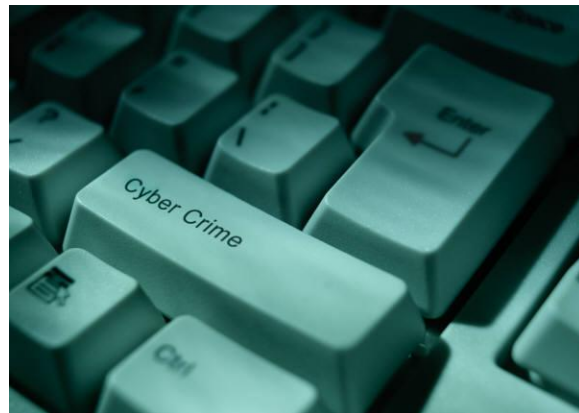


# Incident Response

## Six Best Practices for Managing Cyber Breaches

## What We'll Cover

- Your Challenges in Incident Response
- Six Best Practices for Managing a Cyber Breach
- In Depth: Best Practices for Collecting Volatile Data



## Data is the Lifeblood of Your Company



## Data is the Lifeblood of Your Company



## Cyber Security Trends

Ninety percent of businesses were hit by a cyber security breach in 2010-2011. Breaches cost \$500,000 or more, for up to 41 percent of the businesses reporting a breach. And the top two endpoints under attack are laptops and mobile devices.

- 52 percent of respondents say that 10 percent or less of their IT budget is allocated to security
- 40 percent of respondents didn't know the source of the attacks
- 52 percent said insider abuse led to security breaches at their companies and 48 percent cited malicious software downloads

Source - survey of surveyed 583 IT and security professionals:  
<http://m.zdnet.com/blog/btl/cybersecurity-by-the-numbers-how-bad-is-it/51145>



