Security Management

Keeping the IT Security Administrator Busy

Dr. Jane LeClair
Chief Operating Officer
National Cybersecurity Institute, Excelsior College

James L. Antonakos
SUNY Distinguished Teaching Professor
Computer Science, Broome Community College
NCI Fellow

Security Management Topics

- People, Process, and Technology
- Security Awareness Training
- Security Policies and Procedures
- Password Management
- CSIRT Development and Management
- Network Traffic Capture and Analysis
- Log File Analysis
- Risk Assessment
- Vulnerability Scanning and Mitigation

Security Management Topics

- Data Loss Prevention
- Penetration Testing
- Firewall Management
- Email Administration
- Authentication
- Endpoint Protection Administration
- PCI 3 DSS Compliance
- Remote Computer Security Assistance
- Implementation of the SANS 20 Critical Controls

People, Process, and Technology

- A well-developed security program addresses these three areas:
  - *People:* Employees must be security aware and properly trained. Some individuals may also require certifications as well.
  - *Process:* Proper policies and procedures must be established, along with appropriate controls and measurement metrics, especially for audit purposes.
  - *Technology:* Must be properly configured and monitored. Installation and maintenance must be performed according to established policies and procedures.
- You can not just concentrate on one area.

www.wysiwygventures.com

People, Process, and Technology

- Information security concerns maintaining the confidentiality, integrity, and availability of information and information systems.
- *Confidentiality:* Information is not improperly disclosed.
- *Integrity:* Information is not compromised (altered, deleted).
- *Availability:* Information is accessible when needed.

Security Awareness Training

- Threats do not just come from the outside, they come from the inside.
- Insider threats are even worse than outsider threats, as insiders already have at least two advantages:
  - They are already on the network
  - They have permission to be on the network
- An insider may be innocent and do something incorrectly that causes a problem.
- An insider may be malicious and deliberately do something that causes damage.
- Some protection is offered through security awareness training.

Security Awareness Training

- Security awareness training should be performed upon hiring and at regular intervals during the year.
- Training in the following areas is a good start:
  - Portable Media
  - Safe Wireless
  - Passwords
  - Social Engineering
  - Safe Use of Social Media
  - Safe Email / Web Browsing
  - Data Loss Prevention
  - Safe Desktop
  - File and Disk Encryption Technologies

www.niiconsulting.com

Security Policies and Procedures

- Security policies are put in place to protect the individual and the organization.
- Security policies and procedures must be published and presented to employees so they understand what is required, the correct way to perform specific activities, and the consequences of not doing things properly.
- Proper documentation of policies and procedures is also necessary for auditing purposes.
- Policies and procedures should also align closely with the organization's change management process.

Password Management

- One aspect of password management is having the users create complex passwords and change them on a regular basis.
- Another aspect is maintaining passwords on all servers and other networking equipment, such as managed switches and other appliances.
- User passwords are maintained in a centralized way, for example, residing on a domain controller.
- Server and other passwords may be maintained in a centralized or decentralized fashion,

each having advantages and disadvantages.

