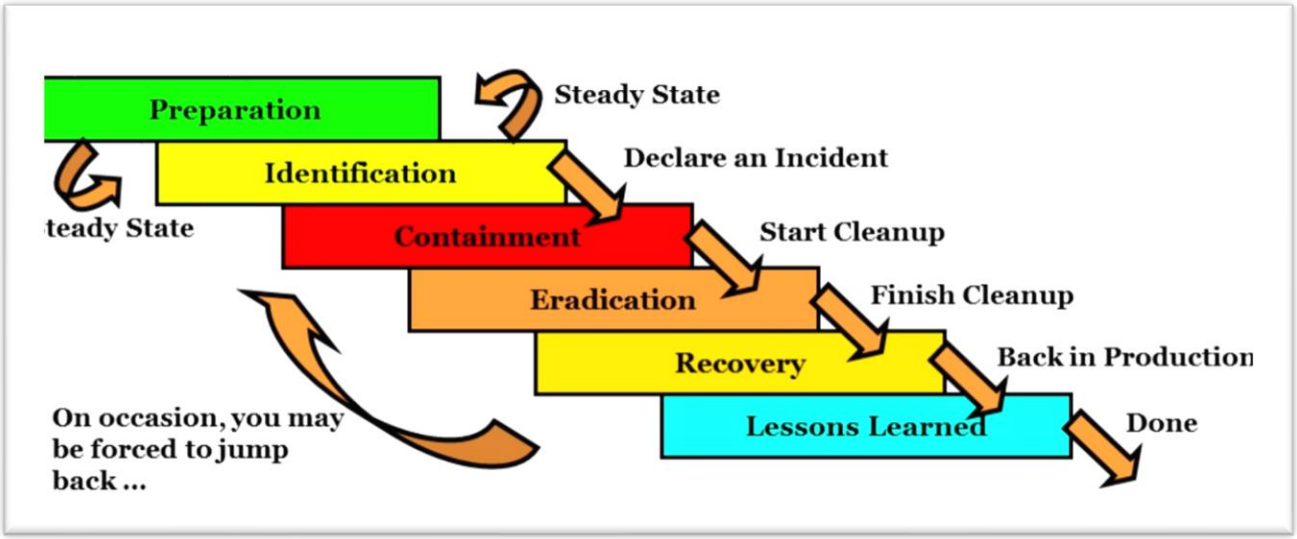
Incident Definition

- The term "incident" refers to an adverse event in an information system and / or network
- … or the threat of the occurrence of such an event
- Focus is on detecting deviations from the normal state of the network and systems
- Examples of incidents include:
    - Unauthorized use of another users account
    - Unauthorized use of system privileges
    - Execution of malicious code that destroys data
- Relates to a very large definition
    - Incident *implies* HARM or the *attempt* to HARM an organization
- Don't want to just look at the malware itself, want to look at how the malware got there
    - Was there any spam
    - Has any malware spread before this got triggered/alerted

Event definition

- It's an occurrence (not an event log)
    - Something that happens
- Examples of events:
    - The system boot sequence a system crash (could be normal behavior for that system)
    - Records of indicators of you logging in you system that goes to your SIEM
        - Records in domain controller (event logs)
        - Computer system
        - DHCP when your computer boots up and gets an IP address
        - Logs on the switch and routers
        - Firewall log when you go to the internet
        - Email server when you check your email

Incident handling process



Incident handling process (SOC)

- **Preparation** (steady state)
  - Vectra has been deployed to all 20 system members
    - Point of contact information available
  - Waiting for an alert to show up in Vectra
  - Have Endgame ready for deployment for an investigation
    - Windows and Linux
- **Identification** (declare an incident)
  - Get an alert in Vectra, notification sent to the affected the system member
  - System member contacts the SOC about an alert. IR is requested to be done by the SOC
  - Identification can happen anywhere in your environment
    - Network perimeter detection (IDS, firewall)
    - Host perimeter detection (local firewall, IPS, when data enters or leaves a host)
    - System level (host) detection (antivirus, endpoint security tools)
  - Application level detection (application log
- **Containment** (start cleanup)
  - Deploy Endgame sensor to host/machine
  - Have sensor protection turned on with Endgame first
    - Credential dumping protection
    - Credential manipulation
    - Event collection
    - Exploit protection
    - Malicious file configuration
    - Permission theft protection
    - Process injection projection
    - Ransomware projection
    - Registry monitor
  - Start the endgame investigation with our standard “file investigation” profile