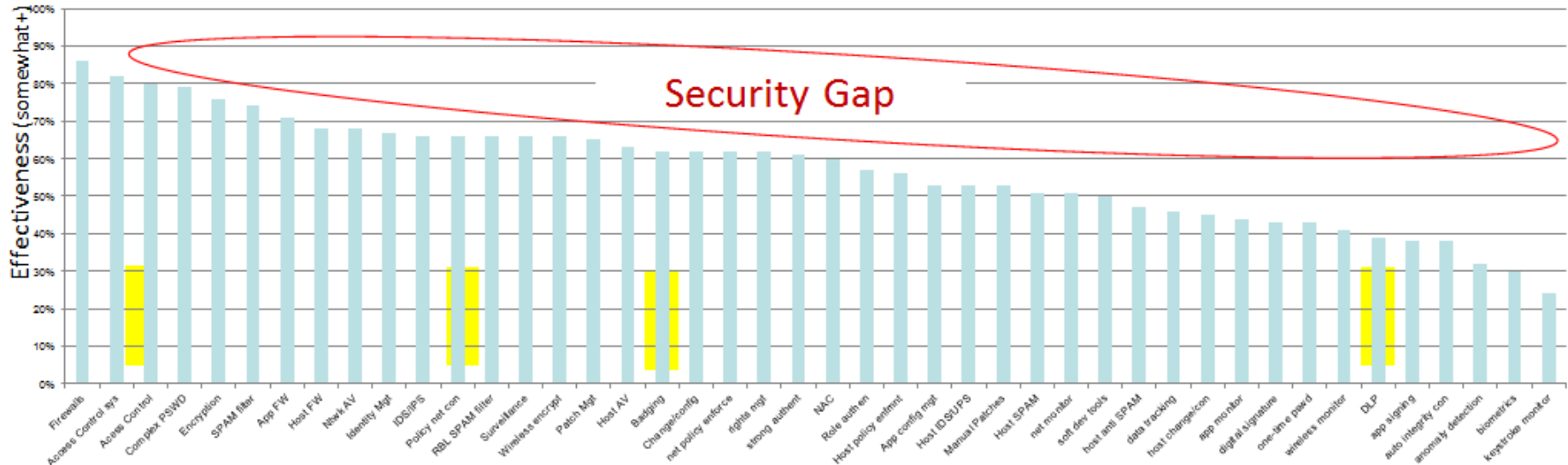
# Incident Response Best Practices



Firewalls rated most effective...at 86%

DLP near the bottom, rated 38% effective

**Multiple technologies must be layered for effective security.**



\*Source: 2010 Cybersecurity Watch Survey

## Large Data Breaches

- **Heartland Payment Systems** – 130 million records – hacked January 2009
- **Target Corporation** – 70 to 110 million records – hacked November 2013
- **TJX Companies, Inc.** – 94 million records – hacked January 2007
- **Sony Corporation** – 77 million records – hacked April 2011
- **National Archives** – 76 million records – improper disposal, October 2009
- **Epsilon** – 60 million records – hacked March 2011
- **LivingSocial, Inc.** – 50 million records – hacked April 2013
- **RockYou, Inc.** – 32 million records – hacked December 2009
- **Zappos.com** – 24 million records – January 2012



## Your Challenges are Many

- Perimeter defense is never enough
- With new technologies, come new exploits
- Threats can also be internal and/or inadvertent
- A determined hacker will find a way (high end)
- Hacking has become “productized” (low end)
- Attacks will continue 24/7/365





## Your Challenges are Many

*Continued*

- Anonymity will challenge attribution
- Malware will be custom designed for specific targets
- You live in a zero-day environment ... if you don't know about it, it is zero day to you
- Polymorphic/metamorphic code is prevalent and evades signature-based detection
- Defenders have to be right 100% of the time



## You've been compromised – now what?

Your network security has been breached — now what do you do? Your data is leaving...

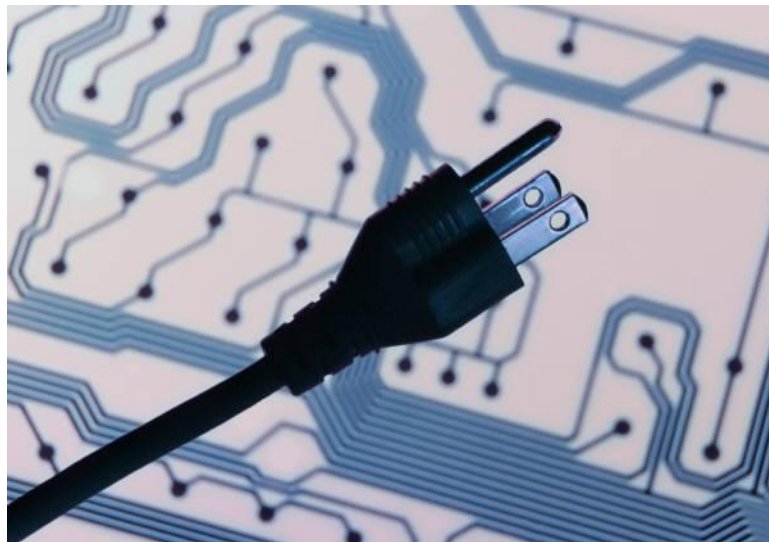
- Is the threat internal or external?
- Inadvertent or malicious?
- Was there malware involved?
  - Where was it?
  - Where is it now?
  - What does it look like?
- Find it, where it went, what it morphed to, and remediate it.



## IR Techniques and Considerations

The traditional method of collecting digital evidence and subsequently examining that evidence has been to shutdown the system, either gracefully or by pulling the plug, and then image all the media contained within the system for later static analysis.

With the advancement of malware today and memory-only resident malicious code that never touches the hard disk, **it is extremely important to try to capture the contents of memory** for inclusion in your overall analysis methods.



## Advanced Persistent Threat

A major problem is the advanced clandestine compromise of a network by sophisticated attackers, known as an “APT” or Advanced Persistent Threat – a “buzzword” that is still a real threat. [APT is used throughout the industry with differing meanings. It is really a specific targeted attack with an intended outcome.]

An APT is intrusion into a network using multiple, sophisticated recon methods that is very hard to eradicate due to the use of stealthy techniques.

