Digital Forensics: Tracking Cyber-Criminals and Hackers

“Know thy self, know thy enemy. A thousand battles, a thousand victories.” - Sun Tzu : “The Art of War”

We're at war?

- Corporate networks face attacks every day (malware, network intrusion attempts, unauthorized access to resources, social engineering, etc.)
- Outsiders are trying to get access in order to spy, commit fraud or disrupt operations
- Insiders may also spy, commit fraud, abuse privilege, misuse resources, seek to sabotage operations.
- Corporate technology teams have the task of protecting the organization's information assets from these all threats.
- Yes, we are at war.

The Corporate Perspective

Why track Cyber-Criminals and Hackers?

- If the source/origin of an attack is known, measures may be put in place to stop the attack.
- Need to know what the attackers have done so that risk can be managed and problems fixed.
- To hold persons accountable for their actions (criminal prosecution, civil litigation, internal disciplinary action)

How do you track Cyber-Criminals and Hackers?

- Gather information about the attacks and attackers
- Analyse the information and compile evidence
- Follow the evidence

Digital Forensics helps to fuel much of these investigations

Digital Forensics

- Digital Forensics is the scientific process of data acquisition, analysis and reporting which supports the investigation of computer technology related incidents.
- Data can come from different sources and devices, hence there are different branches of Digital Forensics – computer forensics, network forensics, mobile device forensics, database forensics etc.

Digital Forensic Process

- Acquire data – how this is done will depend on the kind of devices/systems being targeted and the kind of data being gathered. However it is key that the acquisition process does not alter the data being gathered or else evidence will be compromised. Once data is gathered chain of custody must be preserved.

Digital Forensics Process

- Analyze data – examine gathered data to identify evidence which sheds light the incident being investigated. Look for clues to help answer the what, when, where, why and who questions.

Digital Forensics Process

- Report Findings – The report on findings articulates what the investigation has found. This is key to support building a good case (for legal matters) as well as to facilitate learning and strengthening of the organizations defences.

Sources of Forensic Data in the corporate environment

- Usually the first and most important source of data for forensic investigation in the corporate environment are event log files.
- Event Logs capture details about events which have taken place.
- Event Logs are generated automatically by various systems, applications and devices (Operating Systems eg. Windows, Financial applications, Security systems, network devices).
- There are different types of Event logs which capture different kinds of information about events which have taken place (eg. error logs, audit logs, debug logs, authentication and access logs).
- Event logs are a very rich source of forensic data and can help tremendously in the understanding of what has happened and who did it.

Sources of Forensic Data in the Corporate environment

- Data stored on storage devices (hard disks, computer memory etc.)
- Compromised systems may have evidence of the compromise stored on that systems storage facilities (hard disks, SAN, NAS, memory etc.)
- There may be suspicious files or folders (eg. new executable programs), missing files or folders, data modified from expected norms (eg. changed configuration files) etc.

Sources of Forensic Data in the Corporate environment

- Network traffic and network traffic monitoring data
- The monitoring of network traffic allows for the potential of identifying and tracking network attacks and attackers in real time.
- Most corporate networks are TCP/IP networks. Network traffic flows like little letters in envelopes which must have source and destination addresses stamped on them.
- Monitoring network traffic can allow you to determine where attacks are coming from and potentially, who is attacking your network.

Actually catching the bad guy

- Scenario: Somebody has tried to hack your corporate Internet website.
- They have taken control of your server (you got Pwned) and have uploaded various programs to it with the intent to use that as a springboard to gain access to the rest of your network.
- Your security systems have detected the attack and have alerted you.
- You shut down all internet and internal network access to the compromised server to stop the attack and contain the activities of the attacker.
- You forensically image the storage device of your server to have forensically sound replica you can do analysis on for the purpose of evidence collection.
- You find evidence of the malicious programs uploaded document the evidence
- You review the servers event logs. Your server log files have captured the IP address from which the hacker has connected to your server from. You are able to block that IP address at your firewall and stop future attacks from that address. You are also able identify who that IP address is registered to by doing a Domain Registration query (Whois lookup).