        - Application
        - File system
        - Firewall rules
        - Loaded drivers
        - Network
        - Persistence
        - Process
        - Registry
        - Removable media
        - System configuration
        - Users
- **Eradication** (finish clean up) if system members gives the SOC permission to do the clean up
    - Endpoint response with Endgame
        - Delete file
        - Execute file
        - Get file
        - Kill process
        - Suspend thread
        - Upload file
    - Finish up remediation of host/computer
- **Recovery** (back in production)
    - Machine is back to normal and endgame sensor projection will remain on host for 30 days
- **Lessons learned** (done)
    - Send system member results of investigation
    - User the kill chain to figure out the advisory's strategies
    - Always avoid blame after investigation is done, use incident to enhance policies and procedures

Overview (preparation)

- The goal for preparation phase is to get the team ready to handle incident
    - **People**
    - Policy
    - Data
    - Software/hardware
    - Communications
    - Supplies
    - Transportation
    - Space
    - Power and environmental controls
    - Documentation
- People are the most important part of IR / IT
    - If you can't communicate with people in your organization (management, coworkers) in a personal conversation you aren't going to get any of the things above that you'll need
- People are the first and last line of defense

People (preparation)

- One of the most overlooked aspects of our security posture
- Also, the most easily attacked
    - Via targeted email (spear phishing)
    - Via calls (social engineering)

- Reoccurring training can be a big help
    - Annual training tends to be ineffective
    - Constant reinforcement
- You can also regularly test your users with social-engineering calls and phishing tests
    - Caller ID spoofing is a good test to employ
    - Phisihing frameworks, such as sptoolkit and Phishme
        - https://github.com/jackl0phty/sptoolkit

What you can have system admins look for

- Processes and services
- Files
- Network usage
- Scheduled tasks
- Accounts (new)
- Log entries
- Other unusual items
    - High CPU usage
    - Could be malware that's trying to run or could be memory leakage
- Additional supporting 3rd party tools

When looking at a situation, you need to determine how much damage could be caused:

- How widely deployed is the affected platform or application?
- What is the effect of vulnerability exploration, if a vulnerability is present?
- What is the value of the systems impact so far? What is the value of the data on that system?
- **Can the vulnerability be exploited remotely** (via a network connection)
    - Exploits remotely: most exploits work by a link being sent to a user, and the user clicks on the link. Your browser invokes an application and attacker exploits that application
        - Remotely exploitable vulnerability triggers something in flash or java
        - Almost every application can be invoked through your web browser
- Is a public exploit available? Was one recently released?

When more than one workstation has been compromised

- If an attacker has gained accessed to a computer on the network (domain) they are able to pivot and gains access to other system that are that same domain

Initial Security Incident Questionnaire for Responders

- https://zeltser.com/security-incident-questionnaire-cheat-sheet/

Security Incident Survey Cheat Sheet for Server Administrators

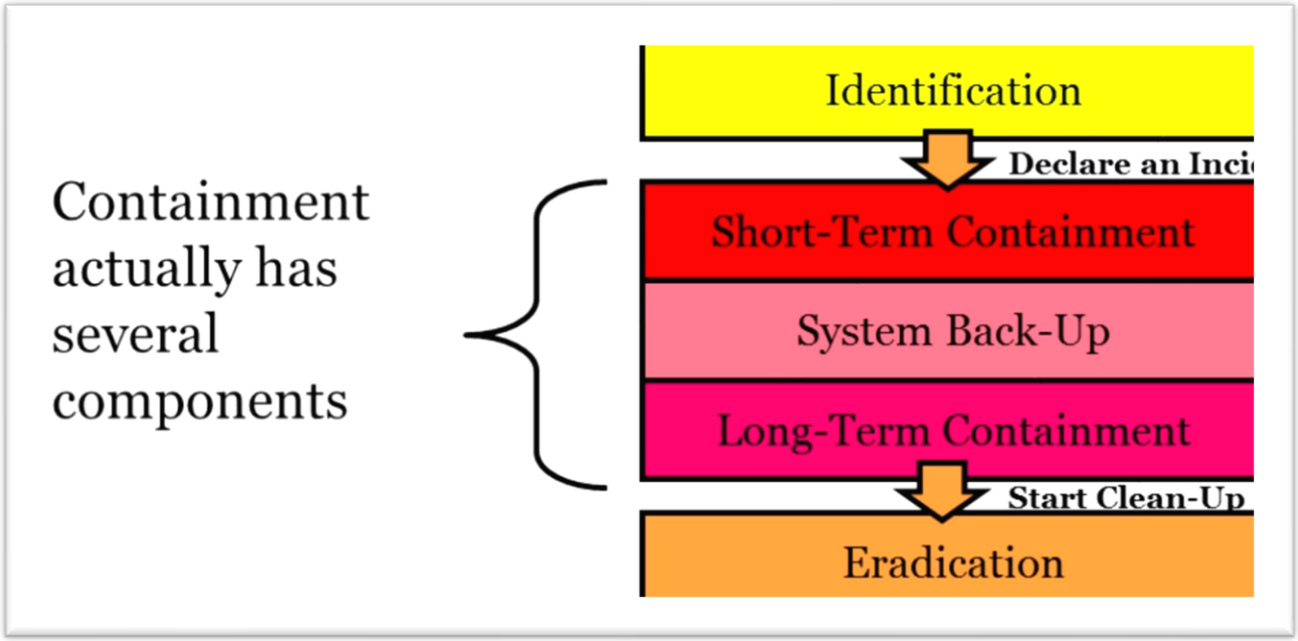
- https://zeltser.com/security-incident-survey-cheat-sheet/