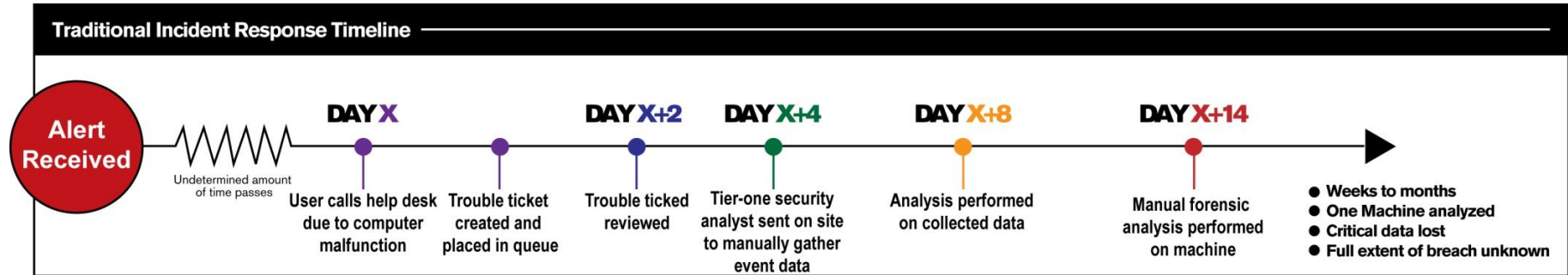
An APT often has five phases:

1. Reconnaissance
2. Attack
3. Compromise
4. Install backdoor
5. Persistent exploitation



## Typical Incident Response Timeline

- Time to detection could be weeks or months
- Typical manual incident response time is several days
- In contrast, network-enabled incident response can be real or near time, and automated with integration into a Security Information and Event Management (SIEM) application.



## Incident Response: Six Best Practices for Managing Cyber Breaches



## Best Practice #1: Prepare

### Training

- Incident response process planning
- Tools and trends
- Security awareness

### Tools

- Layered security
- Manual vs. network-enabled response

### Process

- Understand sensitive data location and use
- Keep systems patched and up-to-date
- Ongoing vulnerability testing
- Implement full incident response process
- Test the process with regular “fire drills”

**The Veterans Administration “unplugged” employees and contractors who do not complete CS training.**

Source: <http://gov.aol.com/2012/04/02/va-to-unplugs-employees-who-skip-cybersecurity-training>

## Best Practice #2: Identify and Expose

- “The art of SIEM is to – at best – identify exactly the critical situations which need to be handled. Not more, not less.”  
– *Martin Kuppinger, Founder and Principal Analyst, KuppingerCole*
- The problem is, no organization can do that perfectly – no SIEM is ever tuned to such a fine degree of precision so that only the “critical situations which need to be handled” are immediately presented to the incident response team.
- Use network-enabled cyber forensics tools to quickly reveal suspect or mutating software on any system in your network through SIEM integration
  - Cross-platform
  - Speed is essential to find and collect actionable volatile data



Source: <http://blogs.kuppingercole.com/kuppinger/2011/10/09/siem-its-not-mainly-about-tools/>



## Best Practice #3: Triage

- Understand the extent of the compromise or capabilities of the malware
- Zero in on the biggest threats first
- Determine if personal identifying information and/or intellectual property was compromised



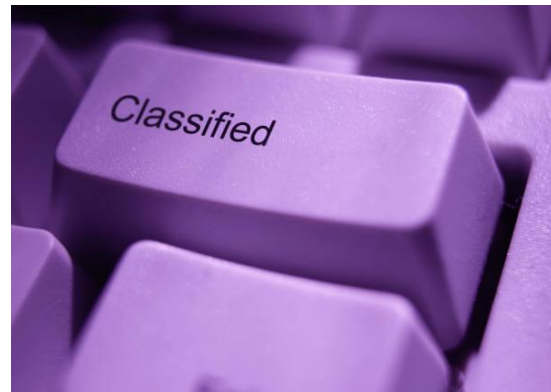
## Best Practice #4: Contain

- Remotely collect malware and relevant data with network-enabled forensic tools
  - Collect and preserve volatile data as evidence (more in a bit)
  - Capturing the crucial malware and artifacts to determine remediation steps
    - It is polymorphic or metamorphic?



## Best Practice #5: Recover & Audit

- Remediate systems by deleting all malicious or unauthorized code
  - Both on the identified systems and then proactive remediation network wide
- Conduct a sensitive data audit of the affected systems
  - Personal identifying information
  - Intellectual property
  - Classified materials
  - etc.



## Best Practice #6: Report & Lesson Learned

- Consult relevant data breach notification regulations
- Breach notification plan for internal stakeholders (Legal, IT, PR, Executive team etc.)
- Reporting – no matter how smart you are, if no one can understand your report, they won't understand the value you are contributing

### Lessons Learned

- What did we intend to do?
- What went right?
- What went wrong?
- What can we do better?
- Adapt, document and implement...

