Southern New Hampshire University

ISE 640 Final Project Forensic Notes

Use the information in this document to help you complete your final project.

Drew Patrick, a director-level employee, is stealing intellectual property from a manufacturing company. The company is heavily involved in high-end development of widgets. Drew has access to corporate secrets and files. He is planning on leaving the company, taking the intellectual property with him, and going to work for a competitor. There is suspicion of him doing this, so human resources (HR) notified the information technology (IT) department to monitor Drew's past history. An internal investigation is launched due to Drew's abnormal behavior. The IT department confirms that they have found large files and emails. Forensics identified unauthorized access, transmission, and storage of intellectual property by Drew. Evidence found will be used to support legal civil and criminal proceedings.

Scenario

ACME Construction Company designs, manufactures, and sells large construction vehicles that can cost upwards of a million dollars. They spent hundreds of thousands of hours redesigning their premier excavator. Every piece that goes into the excavator is individually designed to maximize the longevity of the equipment. Known for attention to detail, high-quality work, and industry innovation, this painstaking work is what sets ACME Construction company apart and is attributed for the excellent reputation they enjoy. This, in turn, allows them to charge a premium on their exceptionally well-built products.

Drew Patrick is a senior manager directly involved with the overall development of ACME's excavators. His role provides him with access to design documentation, schematics, support documents, and any other technical references maintained in the company's research and development (R&D) database. The R&D database is maintained by ACME's information technology (IT) department, which is supported by a security operations center (SOC). The SOC uses Snort as a core component of their security information and event management (SIEM) system to keep tabs on network traffic, authentication requests, file access, and log file analysis.

The SIEM alerted SOC personnel of potential peer-to-peer (P2P) traffic originating from the internet protocol (IP) address associated with Drew's computer. However, analysis of Active Directory logs indicated that Drew was not logged into his account at the time the files were transferred via the P2P application. ACME enforces two-factor authentication and does not allow for computer sharing. The SOC personnel began an incident report based on the identification of P2P traffic, which violates company policy. As per company policy, the SOC personnel gave human resources (HR) and the legal team the incident report. The legal team asked for further investigation. Upon further inspection of the P2P activity, several file transfers were discovered. The files transferred match the names of files in the R&D database containing intellectual property developed by Drew's development team. Additionally, the files were transferred to IP addresses that are not owned or controlled by ACME Corporation.

Analysis of the server access logs indicated that Drew had been logging into the R&D database for several weeks prior to the external file transfers taking place. Network logs from the Intrusion Prevention Systems (IPSs) indicated that the files of interest had been transferred to Drew's desktop computer prior to the external transfer. ACME has a strict policy against maintaining intellectual property anywhere other than the designated servers. File access logs on the R&D servers confirmed that the account belonging to Drew had copied the files in question.

At this point, fearing a loss of intellectual property, in addition to numerous policy violations, ACME called in the digital forensic team to take over the investigation. The forensics team proceeded to capture the log files from relevant computer systems and created a forensically sound copy of the hard disk drive on Drew's computer. The log files investigated included the corporate mail, domain name server (DNS), and dynamic host configuration protocol (DHCP) servers, as well as physical access logs. Additionally, packet capture logs from the firewalls and intrusion detection system (IDS) were gathered and analyzed. This detailed investigation revealed that file transfers of intellectual property were indeed done from Drew's computer, however, Drew's account was not logged in at the time of the transfer. The only account active on the suspect computer was an anonymous account that had been created on 9/17/2016 at 9:57 p.m.

The following notes were provided by the Forensic Team:

Forensic Team Investigation Notes

Notes from the investigative team about the forensic findings of the hard drive image obtained from Drew Patrick's hard drive:

- Chain of custody document was begun with the sizing of the Western Digital Hard Drive 500 GB with serial number NB497356F from Drew Patrick's computer.
- Hard drive was duplicated using forensic toolkit (FTK) software to preserve the original hard drive image. A hash was created for the original and the copied image to prove both images were the same.
- The operating system of the image was Windows-based. The operating system used a new technology file system (NTFS) file structure.
- The hard drive was analyzed using Autopsy and Windows Forensic Toolchest. The sort and index functions were used to isolate the files needed for further analysis. These files include types SQL, Excel, email, chat, and HTML. Slack space was also analyzed.

Files and Findings

EMAIL (Microsoft Outlook): Numerous emails were found that contained references to proprietary information. Some emails were to non-ACME Corporation email accounts, and they promised information pertaining to equipment design. Follow-up emails were found that asked for assurance of a promised managerial position.

CHAT (AOL Instant Messenger): Several chat conversations were recovered containing information about possession of proprietary documents.

SQL (Microsoft Database): SQL database files revealed proprietary information and connection logs to a remote SQL server. Two additional SQL database files were encrypted and were not successfully unencrypted.

EXCEL (Microsoft Excel): Numerous Excel files were located on the hard drive. These files contained parts list and parts specifications concerning proprietary construction equipment. These files had csv and xls extensions.

HTML: Recovered internet web browser cache revealed that the dark web was searched for proprietary information brokers. An email address was created to correspond in the dark web for buyer transactions called constructionseller@darkweb.com. Internet cache also revealed that YouTube was searched for the subjects “selling intellectual property” and “selling on the dark web.” Recovered internet browser history revealed pictures and illustrations on encrypting SQL database files. Internet browser history also revealed searches concerning how to exploit the vulnerabilities of an SQL database.

SLACK SPACE (hidden data and temporary files): Hidden information in the slack space was revealed to contain temporary internet files on searches for “advertising stolen data” and “hacking sql servers.” These files, once revealed, were in plain text and read using Notepad.