Chain of custody

- Do not delete ANY files until the case is closed out, even then if you have storage space, saved them for a document retention timeframe approved by you legal team (or Dan)
- Identity every piece of evidence in your notebook (or your word document)
- Control access to evidence

Containment

- Goal of containment is to stop the bleeding
    - Prevent the attack from getting any deeper into the impacted system or spreading to other system
        - Can use Endgame's sensor protection for this



Characterize incident

- CSIRT case classification document
    - https://www.first.org/resources/guides/csirt_case_classification.html
- Given that we have declared an incident, we need to record its category (one or more), severity (based on current understanding… subject to change) and sensitivity
- Category
    - Denial of service
    - Compromised information
    - Compromised Asset
    - Unlawful Activity
    - Internal Hacking
    - External Hacking
    - Malware
    - E-mail
    - Policy Violation
- Criticality
    - Incident impacts critical system: (sample time for your to customize)
    - Incident impacts non-critical system:4 hrs
    - Possible incident, non-critical: 24 hrs

- Sensitivity: who should be informed?
    - Extremely sensitive (CSIRT, mgmt.)
    - Sensitive (CSIRT, mgmt., sys owners, ops)
    - Less sensitive (employees informed of isolated virus infection)

Initial analyst

- Keep a low profile (SOC will use endgame to avoid detection from the intruder)
    - Avoid looking for the intruder with obvious methods from the compromised machine (ping, traceroute, nslookup)
    - Don't tip your hand to the attacker
    - Maintain standard procedures
- Local handlers should keep making reports to the command center as they gather and analyze evidence

Eradication

- With the bleeding stopped, the goal of the eradication phase is to get rid of the attackers artifacts on the machine
- Determine cause and symptoms of the incident
    - Use information gathered during the identification and containment
    - Try to isolate the attack and determine how it was executed
- If we know where the malware is, we're going to try to remove the root cause of the incident
    - *Malware on a system is not a root cause, it's a symptom*
- How the malware got on the system is the root cause
    - Often times it's a user clicking on a link
- Root cause
    - how did we get compromised in the first place
    - need to eradicate that door that the bad guys are using

Restoring from backup

- locate the most recent clean backup
    - search for a recent backup before an intrusion
    - in case of a rootkit style attack (which modifies the OS itself)
    - wipe the drive (zeroing it out), reformat, and rebuild the system from the original install media and patches