## In Depth: Best Practices for Collecting Volatile Data



## Why volatile data?

- What is volatile data?
- Why is it so important to the incident response process?
- How would an examiner use this data?
- How does you relate volatile data to static data in order to assess threats and risks?

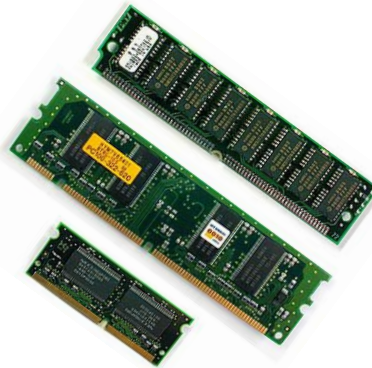


## Volatile Data Defined

Volatile data exists in the main memory (RAM) of a server or workstation; if power is lost or a system fault occurs, the data will be lost. Volatile data includes:

- Currently logged on user
- TCP and UDP port information
- Open files
- Running processes and applications
- Encrypted volumes and RAM drives
- System resource utilization.

In general, volatile data stored in RAM is used by the system for administration and processing purposes.



**In contrast static (or nonvolatile) data is information stored on hard drives, USB devices, CDs, etc., and is typically not lost when a power loss or system fault occurs.**

## Heisenberg Principle and Incident Response

Because you will be collecting volatile data on a live system, **things will constantly be changing as information is being gathered and copied.**

One of the principles of quantum physics is the Heisenberg Uncertainty Principle named after Werner Heisenberg.

Heisenberg formulated the principle associated with measuring the location of an atomic particle or the motion of that same atomic particle in space, but not being able to do both because **the action of one procedure alters the outcome of the second.** This is due to the fact that in order to measure it, you have to stop its motion.

The same principle applies in incident response today; **you cannot collect volatile data without inadvertently introducing additional data during the collection process.** You also can't stop the computer or freeze its activity while you copy the exact state everything is in. Therefore **the order in which you collect the volatile data is important.** Data that is considered more volatile than others should be collected first.

$$\Delta p \Delta x \geq \frac{1}{2} \hbar$$

### Order of volatility

- Memory contents (RAM)
- Network information
- Running process information
- Disk contents (static data)



## Collecting Volatile Data

Collecting volatile data is similar to photographing and documenting a crime scene.

Keeping with the analogy, the ability to get an accurate picture of the volatile data from a running machine is referred to as a “snapshot.”

**Snapshots gather volatile data and provide information on what was occurring on a system at a given point in time.**

A volatile data snapshot can then be analyzed in an attempt to discover the source and extent of an intrusion or compromise as well as provide leads for additional investigation.



## What volatile data can reveal

Volatile data may reveal invaluable information both during and after an incident has occurred.

Analysis of volatile data captures can answer questions such as:

- Are any ports open that should not be?
- Are unfamiliar services or machines accessing the system?
- Are unknown applications or processes executing?

Such information helps you determine what was happening on the system at the point in time the snapshot was taken, and if an attack was actively occurring.



## Correlation with Static Data

The correlation of volatile data and static data is essential, but not exhaustive to the incident response and examination process.

**Volatile data can help you determine if suspicious activities or applications are active on a system** and help guide you in the search for backdoors or malicious code.

Additionally it may help you determine who and what is accessing the system and its resources whether internal or externally. One of the most important aspects of volatile data capture is that it **provides you with the ability to quickly ascertain if unauthorized ports, processes, or applications are active.**

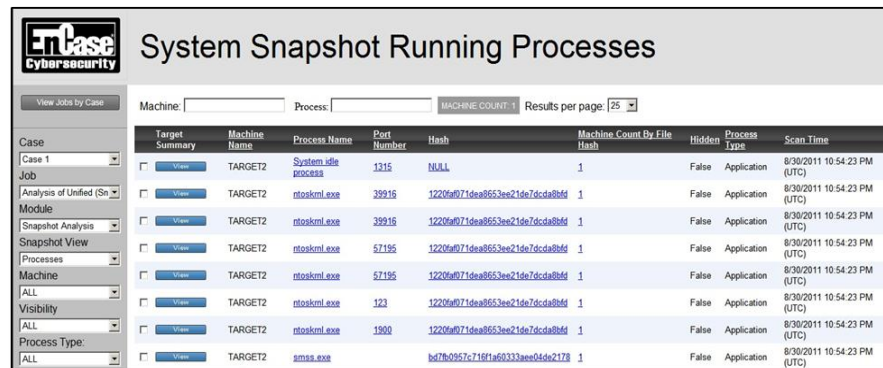
This information is **critical when deciding whether to continue system operation or take the system offline.** This is a crucial component of incident response triage; the ability to rapidly determine to what extent if any a system has been compromised.