news.dice.com

CSIRT Development and Management

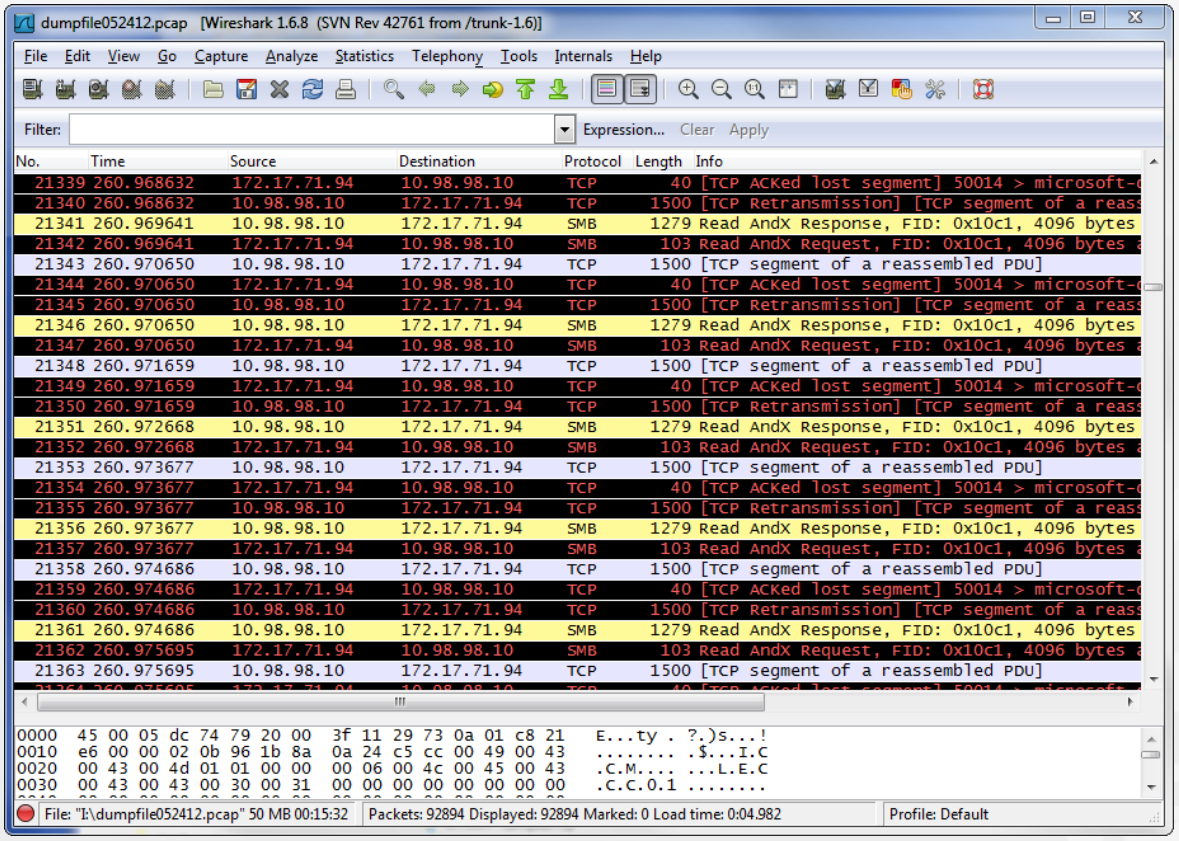
- A Computer Security Incident Response Team requires a great deal of effort to establish.
- Representatives from all areas of the organization make up the CSIRT, not just members of IT staff.
- The CSIRT must have the necessary authority to engage individuals and investigate systems.
- The CSIRT members should participate in multiple table-top scenarios, each covering a different type of security incident, in order to fine-tune their response flowchart.
- CSIRT incident reporting procedures must be announced to the entire organization.

CSIRT Development and Management

- Anonymous reporting may be necessary.
- Initial triage involves determining if a report involves a security event or a security incident:
  - Event: Informational (such as announcing a new patch release) or observation of suspicious activity (phishing email or phone call received).
  - Incident: System has been compromised or physical area has been breached.
- Incident response may involve law enforcement, public relations, insurance carrier, and legal representatives.
- Post-incident discussion required for CSIRT team to determine lessons learned and make necessary changes to help prevent similar incident in the future.

Network Traffic Capture and Analysis

- It is sometimes necessary to capture and analyze network traffic to determine the cause of an issue.