Removing malicious software

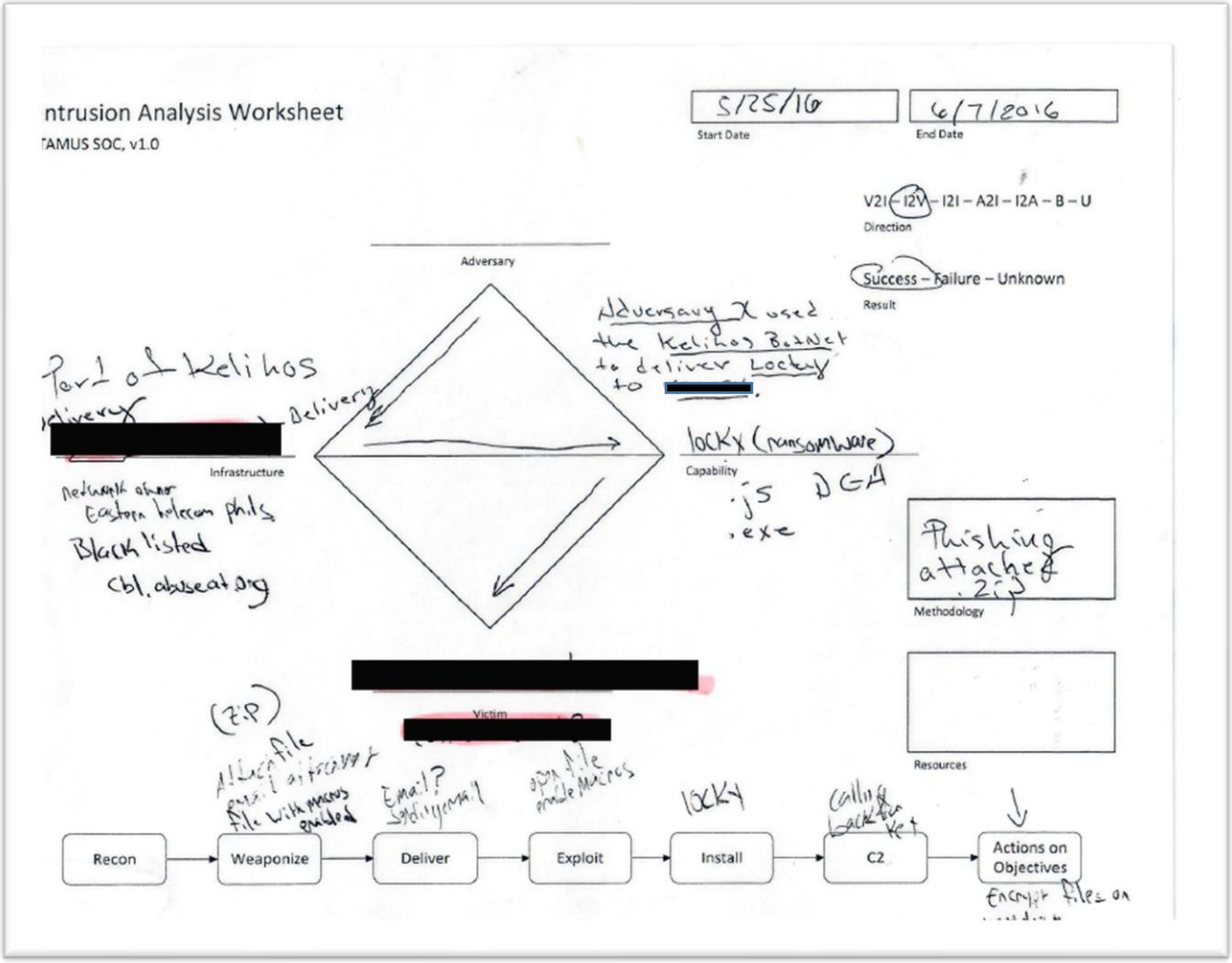
- remove malware inserted by the attacker
    - virus infestations
    - backdoors
    - rootkits and kernel level rootkits
- If you have a rootkit or kernel level rootkit you should rebuild from scratch
    - format the drive
    - OS (and patches)
    - Applications (and patches!)
    - Data (hardest one… possibly tainted backup)
- Encourage the impacted business unit to rebuild, reviewed by the computer security team (including incident handlers)
- Unfortunately, there may be times where the attacker didn't use malware
    - Use malware for initial infection on a standalone workstation

- From that point on, going to try to get remote desktop access, or citrix access (secure application access solution that provides administrators granular application-level control while empowering users with access from anywhere)

- Bad guy wants to get deep inside the organization
  - When the attacker is already that far into the organization, its almost impossible to detect with stand ways

Looking for artifacts to come back

- One of the most important things handlers can do during recovery and follow up is to check regularly for re-compromise
- Note that attackers don't always use malware; sometimes, they log in via normal mechanisms for which we can look
- Windows reg command
  - Look for unusual processes
- Windows wmic or tasklist commands, or Linux ps command
  - Looking for accounts used by the attacker
- Windows wmic useraccount or net user commands, or Linux cat /etc/passwd
  - Look for simultaneous login
- Look at the Spam filer logs
  - Bad guys could be trying to claw their way back in by trying a spear phishing attack



Instruction analyst model

Enterprise IR

- Determine if one system is compromised can be difficult
- Doing this at scale across thousands of system can seem impossible
- With the right tools (endpoint security platform) and techniques it is possible
- Many of the data points are already being collected in your environment (IDS)
- You just need to know where to look

All of your malware is going to go through these different points (this is your bottle neck)

- Web proxy
- DNS cache (DNS resolution)
- Connection logs (makes connection through your firewall)
- If you try to look at everything, you're not going to see anything
- Going to go through your web proxy, going to do DNS resolution and make connections through your firewall

DNS data

- DNS can be very powerful
- Simply reviewing a DNS server's log and cache can reveal systems that are connected to know bad IP addresses and domains
- Dns-blacklist.py can review IP addresses and domains
- Malware Domain list is a great site for updated lists of know bad actors
    - https://www.malwaredomainlist.com/mdl.php

