Back to the Basics

Dr. Eric Cole

Current Threat Level: RED
2Q 2014

- Current Risks:
  - Data Theft
  - Long term compromise
  - Command and control capability
  - Competitive advantage
- Current Threats:
  - Trusted Insiders
  - Supply Chain
- Current Vulnerabilities
  - Lack of segmentation
  - No data discovery
  - Systems not properly hardened

Myths About Attacks

- They only target governments
- Small organizations are not a target
- Destruction is the main goal
- The focus is on stealing information only
- Attackers want to take a piece of information and leave

Why Attacks are Successful?

- Organizations do not have security devices properly configured
- Not understanding the difference between a product and a solution
- Lack of data classification
- Not sufficient logging and correlation
- Too much visibility on the internal network
- Minimal asset management and configuration control
- Failure to institute least privilege

Prevention is Ideal

But

Detection is a Must

WHY?

PREVENT – DETECT – RESPONSE

Core to Success:

- Asset Inventory
- Configuration Management
- Change Control
- Segmentation

5 Steps to a Secure Future

Step 1: Identify Critical Data

Align critical assets with threats and vulnerabilities to focus on risk

Assets	Threats	Vulnerabilities

Risk Based Thinking

1) What is the risk?
2) Is it the highest priority risk?
3) Is it the most cost effective way of reducing the risk?

Step 2: Align the Defense with the Offense

1) Reconnaissance
2) Scanning
3) Exploitation
4) Creating backdoors
5) Covering tracks