## Volatile Data Components

- **Process memory dumps** – Dumps of memory areas used to run specific processes (identified via process ID number or PID).
- **Open ports** – Open ports are the active endpoints to a logical TCP or UDP connection on a system at a particular point in time.
- **Active sockets/current connections** – As open ports indicate active endpoints, active connections are established sockets or vectors of communication between two endpoints (application to application, or host to host).

**\*NOTE:** *It is important to obtain information about the actual programs that have opened ports or are responsible for active sockets.*



The screenshot shows the 'System Snapshot Running Processes' window in EnCase Cybersecurity. It features a sidebar with navigation options like 'Case', 'Job', 'Module', 'Snapshot View', 'Processes', 'Machine', 'Visibility', and 'Process Type'. The main area displays a table of running processes for a specific machine (TARGET2). The table includes columns for Target Summary, Machine Name, Process Name, Port Number, Hash, Machine Count By File Hash, Hidden status, Process Type, and Scan Time. Each row has a 'View' button next to the process name.

Target Summary	Machine Name	Process Name	Port Number	Hash	Machine Count By File Hash	Hidden	Process Type	Scan Time
<input type="checkbox"/> View	TARGET2	System Idle process	1215	NUL	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	ntoskml.exe	39915	1220f071dea8653ee21de7dcda86d	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	ntoskml.exe	39915	1220f071dea8653ee21de7dcda86d	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	ntoskml.exe	57195	1220f071dea8653ee21de7dcda86d	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	ntoskml.exe	57195	1220f071dea8653ee21de7dcda86d	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	ntoskml.exe	123	1220f071dea8653ee21de7dcda86d	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	ntoskml.exe	1900	1220f071dea8653ee21de7dcda86d	1	False	Application	8/30/2011 10:54:23 PM (UTC)
<input type="checkbox"/> View	TARGET2	smss.exe		bd7b0957c718f1a69333aee05de2178	1	False	Application	8/30/2011 10:54:23 PM (UTC)

## Volatile Data Components

- **Active processes** – Active processes are the executables that are running on a computer at a particular point in time, including hidden processes
- **Active services** – Active services are those programs that are being run (and sometimes autostarted) as a service on the system (e.g., DHCP Client).
- **Open files** – Open files are the files that are in use on a computer at a particular point in time.
- **Currently logged on users** – A record of those users currently logged on or interacting with the system.

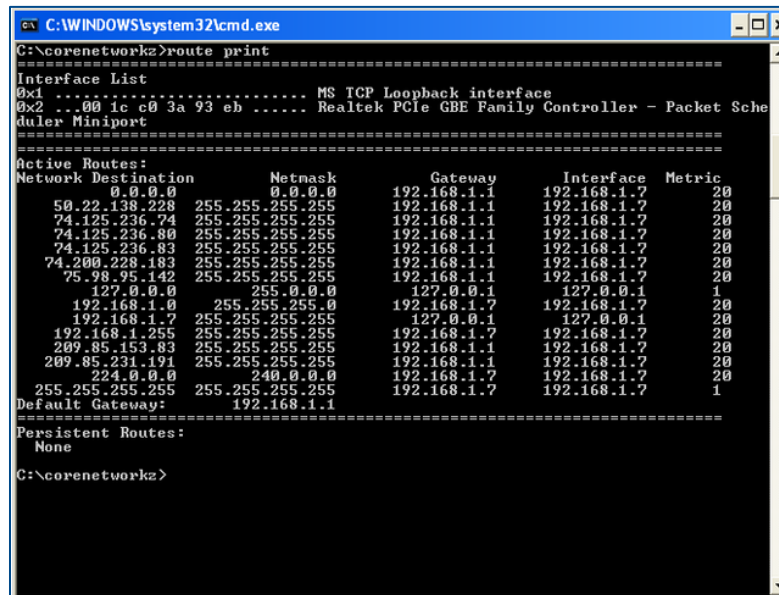
```
C:\>userdump.exe -p
User Mode Process Dumper (Version 8.0.2826.0)
Copyright (c) 1999-2005 Microsoft Corp. All rights reserved.
```

```
0 System Idle Process
4 System
624 SMSS.EXE
676 CSRSS.EXE
700 WINLOGON.EXE
744 SERVICES.EXE
756 LSASS.EXE
892 SUCHOST.EXE
968 SUCHOST.EXE
1308 SUCHOST.EXE
1484 SUCHOST.EXE
1572 SUCHOST.EXE
1736 SPOOLSV.EXE
224 DefWatch.exe
252 enstart.exe
328 NGCTW32.EXE
400 Rtvscan.exe
412 NUSUC32.EXE
512 SMAgent.exe
1088 vmware-authd.exe
1148 umnat.exe
1180 umnetdhcp.exe
2012 ALG.EXE
680 EXPLORER.EXE
1624 UPTray.exe
552 WZQKPKICK.EXE
1352 Snagit32.exe
1732 TSCHElp.exe
1284 TrueCrypt.exe
720 dllhost.exe
2740 QUP32.EXE
2428 WINWORD.EXE
3120 cmd.exe
2452 EnCase.exe
3384 iexplore.exe
1784 nc.exe
2868 cmd.exe
2544 iexplore.exe
3044 userdump.exe
```

```
C:\>
```