Security measures are like waves and the bad guy is like a surfer

- As the bad guy is attacking your network the wave behind it is tracking their IP and domains and the bad guy is right in front of the waves
    - always staying in front
- Malware and domains that are used to attack our network are going to be different than the domains that are used to attack other networks and agencies

If you grab DNS data form the first of the month and do an analysis on it at the end of the month on an up to date blacklist

- You're going to see system that are making a connection to bad domains a lot clear

Web proxy data

- A lot of malware uses http as its command and control protocol
    - You can look at the domains, but you can also look at the URLs (how long they are)
- Some bad guys use base 64 encoding and they encode their URLS
    - They put command and control in the URL instead of the payload

User agent string

- During a HTTP request, the web client sends information about itself in a string with the prefix "User-agent"
    - This information typically identifies the client browser, host operating system and language
- It can be modified or spoofed by the end user
    - Can be done by using netcat
- Unique identifier for your browser
- It is your browser saying "I'm Firefox, I'm windows 10, I'm MS edge on windows 10
- A lot of malware is using statically built user agent strings on their source codes
    - From windows 7 and even XP
- You need to look at the agent strings and play "which of these is not like the other" and which of these does not belong
- Review the length of URLs being visited
    - Many malicious URLs are very long
- Review user agent strings
    - Many malware specimens use older or odd user agent strings

Example of user agent strings:

- Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
    - **Mozilla/5.0**: indicates browser compliant with historical standards
    - **Trident/7.0**: rv:11.0: Internet Explorer 11.0, which user Trident rendering engine
    - **Windows NT 10**: the browser is running on windows 10:
        - NT 6.3 is Windows 8.1/2012R2, NT 6.2 is Windows 8/2012, NT 6.1 is Windows 7/2008R2 and NT 6.0 is Vista/2008

GET and POST methods

- **GET**: a client a GET request to obtain a web resource from the server by passing any parameters via the URL
    - Allows for bookmarks to save parameters
        - Could be dangerous for authentication related and session tracking parameters
    - Easy manipulation by attacker and pen testers
- **POST**: a client uses a POST to request a web resource but passes parameters via the HTTP payload:
    - Still can be manipulated
    - Often can be changed to a GET for simpler scripting
        - If the application supports method interchange
        - Register globals is one way this happens in PHP
- **HEAD**: will return only the HTTP header:
    - Results of a request
    - Speeds up testing if the testers is interested in header data
- When you have sensitive data in your GET, you have problems
- GET/POST are both used for sending and receiving data

Connection data (malware phoning)

- Called beaconing
  - When malware phones home
- Characteristics of beaconing
  - Have a backdoor that beacons out every 30 seconds
  - Backdoor that beacons out at random intervals
  - Makes a connection and stays established for more than 24 hours
- All of this abnormal

WMIC

- Can get a list of process and can get all the software that's on a system
  - Dump every piece of software installed
- Let's pull everything
  - C:\ > wmic product get name,version
  - C:\> wmic /node:@system.txt product get description,name,vender /format:scv> softwareInventory.txt
- The /node:@system.txt allows you to run the same command on multiple systems

Cybercrime laws

- https://www.justice.gov/criminal-ccips
- https://www.hg.org/computer-crime.html

Follow the TCP stream

- Client traffic is red; server is blue
  - Note the client header, include the user agent and other fields
- User actually going to a website (below)

Normal GET request from a user (Follow TCP stream)

GET /exercise1.html HTTP/1.1
HOST: www.sec542.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html, application/xhtml+xml,application/xml;q=0.8
Accept-Language: en-US, en;q=0.5
Accept-Encoding; gzip, deflate
Connect: keep-alive
Pragma: no-cache
Cache-control: no-cache

HTTP/1.1 200 OK
Date: Fri, 02 Jan 2015 19:36:59 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Sun, 21 Dec 2014 19:49:22 GMT
Etag: "33e-50abf3de16ea5-gzip"

- Encrypted with Gzip (gunzip)
  - Doesn't let you see the connect
  - Doesn't get decompressed

- Wireshark will show you that it is encrypted by Gzip
    - Follow won't show you the decrypted input, shows you the raw
- Handcrafted POST sends the bare minimum of input, while real web browsers send much more
    - Browsers are much more chatty and have more headers
    - Don't have the accept-language and accept-encoding