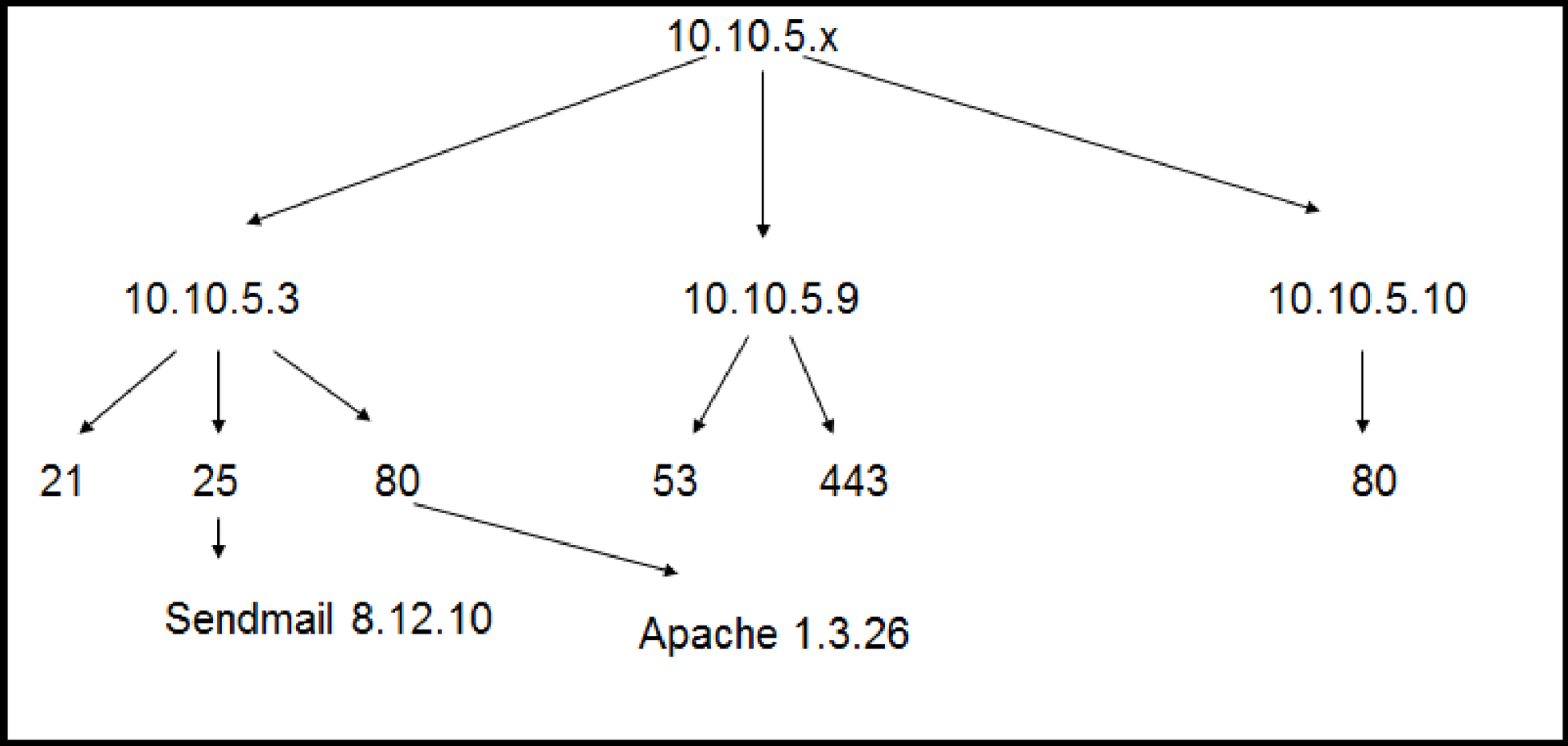
Step 3: Know thy Organization

If the offense knows more than the defense you will lose

Requirements:

a) Accurate up to date network diagram
b) Network visibility map
c) Configuration management and change control

You Cannot Protect What You Do Not Know About



Data Flow is Critical

Step 4: Defense in Depth

There is no such thing as an unstoppable adversary

Requirements:

a) Inbound prevention
b) Outbound Detection
c) Log correlation
d) Anomaly detection

Step 5: Common Metrics

Everyone must be using the same playbook in order to win

Requirements:

a) Utilize the critical controls
   i. Offense informing the defense
   ii. Automation and continuous monitoring of security
   iii. Metrics to drive measurement and compliance

www.sans.org/critical-security-controls/

Critical Control		Effect on Attack Mitigation
1.	Inventory of Authorized and Unauthorized Devices	Very High
2.	Inventory of Authorized and Unauthorized Software	Very High
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4.	Continuous Vulnerability Assessment and Remediation	Very High
5.	Malware Defenses	High
6.	Application Software Security	High
7.	Wireless Device Control	High
8.	Data Recovery Capability	Moderately High to High
9.	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11.	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12.	Controlled Use of Administrative Privileges	Moderate to Moderately High
13.	Boundary Defense	Moderate
14.	Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15.	Controlled Access Based on the Need to Know	Moderate
16.	Account Monitoring and Control	Moderate
17.	Data Loss Prevention	Moderately Low to Moderate
18.	Incident Response Capability	Moderately Low to Moderate
19.	Secure Network Engineering	Low
20.	Penetration Tests and Red Team Exercises	Low

VERY HIGH — These controls address operational conditions that are actively targeted and exploited by all threats.

HIGH — These controls address known initial entry points for targeted attacks.

MODERATE — These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.

LOW — These controls are about optimizing, validating, and/or effectively managing controls.

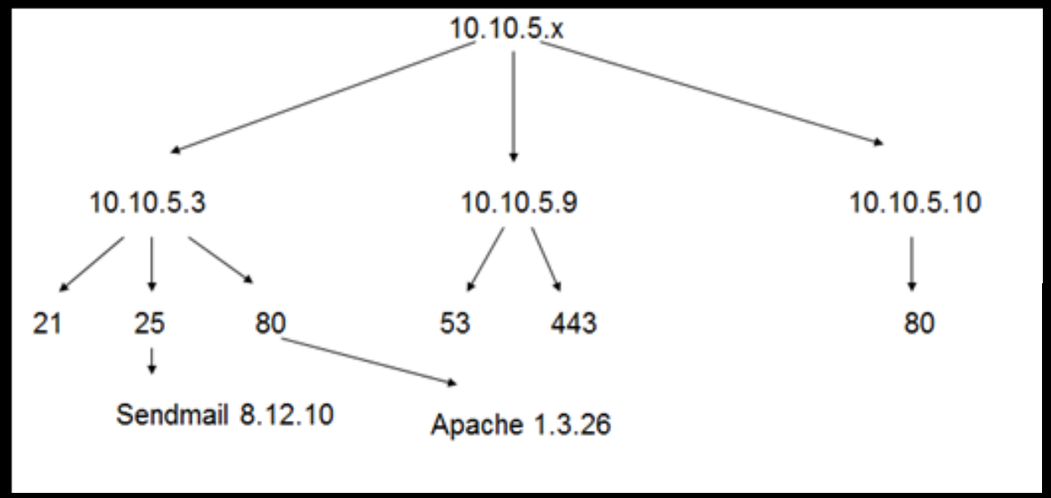
*Figure 1: The 20 Critical Security Controls (Version 3.1) and Their Effect on Attack Mitigation (Adapted from **www.sans.org/critical-security-controls/winter-2012-poster.pdf**.)*

