Auditing Network Architecture

Prepared and presented by: Tanya Baccam
CPA, CITP, CISSP, CISA, CISM, GPPA, GCIH, GSEC, OCP DBA
Baccam Consulting LLC
tanya@securityaudits.org

Agenda

- Understand the components when auditing network architecture
- Look at some of the key components in the network architecture

Network Diagrams

- Logical diagram
  - Systems and protocols being utilized
  - Flow of information
  - VLAN and logical network separation is identified
- Physical diagram
  - Identify what ports plug into which devices
  - Essential for identifying defensive strategies and protecting connections

APT Life Cycle

Can you figure and how a break occurred and the extent?

What are your targets?

Have you audited your controls?

Are your users the weakest link?

Can you see what's happening on your network?

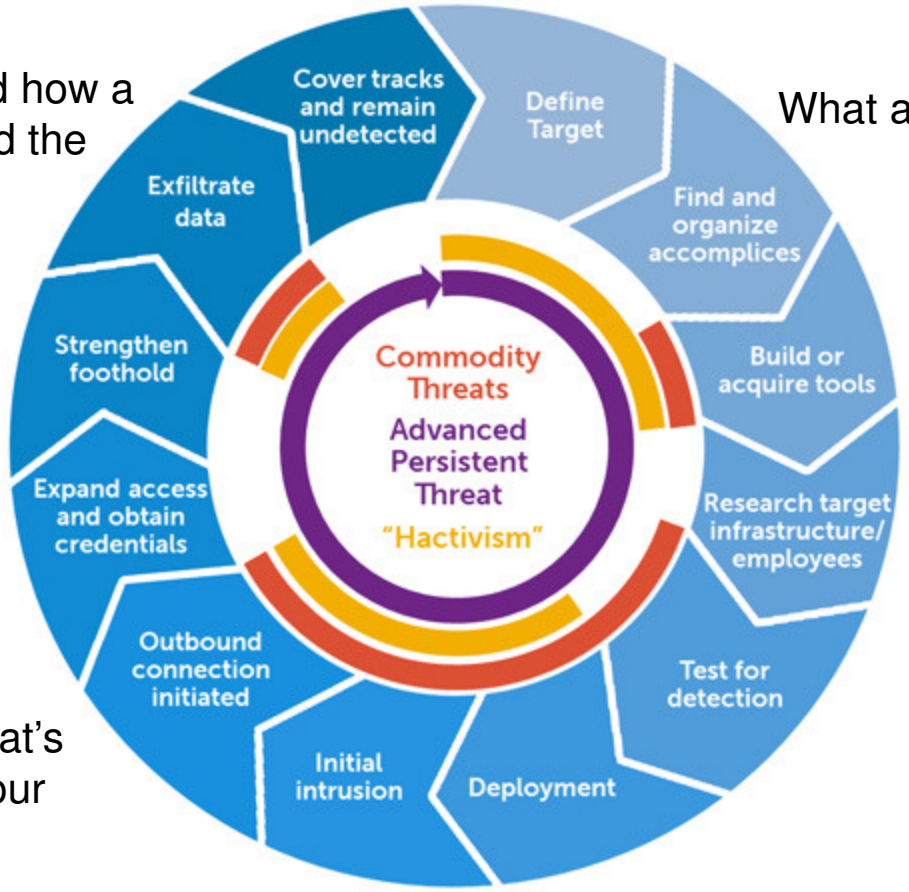


Diagram Source:
https://en.wikipedia.org/wiki/Advanced_persistent_threat

Layered Security Throughout the Environment

Malware

Known threats with signatures

Anti-virus

Unlicensed Software

Zero Day Threats

Mutating Threats

Application Whitelisting

Unauthorized system changes

Auditing/Logging

Preventive and Detective Solutions are necessary

Segmentation and Isolation

- Helps to contain breeches
- You are adding perimeters through the network
- Create security zones