Actually Catching the Bad Guys

- You contact law enforcement, make a report to them, and turn over the reports of your findings to them as well as your forensically acquired data (maintaining chain of custody).
- Law enforcement does their own investigation.
- Law enforcement makes contact with the registered owner of the IP address (in this case, it's an Internet Service Provider).
- Law enforcement works with the Internet service provider to identify which of their customers was issued that IP address during the time of the attack.
- The real identity and address of the customer who had that address is identified.
- Law enforcement gets the necessary clearance to monitor the internet activity of the suspect and works with the ISP to do this.

Actually Catching the Bad Guys

- The suspect is observed engaging in suspicious activity similar to the attack which triggered this investigation.
- Law enforcement raids the address of the suspect, arrests him, and confiscates all computer equipment on the premisis.
- Law enforcement conducts their own digital forensic examination of all the seized equipment and finds evidence of connection to the victim’s server at the time of the attack (web browser history), hacking tools, and copies of the same malicious programs which were uploaded to the victims web server in the attack.
- They have found the smoking gun!
- The suspect is charged, tried and found guilty, thanks largely to the forensic evidence collected by the victim and law enforcement.

The End

Yaaaay!

Enter Anti-Forensics : Because nothing in life is ever really that easy

“All warfare is based on deception” – Sun Tzu: “The Art of War”

Know thy enemy

- You cannot fight what you cannot see. If you don't know you've been attacked, you can't investigate. Elite hackers are stealthy.
- They have techniques for evading security systems such as intrusion detection systems
- They leave little evidence of their presence and they remove of whatever evidence does exist after they have done their work.
- They plant "evidence" to distract investigators. They have you looking over there  when they were really over 

Anti-forensics Tradecraft

- Use encryption to avoid scrutiny from network intrusion detection systems.
- Use obfuscation techniques and encryption to keep anti-malware programs from detecting your malicious code
- Use encryption to hide the existence of attack tools and other incriminating evidence on the attackers own computer systems so that there is little or no evidence available to prosecute them.
- Many security systems are signature based – they can only detect what they know about. Bad guys use polymorphism (shape shifting) to make their malicious programs look different every time they deploy it. Security systems won't recognize it and thus won't be able to detect it.
- Modify event log data. Erase all records of bad guy's activities on the system. Can you trust the event log data stored on a compromised system?
- Hide information (attack tools and programs, stolen data) in plain sight using techniques such as steganography (putting data in image files), alternate data streams – methods not detectable by "regular" detective methods.
- Replace regular system programs and functions with "evil" versions designed to hide the truth about the state of the system after the bad guy has compromised it – aka "The Root Kit"
- Anonymize network (Internet) connectivity. Make it so that the IP address the bad guy appears to be connecting from cannot ultimately lead to the revelation of his real identiy and location – (use proxy servers, TOR network, wardrive open WiFi hotspots, botnets and compromised end user computers).

So now what?

- Accept the fact that it is war, and there is an “arms race”.
- Know the enemy’s tactics and plan your defence with those tactics in mind.
- Implement defence in depth. Do not just rely on one method of defence or detection. Do not rely on just one source of data for investigation.
- Architect your environment to allow for reliable and convenient practice of sound digital forensic processes.

Examples?

- Protect log data. Implement centralized remote logging to secure log management platforms so that if a system is compromised, its log data is securely stored on another system which has not been compromised. Trust in the logs is thus preserved.
- Use Change detection systems to monitor files and resources on critical systems for unauthorized changes. Some of these systems can gather forensic data from the systems they protect and store them remotely on secure systems and thus aide in sound forensic investigation.
- Monitor networks in real time. Know your network. Understand what is normal behaviour so you can identify attacks based on anomalies.
- Pull it all together. Look into implementing Security Information and Event Management systems and processes to allow for correlation of the various sources of security and event data in your environment so that you can more readily detect security incidents, and investigate them.

The End

For real this time.

Thank you.