Provided by author

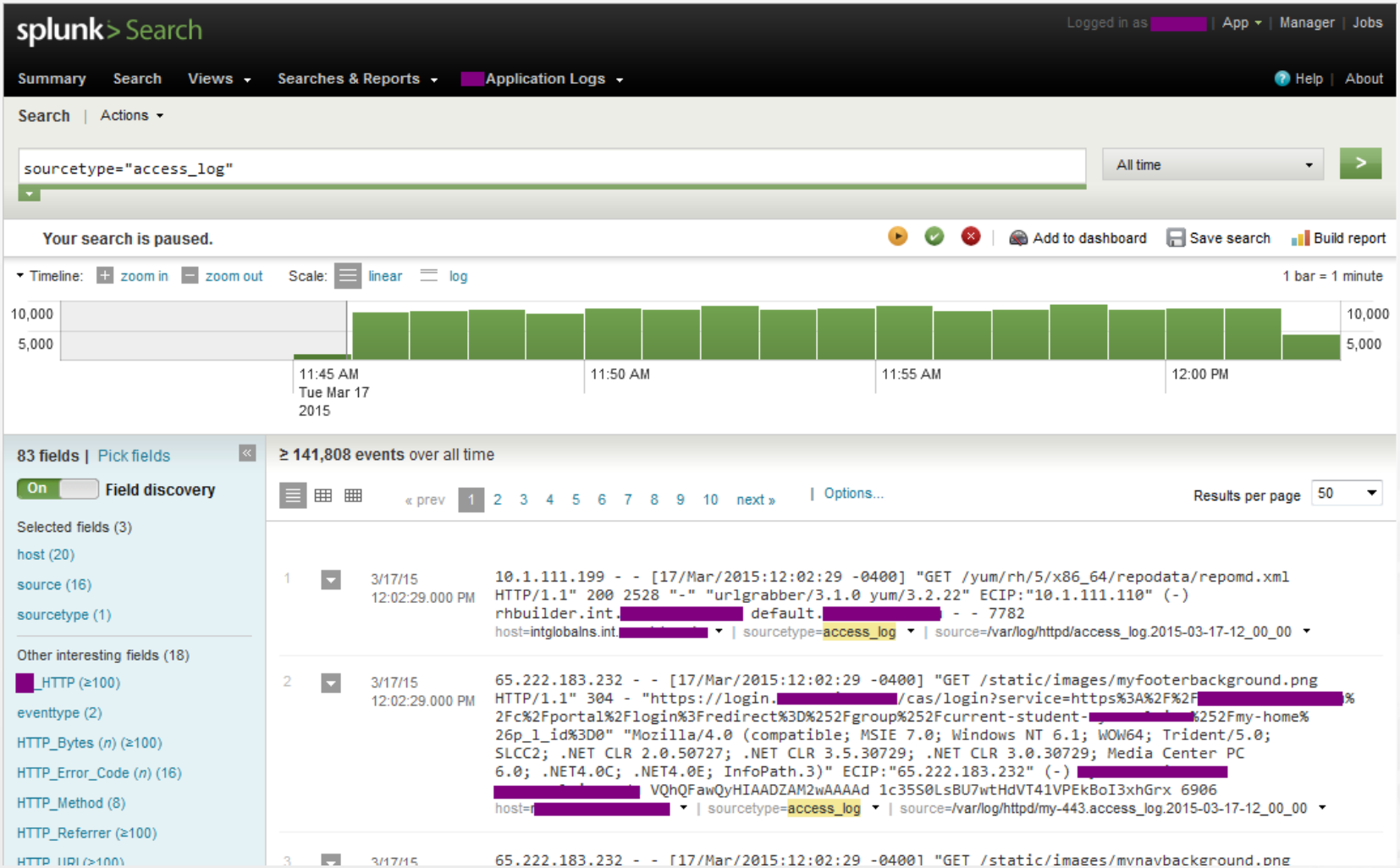
Network Traffic Capture and Analysis

- But how do you capture all network traffic on a switched LAN? There are at least two solutions:
- Utilize Span / Mirror port on switch
- Insert a hub onto the network segment
- Do you worry about interrupting traffic when inserting the hub? No.
- Why not?
  - It will not take very long to insert the hub.
  - If traffic is UDP based, who cares?
  - If traffic is TCP based, it will retry.
- Vendor may require a traffic capture for their troubleshooting.

Log File Analysis

- Sometimes the only way to determine if an attack has taken place is to examine the log files generated by the different servers and network components.
- If there are no log files, the organization is at risk and has reduced ability to respond to or investigate an attack.
- If there are log files, but no one is reviewing them, the organization is still at risk.
- There may be too many log files, or log files too large in size, to be reviewed in a timely manner by IT staff. This makes a third-party service very helpful.