Handcrafted post using NetCat

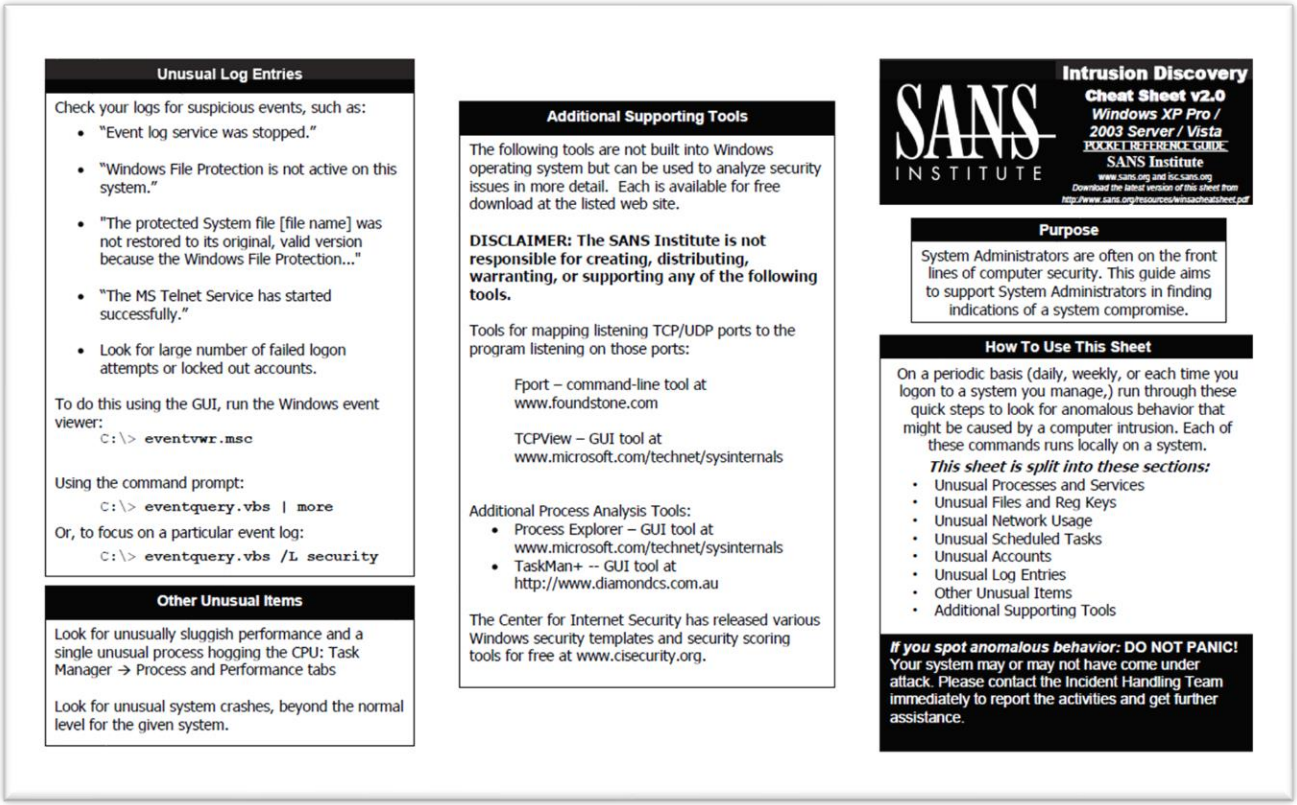
```
POST /form_auth/login.php HTTP/1.0
Content-Length: 34

User=marvin&pass=test&button=Login
HTTP/1.1 200 OK
Date: Fri, 02 Jan 2015 19:38:00 MGT
Server: apache/2.4.7 (Ubuntu)
X-Powered-by: PHP/5.5.9-lubuntu4.5
Vary: Accept-encoding
Content-Length: 833
Connection: close
Content-Type: text/html
```

- Machine traffic using netcat ^^^^
    - There's less input
    - A way to ID C2 even if they have a good user agent
        - Look at the number of headers counted, they don't have enough flair going on to look like a normal browser

What is a port?

- Port is like an entry point or exit point to a house
    - If you look at your house, you have doors, windows, pipes, electrical lines (all ports coming in and out of your house)
- There are 65,536 ports (doors in your computer)
    - Doors coming in and out of your house
    - Some of the doors are locked and some of them are unlocked
- If you see a port (door) that's unlocked on your computer (house) you can lock it and prevent anyone getting in
- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
- http://www.infosyssec.org/infosyssec/security/portlookup.html



Unusual Log Entries

Check your logs for suspicious events, such as:

- "Event log service was stopped."
- "Windows File Protection is not active on this system."
- "The protected System file [file name] was not restored to its original, valid version because the Windows File Protection..."
- "The MS Telnet Service has started successfully."
- Look for large number of failed logon attempts or locked out accounts.