Defense-in-Depth

- Always remember DID!
  - All audits must consider the “Big Picture”
- Many components make up a network’s defenses
  - Perimeter routers
  - Perimeter firewalls
  - Internal routers
  - Internal firewalls
  - Network-based IDS/IPS
  - Host-based IDS/IPS
  - NAC
  - Application Whitelisting
  - Policies and procedures
  - Advanced Malware Protection

Firewall Rulebase Principles

- A "default deny" policy should exist
  - The last rule should be deny everything, and should log any traffic that is processed by the rule
- Rules should be specific
  - Rule should not allow access from any source or from a source network address
  - Rules should not allow access to any destination or to a destination network address
  - Rules should not allow access to any destination port or a large range of destination ports
- Rules should not overlap or duplicate each other
- Rules should not contradict other rule
- Rules should be utilized
  - Disabled or unused rules should not exist as they make the rulebase more complicated
- Services should be secured
  - No clear text protocols should be allowed
  - Dangerous services should not be allowed
- Logging should occur for all rules
- All rules should have a business justification

Next Generation Firewalls

- Goes beyond basic filtering
  - Basic filtering is the typical Protocol, source IP, destination IP, source port/process, destination port/process
- Filter at the application layer
  - Beyond packet inspection to application control
- As security “features” are enabled, throughput drops
  - Ex. Integrated IPS, External intelligence sources, decryption and protocol decoders, etc.
- Not all NGFWs are the same!

NextGen Filtering Examples

- Source
  - Ex. Device type, authentication type or Active Directory user
- Destination
  - FQDNs
- Application filtering, not just service filtering
- Action may be encrypt/decrypt, DLP, filter, etc.

Next Generation Capabilities

- Make decisions based on applications, not ports
  - Application signatures
- Identify users, not IP addresses
  - Login and user activity monitoring, etc.
- Inspect payload and content, not just headers
  - Malware
  - Attack traffic
  - URL filtering
  - Blocking certain file types

IDS/IPS Detection

- Signature-based Detection: patterns that correspond to a known threat
- Anomaly-based Detection: comparing definitions of what activity is considered normal against observed events to identify significant deviations
- Stateful Protocol Analysis: comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations

Host-Based

- Advantages
  - Verify success or failure of an attack
  - Monitor specific system activities
  - Detect attacks that are not identified by network-based systems
    - Ex. From a keyboard
  - Well-suited for encrypted and switched environments
  - Near real-time detection and response
  - Do not require additional hardware
  - Lower cost

- Disadvantages
  - Capabilities are compromised as soon as the host machine is compromised
  - Additional overhead to the OS
  - Must exist on each individual system
  - Application-specific
  - Can not monitor attacks that target multiple hosts
  - Often have difficulty detecting and operating during denial-of-service attacks
  - Parasitic software

Network-Based

- Advantages
  - Stealthy
  - No effect on existing systems or infrastructure when deployed
  - OS independent
  - Capabilities are not compromised when a host is compromised
  - No additional overhead to the OS
  - Can monitor multiple systems
- Disadvantages
  - Not very scalable
  - Based on predefined attack signatures
  - Can not monitor "on host" activity
  - Can not monitor encrypted traffic easily or without taking up significant resources
  - Additional hardware required
  - Higher cost

Checklist for IDS/IPS

- Are zones created and identify with appropriate controls?
- Does architectural placement make sense?
- How is traffic being captured – hub, switch, etc.?
- Technical Validation
  - Verify port scan detection
    - Multiple speeds
  - Verify payload detection
  - Verify fragmentation identification
- Are signatures up to date? How often do updates occur?
- Is the notification or alerting system used?
- Are logs being reviewed? Centralized?
- What traffic is/is not being monitored? Encrypted traffic? “Blind” network segments?
- Is NTP configured?
- Where is the management interface accessible from?

What is HIPS?