Log File Analysis



Provided by author

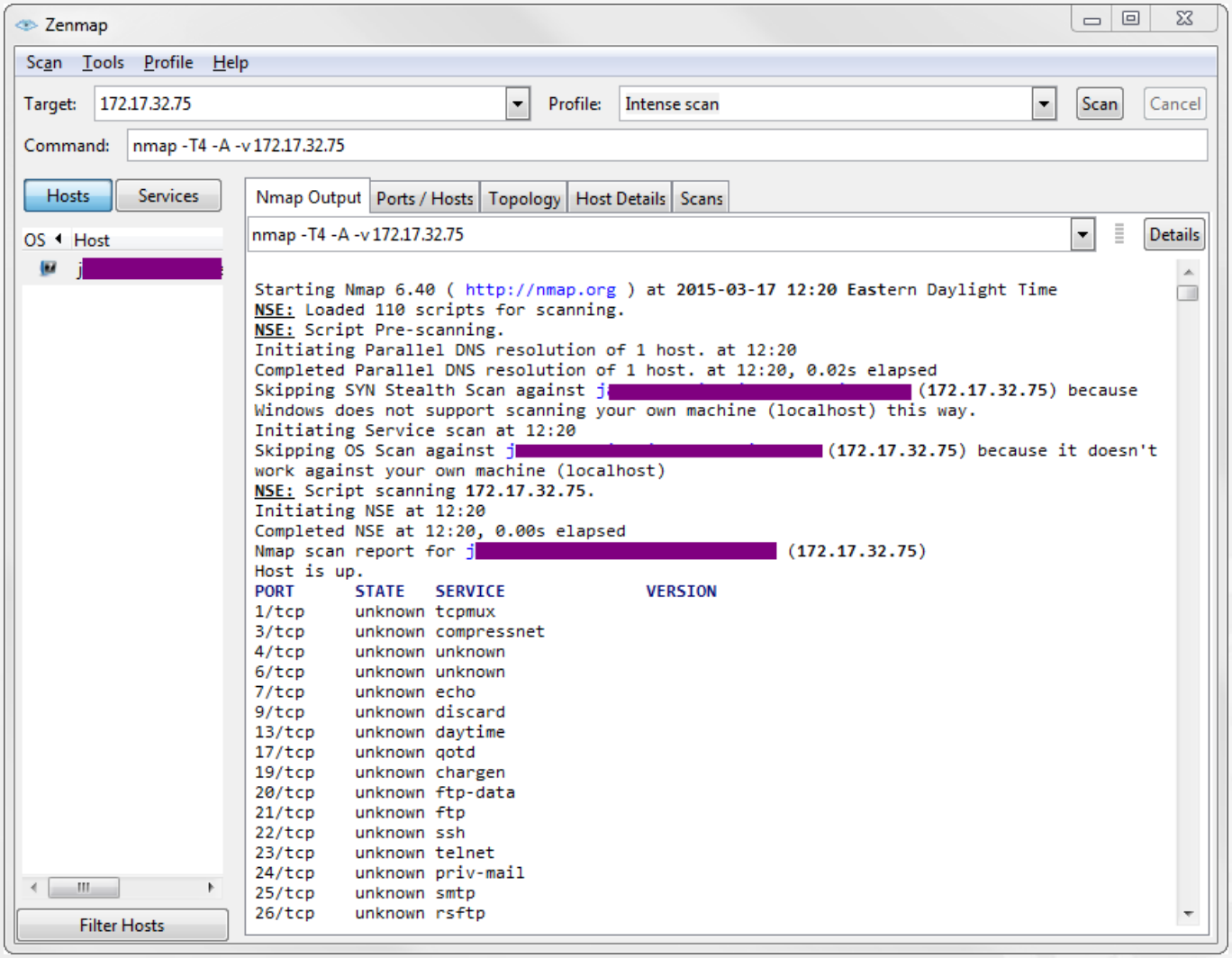
Risk Assessment

- An organization that has never undergone a risk assessment is, oddly enough, at risk.
- A risk assessment is used to identify organizational assets and the owners of each asset, determine the threats to the assets and the probabilities of the threats being successful, and the impact on the organization if an asset is compromised.
- High-priority assets should have their threats reduced or eliminated first.
- The organization leadership can choose to mitigate an identified threat, or to live with it, based on the costs involved (in both time and resources).

Vulnerability Scanning and Mitigation

- Regular vulnerability scans of all systems on the organizations network is an important way of detecting where security holes may exist.
- There are free tools to accomplish this scanning, such as NMAP.
- Mitigation requires time and effort from IT staff.
- It may be necessary to run a system without recent patches applied, due to software requirements or dependencies on other systems. In this case, the reason for keeping the system vulnerable should be documented.
- If you weaken security in one area, you must strengthen it in another.