To do this using the GUI, run the Windows event viewer:

```
C:\> eventvwr.msc
```

Using the command prompt:

```
C:\> eventquery.vbs | more
```

Or, to focus on a particular event log:

```
C:\> eventquery.vbs /L security
```

Other Unusual Items

Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager → Process and Performance tabs

Look for unusual system crashes, beyond the normal level for the given system.

Additional Supporting Tools

The following tools are not built into Windows operating system but can be used to analyze security issues in more detail. Each is available for free download at the listed web site.

DISCLAIMER: The SANS Institute is not responsible for creating, distributing, warranting, or supporting any of the following tools.

Tools for mapping listening TCP/UDP ports to the program listening on those ports:

Fport – command-line tool at www.foundstone.com

TCPView – GUI tool at www.microsoft.com/technet/sysinternals

Additional Process Analysis Tools:

- Process Explorer – GUI tool at www.microsoft.com/technet/sysinternals
- TaskMan+ -- GUI tool at http://www.diamondcs.com.au

The Center for Internet Security has released various Windows security templates and security scoring tools for free at www.cisecurity.org.

SANS INSTITUTE

Intrusion Discovery Cheat Sheet v2.0

Windows XP Pro / 2003 Server / Vista

POCKET REFERENCE GUIDE

SANS Institute

www.sans.org and isc.sans.org

Download the latest version of this sheet from http://www.sans.org/resources/winsacheatsheet.pdf

Purpose

System Administrators are often on the front lines of computer security. This guide aims to support System Administrators in finding indications of a system compromise.

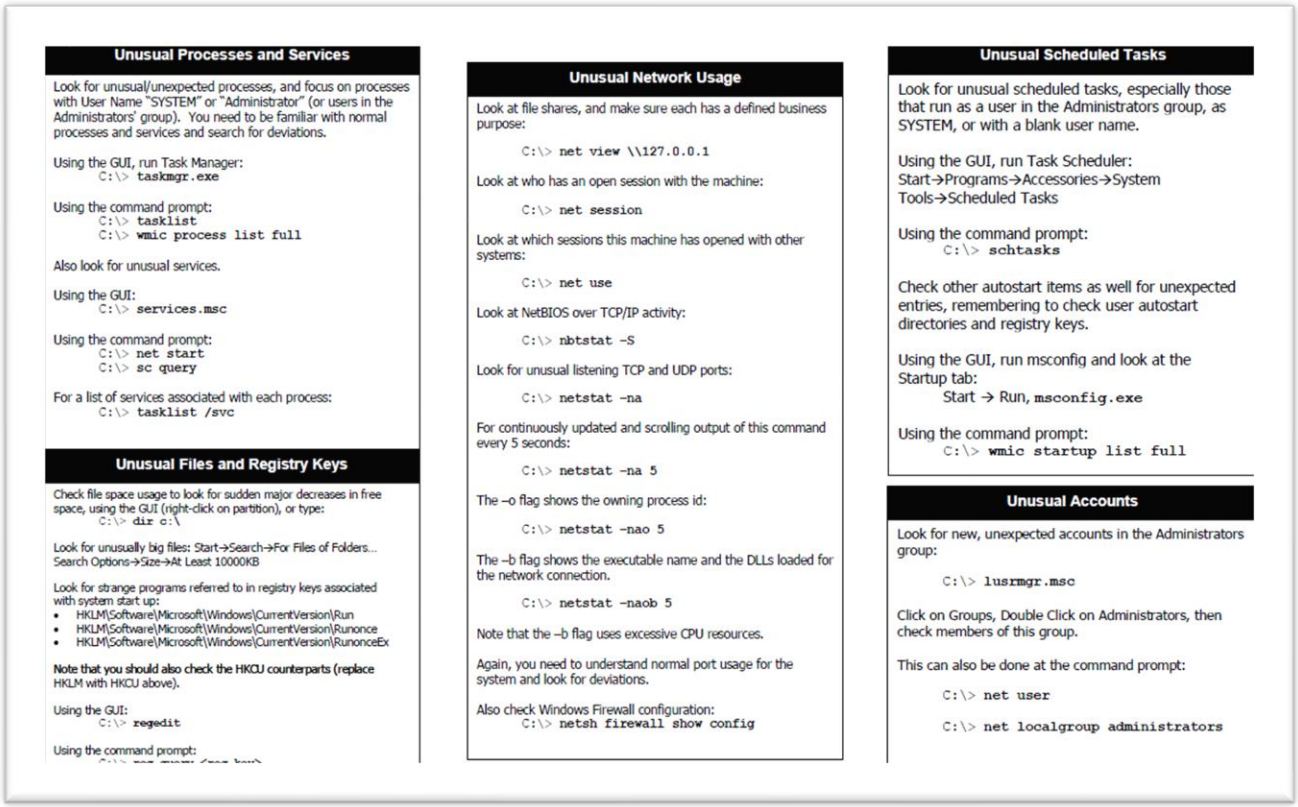
How To Use This Sheet

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Unusual Processes and Services
- Unusual Files and Reg Keys
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- Other Unusual Items
- Additional Supporting Tools

If you spot anomalous behavior: **DO NOT PANIC!** Your system may or may not have come under attack. Please contact the Incident Handling Team immediately to report the activities and get further assistance.