- Host is responsible for protecting itself
  - Addresses switching & encryption issues
  - Potential for lower false positives
- Can protect exposed services
  - Unexpected data formats
  - Zero-day and APT
    - Learning mode makes this easier
    - Should be a smaller curve than NIPS
    - More accurate info to work with

HIPS Deployment

- Any server with Internet facing services
- High asset/critical resources
- Users with a high level of network access
- Potentially useful on any system with Internet access

Does HIPS Fix Everything?

- Good for securing exposed applications
- May not be able to generate a whitelist for every application in all cases
- Sometimes it's sufficient to simply identify if an application should be permitted to execute
  - App does not interface with the network
- Application control or application whitelisting can be extremely useful when looking at applications

Application Control

- Control of software running on an end system
- Whitelisting of applications
- Permits enforcement of “acceptable use” policy regarding software
- A good system can also augment
  - License monitoring
  - Track source of individual files
  - Tracing back rogue software
  - Assist in troubleshooting

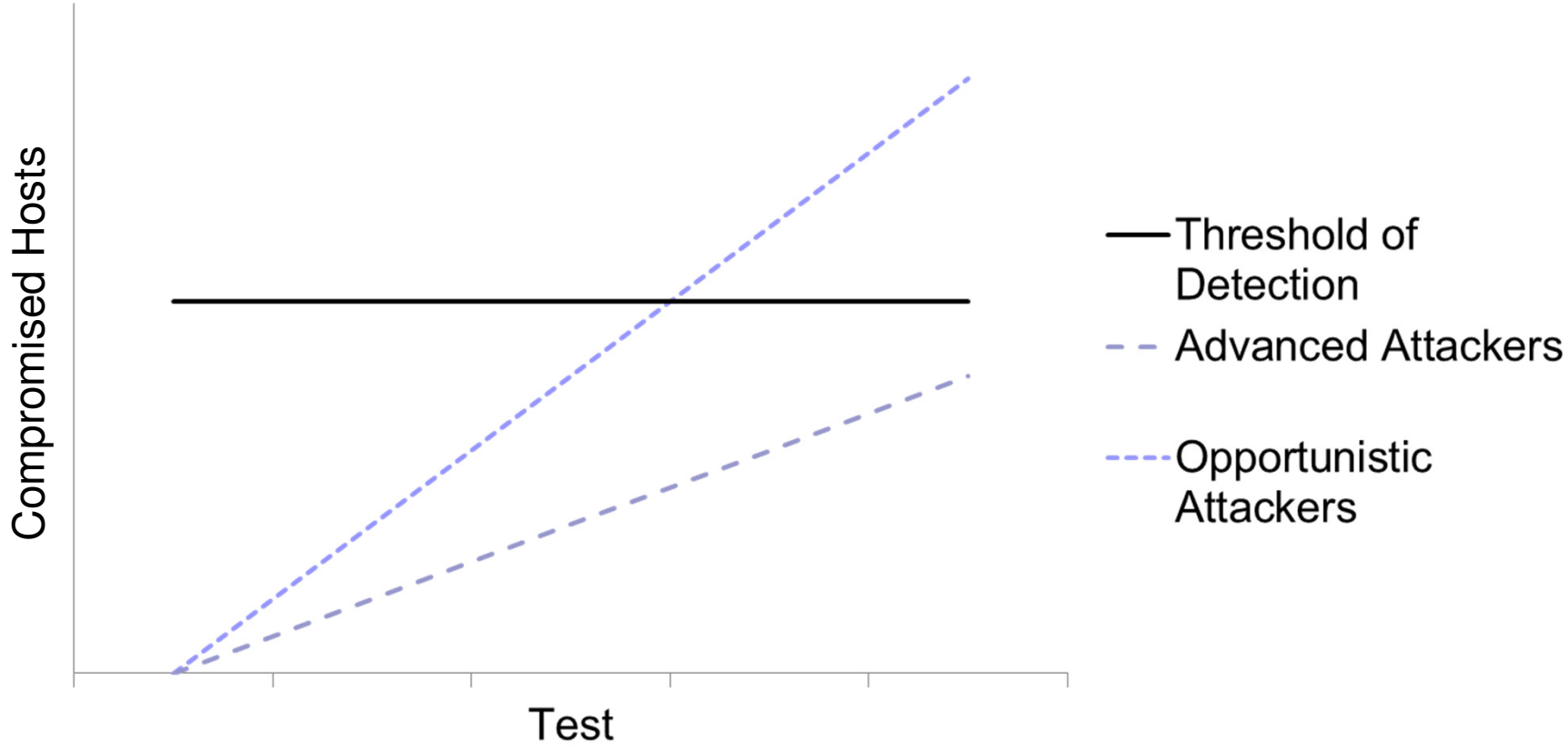
Application Control Provides

- Blocking the infection of malware
  - AV only finds malware we know about
- Enforcing acceptable use policy
  - No more blocking at the border
- Maintain the system in a corporate approved state
- Same concept as “default allow” versus “default deny” for firewalls

Whitelisting Deployment

- Mobile users
- Desktops with Internet access
- “Problem” users
- Publicly accessible systems
- When data integrity needs to be maintained
- File database is the “backbone”

Attackers Have Changed



Endpoint Threat Protection & Response

- Detection
  - Monitor in real-time
  - Conduct behavior analysis
  - Predict attacks without signatures
  - Identify abnormal activity
  - Integrate threat intelligence – learn from others
- Response
  - Record activity on endpoints
  - Contain threats
  - Investigate threats
  - Remediate and adjust based on results

Detection versus Discovery

- Attacks are often detected
  - They are a in log *somewhere*!