Bottom Line….

It is time to take control of your data

Let’s stop making an easy target for the adversary

Winning at Cyber Defense



1) What is the risk?
2) Is it the highest priority risk?
3) Is it the most cost effective way of reducing the risk?

Assets	Threats	Vulnerabilities

Critical Control		Effect on Attack Mitigation
1.	Inventory of Authorized and Unauthorized Devices	Very High
2.	Inventory of Authorized and Unauthorized Software	Very High
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4.	Continuous Vulnerability Assessment and Remediation	Very High
5.	Malware Defenses	High
6.	Application Software Security	High
7.	Wireless Device Control	High
8.	Data Recovery Capability	Moderately High to High
9.	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11.	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12.	Controlled Use of Administrative Privileges	Moderate to Moderately High
13.	Boundary Defense	Moderate
14.	Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15.	Controlled Access Based on the Need to Know	Moderate
16.	Account Monitoring and Control	Moderate
17.	Data Loss Prevention	Moderately Low to Moderate
18.	Incident Response Capability	Moderately Low to Moderate
19.	Secure Network Engineering	Low
20.	Penetration Tests and Red Team Exercises	Low

VERY HIGH These controls address operational conditions that are actively targeted and exploited by all threats.

HIGH These controls address known initial entry points for targeted attacks.

MODERATE These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact.

LOW These controls are about optimizing, validating, and/or effectively managing controls.

*Figure 1: The 20 Critical Security Controls (Version 3.1) and Their Effect on Attack Mitigation (Adapted from **www.sans.org/critical-security-controls/winter-2012-poster.pdf**.)*

THANK YOU for your time

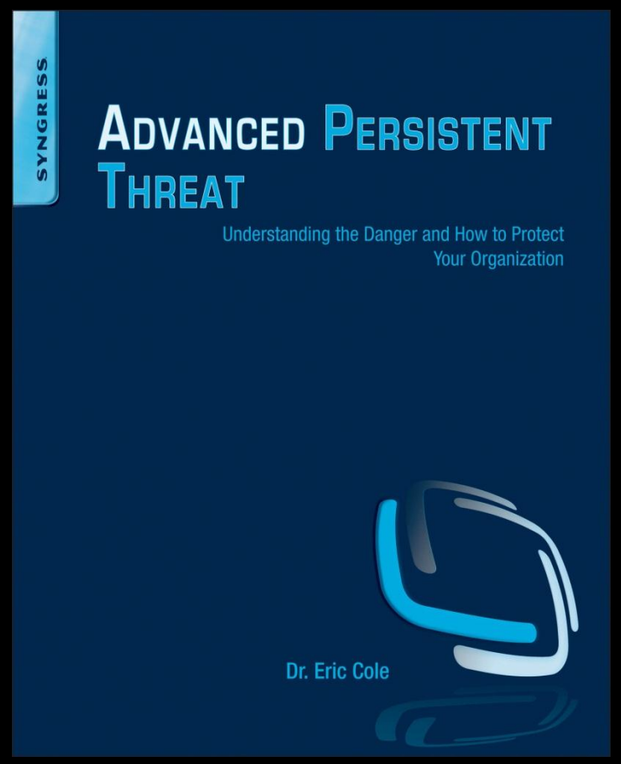
Dr. Eric Cole

Twitter: drericcole

ecole@secureanchor.com

eric@sans.org

www.securityhaven.com



SANS CYBER DEFENSE

SECURE ANCHOR