Unusual Processes and Services

Look for unusual/unexpected processes, and focus on processes with User Name "SYSTEM" or "Administrator" (or users in the Administrators' group). You need to be familiar with normal processes and services and search for deviations.

Using the GUI, run Task Manager:
```
C:\> taskmgr.exe
```

Using the command prompt:
```
C:\> tasklist
C:\> wmic process list full
```

Also look for unusual services.

Using the GUI:
```
C:\> services.msc
```

Using the command prompt:
```
C:\> net start
C:\> sc query
```

For a list of services associated with each process:
```
C:\> tasklist /svc
```

Unusual Files and Registry Keys

Check file space usage to look for sudden major decreases in free space, using the GUI (right-click on partition), or type:
```
C:\> dir c:\
```

Look for unusually big files: Start→Search→For Files of Folders... Search Options→Size→At Least 10000KB

Look for strange programs referred to in registry keys associated with system start up:
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

Note that you should also check the HKCU counterparts (replace HKLM with HKCU above).

Using the GUI:
```
C:\> regedit
```

Using the command prompt:

Unusual Network Usage

Look at file shares, and make sure each has a defined business purpose:
```
C:\> net view \\127.0.0.1
```

Look at who has an open session with the machine:
```
C:\> net session
```

Look at which sessions this machine has opened with other systems:
```
C:\> net use
```

Look at NetBIOS over TCP/IP activity:
```
C:\> nbtstat -S
```

Look for unusual listening TCP and UDP ports:
```
C:\> netstat -na
```

For continuously updated and scrolling output of this command every 5 seconds:
```
C:\> netstat -na 5
```

The –o flag shows the owning process id:
```
C:\> netstat -nao 5
```

The –b flag shows the executable name and the DLLs loaded for the network connection.
```
C:\> netstat -naob 5
```

Note that the –b flag uses excessive CPU resources.

Again, you need to understand normal port usage for the system and look for deviations.

Also check Windows Firewall configuration:
```
C:\> netsh firewall show config
```

Unusual Scheduled Tasks

Look for unusual scheduled tasks, especially those that run as a user in the Administrators group, as SYSTEM, or with a blank user name.

Using the GUI, run Task Scheduler:
Start→Programs→Accessories→System Tools→Scheduled Tasks

Using the command prompt:
```
C:\> schtasks
```

Check other autostart items as well for unexpected entries, remembering to check user autostart directories and registry keys.

Using the GUI, run msconfig and look at the Startup tab:
Start → Run, `msconfig.exe`

Using the command prompt:
```
C:\> wmic startup list full
```

Unusual Accounts

Look for new, unexpected accounts in the Administrators group:
```
C:\> lusrmgr.msc
```

Click on Groups, Double Click on Administrators, then check members of this group.

This can also be done at the command prompt:
```
C:\> net user

C:\> net localgroup administrators
```

What is a rootkit?

- A rootkit is a special variant of a Trojan, a.k.a. a RAT (Remote Administration Tool). What separates a rootkit from a regular Trojan is that a rootkit, by definition, occupies Ring 0, also known as root or kernel level, the highest run privilege available, which is where the OS (Operating System) itself runs
- Rootkits subvert the OS through the kernel (core operating system) or privileged drivers. This enables a rootkit to operate as a part of the OS itself rather than a program being run by the OS. This high level of sophistication makes rootkits extremely difficult to detect and remove. Often anti-virus products will be unable to detect or remove a rootkit once it has taken over the OS and more specialized detection and removal procedures are required

Registry entries which could be used to load a rootkit into memory should also be given looked at, examples:

- HKLM\SYSTEM\CurrentControlSet\Services,
- HKLM\Software\Microsoft\Windows\CurrentVersion*
- HKCU\Software\Microsoft\Windows\CurrentVersion*
- HKLM\Software\Microsoft\InternetExplorer*
- HKCU\Software\Microsoft\Internet Explorer*
- HKCR\exefile\shell\open\command HKLM\Software\Classes\exefile\shell\open\command HKLM\Software\Microsoft\ActiveSetup\InstalledComponents
- Look in system directories for hidden files
    - C:\Windows\system32