- Discovery is often missed
  - Out of the millions of log entries I have, how do I find the one that's a problem?

Evaluating Endpoint Threat Detection and Response

- User impact
- Continuous monitoring
- Centralized storage
- Threat intelligence
- Prevent untrusted software
- Integrate with other security devices
- Facilitate a quick response
- Platforms covered

Data Loss Prevention (DLP)

- Prevent the leakage of sensitive information
  - Credit card information
  - Medical records
  - Social security numbers
  - Some customizable options
- Wikileaks document releases has really brought attention to this industry
- Being adopted by many regulatory standards

DLP Deficiencies

- Regular expressions are simple pattern matching
  - Change the pattern and the data goes undetected
    - Simple encryption
    - Stenography
- Working with RegX is a steep learning curve
- Network based rarely checks all ports
- Host based requires (yet another) agent
  - Can cause noticeable degradation in performance

Advanced Malware Protection

- Understand the Problem
- Look at the adversary
- Look at Advanced Malware Protection
- Sandboxing
- Overview of solutions including Cuckoo and FireEye

Methods of Evaluation

- IP address blacklisting
- File activity
  - Type, protocol and direction of file transfers
- Further, more in depth evaluation
  - Sandboxing
  - Lookups in the cloud

Summary

- Discussed the components when auditing network architecture
- Reviewed some of the key components in the network architecture

Courses Available

- SANS Sec502: Perimeter Protection In-Depth
  - June 15-June 20, 2015
  - http://www.sans.org/event/sansfire-2015/course/perimeter-protection-in-depth
- Auditing Network Security in Dallas, TX
  - April 27-29, 2015
- Auditing Active Directory and Windows in Dallas, TX
  - May 18-20, 2015
- Foundations of IT Auditing in Dallas, TX
  - June 23-25, 2015
- Auditing UNIX/Linux in Dallas, TX
  - July 9-10, 2015
- Auditing Oracle in Dallas, TX
  - September 21-23, 2015
- Auditing Web Applications

- See www.securityaudits.org/events.html for more information and to register

Thank you!

Prepared and presented by: Tanya Baccam
CPA, CITP, CISSP, CISA, CISM, GPPA, GCIH, GSEC, OCP DBA
Baccam Consulting LLC
tanya@securityaudits.org