Vulnerability Scanning and Mitigation



Provided by author

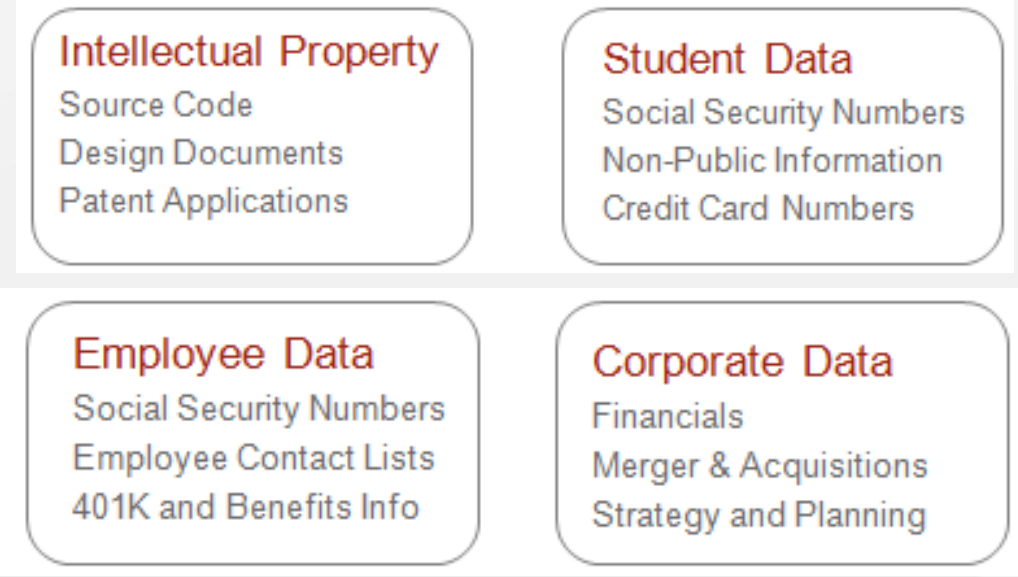
Data Loss Prevention

- Data loss prevention has to do with personally identifiable information leaving the organization improperly protected, or being improperly shared or revealed. Examples:
  - Social security numbers being sent in plain text via email.
  - Individuals discussing protected information and being overheard by others.
  - An employee improperly copying data files to a USB drive or laptop.
- Business Challenge: Confidential information needs to be protected while stored (Data At Rest) and exchanged (Data In Motion).

Data Loss Prevention

Secure Data from:

- Accidental loss or destruction
- Accidental dissemination
- Accidental access
- Unauthorized changes



Provided by author

Penetration Testing

- Penetration testing is one component of a security audit or risk assessment.
- Penetration testing is also a requirement for certain compliance standards, such as PCI, and must be performed at specific intervals during the year.
- There are two main types of penetration tests:
  - Black Box: The penetration tester is not given any information about the network, its systems, or the organization. Everything must be discovered.
  - White Box: The penetration tester is given some information to get started, such as a network diagram and possibly a user account with typical privileges.