## Volatile Data Components

- **Scheduled jobs** – Scheduled jobs are tasks that have been entered into the Task Scheduler for completion/execution.
- **Cached NetBIOS name table** – This table maps the NetBIOS names of recently connected hosts to their IP addresses.
- **Internal routing tables** – These tables show the current routing information the system uses to route outgoing data.
- **Encrypted volumes or RAM drives** – These are volumes that appear as normal storage volumes to the user, but will be closed or locked if viewed offline.



```
C:\WINDOWS\system32\cmd.exe
C:\corenetworkz>route print

Interface List
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 1c c0 3a 93 eb ..... Realtek PCIe GBE Family Controller - Packet Scheduler Miniport
=====

Active Routes:
=====
Network Destination        Netmask          Gateway           Interface         Metric
-----
0.0.0.0                    0.0.0.0          192.168.1.1       192.168.1.7       20
50.22.138.228             255.255.255.255  192.168.1.1       192.168.1.7       20
74.125.236.74             255.255.255.255  192.168.1.1       192.168.1.7       20
74.125.236.80             255.255.255.255  192.168.1.1       192.168.1.7       20
74.125.236.83             255.255.255.255  192.168.1.1       192.168.1.7       20
74.200.228.183            255.255.255.255  192.168.1.1       192.168.1.7       20
75.98.95.142              255.255.255.255  192.168.1.1       192.168.1.7       20
127.0.0.0                 255.0.0.0        127.0.0.1         127.0.0.1         1
192.168.1.0               255.255.255.0    192.168.1.7       192.168.1.7       20
192.168.1.7               255.255.255.255  127.0.0.1         127.0.0.1         20
192.168.1.255             255.255.255.255  192.168.1.7       192.168.1.7       20
209.85.153.83             255.255.255.255  192.168.1.1       192.168.1.7       20
209.85.231.191           255.255.255.255  192.168.1.1       192.168.1.7       20
224.0.0.0                 240.0.0.0        192.168.1.7       192.168.1.7       20
255.255.255.255           255.255.255.255  192.168.1.7       192.168.1.7       1
Default Gateway:          192.168.1.1

Persistent Routes:
None

C:\corenetworkz>
```

## Requirements of Volatile Data Acquisition

While capturing volatile data from systems is a critical component of the incident management and response process, there are several considerations for which an investigator must plan. Among other requirements NIST urges that the collection of volatile data be:



- Performed with minimal invasiveness (NIST guidelines)
- Performed as early in the process as possible
- Preserved for further or future analysis
- Performed using a repeatable process to prevent inconsistencies

# Key Takeaways





## Key Takeaways

- Your network security will be breached...it is a reality of the world in which we operate and do business
- How quickly you identify the breach; stop the exfiltration of personal data, intellectual property or classified material; and remediate the threat makes all of the difference in risk, cost and exposure
- There are six essential phases to an incident response that you need to know, and prepare for, to successfully manage a cyber breach
- Preserve volatile data as quickly as possible, using best practices



# Questions?



# Thanks!

Richard Thompson  
richard.thompson@encase.com