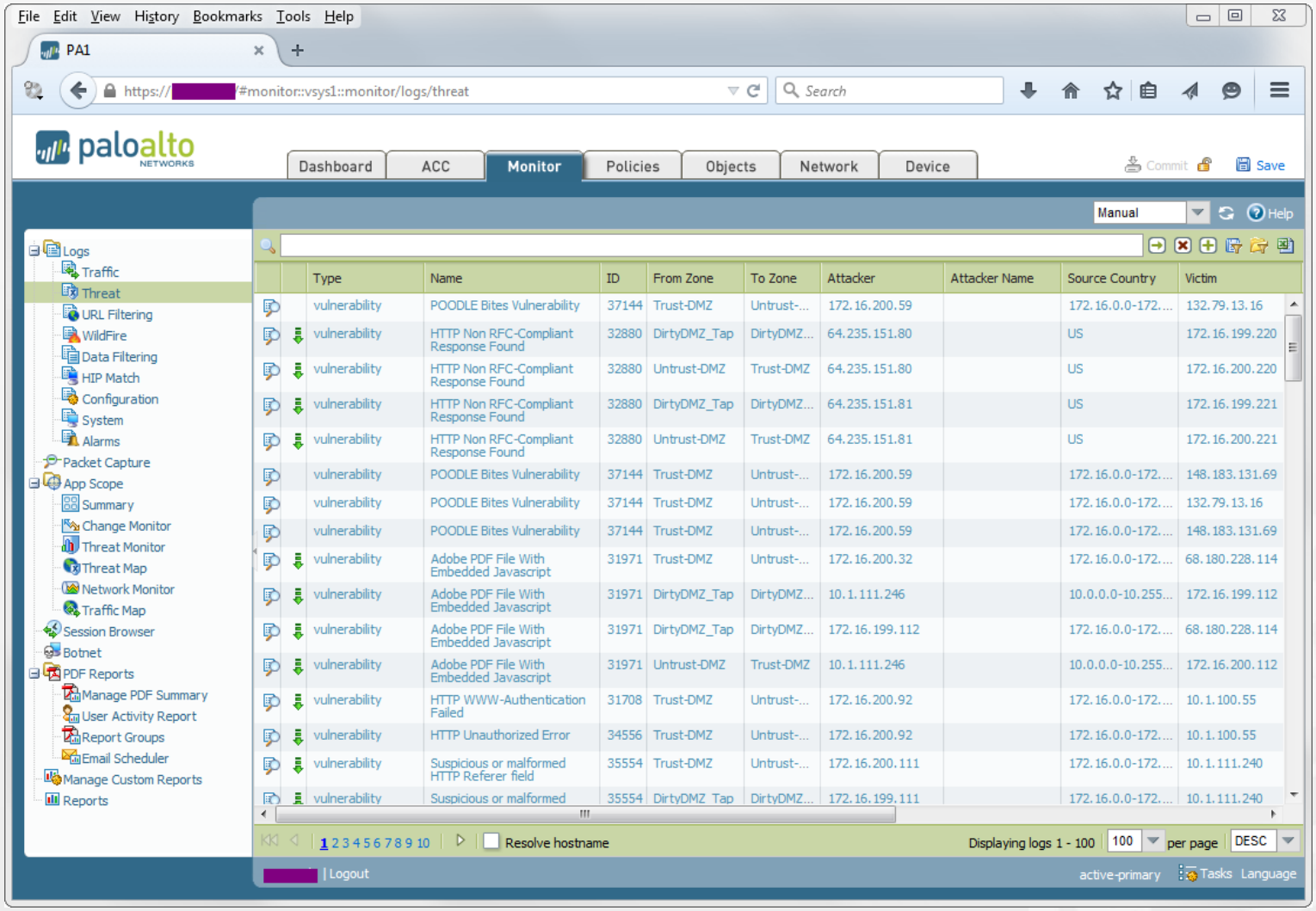
Penetration Testing

- A penetration testing is a snapshot in time of present vulnerabilities.
- These vulnerabilities must be addressed before the next penetration test.
- It may be wise to keep using the same vendor to perform successive penetration tests, as they will have the best knowledge of the organizations network and systems.
- If a penetration test does not reveal any vulnerabilities, that does not mean the organization is not vulnerable, as attacks change every day and new attacks (such as zero-day vulnerabilities) appear without warning.

Firewall Management

- Simply adding a firewall to a network does not automatically add protection.
- The firewall must have rules added to control the flow of traffic into and out-of the network.
- Once the rules have been added, the firewall must be monitored to determine its effectiveness and the rules modified accordingly.
- Firewall rules must be changed, added, or removed in alignment with the organizations change management process.
- Next-generation firewalls provide additional protection.

Firewall Management



Provided by author

Email Administration

- Email administration involves all of the following:
  - Creating email accounts for users
  - Suspending or deleting email accounts for users who have left the organization
  - Combating SPAM (blacklisting domains)
  - Responding to malware sent via attachments
  - Educating users on phishing and other email scams
  - Getting the organizations email domain un-blacklisted (which sometimes occurs when bulk emails are sent out)
  - Reviewing emails of “important” employees who have left the organization.

Authentication

- Recall that authentication is based on any of the following:
  - Something you know (username, password, PIN code)
  - Something you have (hardware token, smart card)
  - Something you are (facial recognition, iris pattern, hand geometry, fingerprint)
- Two-factor authentication uses any two of these three authentication areas.
- Authentication is not just for people...

one system may need to authenticate

with another system.

Provided by author

Endpoint Protection Administration

- Servers and user workstations are the endpoints in an organizations network.
- Protecting the endpoint requires some kind of anti-virus solution, no matter how secure the network is or how hardened the servers may be.
- In a small organization, individual AV software installations are easy to maintain.
- In a large organization, a centralized AV management system must be used, which pushes updates out to clients installed on each endpoint.

Endpoint Protection Administration

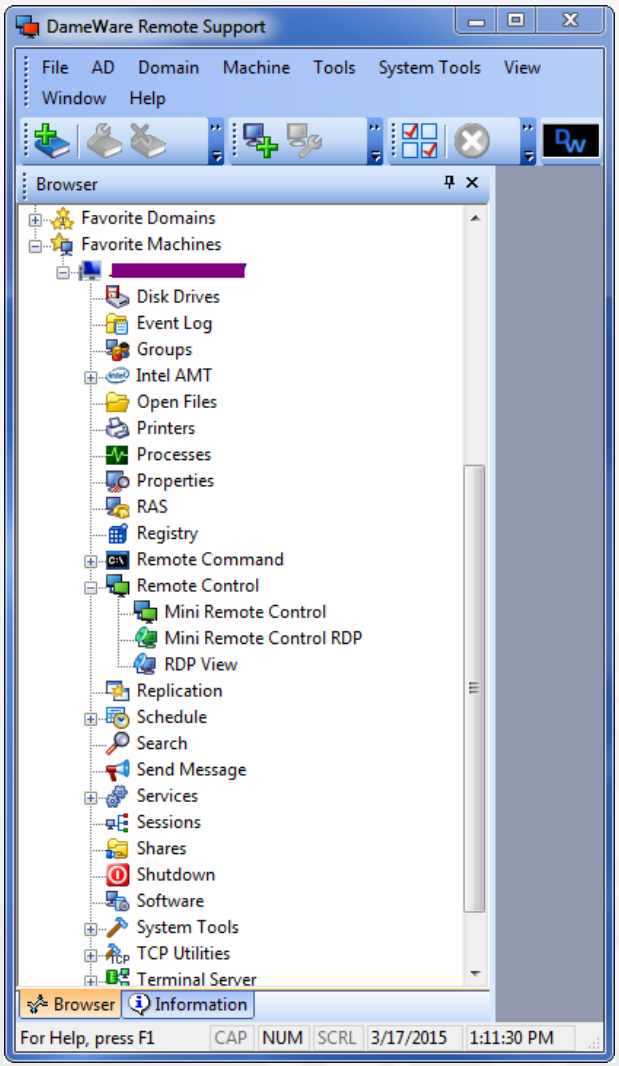
Provided by author

PCI 3 DSS Compliance

- Compliance with state and federal laws, as well as accepted standards, is an important aspect of security management.
- Being out of compliance could result in fines and the loss of ability to accept credit card transactions.
- The questionnaire for PCI 3 compliance contains over 300 items that must be addressed. This is not a job that can be handled by one person. An entire team of individuals is required.
- PCI compliance becomes much simpler if no cardholder data is stored on the organizations systems.

Remote Computer Security Assistance

- Whether users are onsite or offsite, being able to connect to their computer remotely is not only a time saver, but a good security practice, as it allows Help Desk staff or the IT security administrator to quickly diagnose a problem and address it, without leaving their computer.



Provided by author

Implementation of the SANS 20 Critical Controls

- The SANS 20 Critical Controls are a great starting point for an organization that does not have a security program in place, or for an organization that wants to strengthen its existing security program.
- A control is put in place to avoid, counteract, or minimize damage to organizational assets, people, and information.
- The more controls that can be automated, the better, as this provides more efficient situational awareness.
- A control is only effective if it is monitored and enforced.

Implementation of the SANS 20 Critical Controls

- A control that is inconvenient will be avoided or circumvented.

www.babble.com

www.crashgate.org

Implementation of the SANS 20 Critical Controls

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- Critical Control 5: Malware Defenses
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Implementation of the SANS 20 Critical Controls

- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

Conclusion

- Security management involves working in three areas: people, process, and technology.
- All three areas are important and dependent on each other.
- One main goal of a security management program is to help guarantee the confidentiality, integrity, and availability of information and information systems.
- *People:* Security awareness training continues to be a critical tool in educating users on how to protect information and information assets, and use their computers and the organization's network safely.

Conclusion

- *Process:* Establishing, publicizing, and monitoring security policies and procedures helps protect individuals and organizational assets.
- *Technology:* Just putting firewalls, IDS appliances, and security software in place does not automatically provide protection. Each piece of technology must be properly configured, and then monitored and fine-tuned as its performance is continuously evaluated.
- If security is weakened in one area, it must be strengthened in another.
- Being secure today does not guarantee being secure tomorrow. Everyday vigilance is required.