Consensus Audit Guidelines

Edgart Katarahweire(CCNA,CISA,CISM)
AH Consulting
kedgart@ahcul.com

Outline

- What is this?
- Why discuss this?
- The controls, rationale and vetted tools

- Consensus Audit Guidelines?

Consensus Audit Guidelines sounds pretty boring, let's think about it as something cool like "Cyber-Defense Initiative" or "Saving the Internet from organized crime."

What it is

- These Top 20 Controls were agreed upon by a powerful consortium brought together by John Gilligan (previously CIO of the US Department of Energy and the US Air Force) under the auspices of the Center for Strategic and International Studies.
- Members of the Consortium include NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.

Guiding Principles

- Defenses should focus on addressing the **most common and damaging attack** activities occurring today, and those anticipated in the near future.
- Enterprise environments must ensure **consistent controls across** an enterprise to effectively negate attacks.
- Defenses should be **automated where possible**, and **periodically or continuously measured using automated measurement** techniques where feasible.
- To address current attacks occurring on a frequent basis against numerous organizations, a **variety of specific technical activities should be undertaken to produce a more consistent defense.**

Why use them?

- The automation of these Top 20 Controls will radically lower the cost of security while improving its effectiveness. The US State Department, under CISO John Streufert, has already demonstrated more than 80% reduction in "measured" security risk through the rigorous automation and measurement of the Top 20 Controls.

Why…

- We have high regard for NIST's work. However, the problem for organizations trying to follow NIST's guidelines amid today's increasing cyber threats is akin to confronting a raging new pandemic with an encyclopedic field guide to holistic health care.

-John Gilligan

Team Lead

Why….

- We are at war.
- http://www.cadre.au.af.mil/main.htm
- **Cyberspace Operations-** AFDD 3-12 is the Air Force's foundational doctrine publication for Air Force operations in, through, and from the cyberspace domain. It defines Cyberspace Superiority and speaks to Air Force support of maintaining Cyberspace Superiority, a common military function
- We are fighting organized crime.

Relationship to NIST

- "The National Institute of Standards and Technology (NIST) has produced excellent security guidelines that provide a very comprehensive set of security controls in **NIST Special Publication 800-53, revision 3**. This document by contrast seeks to identify a subset of security control activities that CISOs, CIOs and IGs can focus on as their top, shared priority for cyber security based on attacks occurring today and those anticipated in the near future. As noted above, the 20 Critical Controls only address principally technical control areas. However, the controls do map directly to about one third of the **145 controls identified in NIST Special Publication 800-53.** In fact the mapping shows that the **20 Critical Controls are a proper subset of the Priority 1 items in 800-53."**

Guidelines Version 2.3

- 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 Laptops, Workstations, and Servers
- Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Guidelines

- Critical Control 5: Boundary Defense
- Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 7: Application Software Security
- Critical Control 8: Controlled Use of Administrative Privileges
- Critical Control 9: Controlled Access Based on Need to Know

Guidelines

- Critical Control 10: Continuous Vulnerability Assessment and Remediation
- Critical Control 11: Account Monitoring and Control
- Critical Control 12: Malware Defenses
- Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 14: Wireless Device Control
- Critical Control 15: Data Loss Prevention

Guidelines

- Critical Control 16: Secure Network Engineering
- Critical Control 17: Penetration Tests and Red Team Exercises
- Critical Control 18: Incident Response Capability
- Critical Control 19: Data Recovery Capability
- Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Rationale - Many criminal groups and nation states deploy systems that continuously scan :

- Address spaces of target organizations waiting for new, unprotected systems to be attached to the network.
- Experimental or test systems that are briefly connected to the network but not included in the standard asset inventory of an organization.

Critical Control 1: Inventory of Authorized and Unauthorized Devices Tools

- BSA Visibility (Insightix)
- IPSonar (Lumeta)
- CCM Primary, IP360 Secondary (nCircle)
- SecureFusion (Symantec)
- CounterAct (ForeScout Technologies)
- **Nessus & SecurityCenter (Tenable)**

How can this control be implemented, automated, and its effectiveness measured?

- Automated asset inventory discovery tool and build a preliminary asset inventory of systems connected to the enterprise network.
- Maintain an asset inventory of all systems connected to the network and the network devices themselves
- Ensure that network inventory monitoring tools are operational and continuously monitoring
- Secure the asset inventory database and related systems, ensuring that they are included in periodic vulnerability scans and that asset information is encrypted.
- To evaluate the effectiveness of automated asset inventory tools, periodically attach several hardened computer systems not already included in asset inventories to the network and measure the delay before each device connection is disabled or the installers confronted.
- Asset inventory should include removable media devices, including USB tokens, external hard drives, and other related information storage devices.

Critical Control 2: Inventory of Authorized and Unauthorized Software

Computer attackers deploy systems that continuously scan address spaces of target organizations looking for:

- vulnerable versions of software that can be remotely exploited. Some attackers also
- Distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites.

Without the ability to inventory and control which programs are installed and allowed to run on their machines, enterprises make their systems more vulnerable.

Critical Control 2: Inventory of Authorized and Unauthorized Software
Tools

- Parity (Bit9)
- CCM Primary & IP360 Secondary (nCircle)
- Nessus & SecurityCenter (Tenable)
- CounterAct (ForeScout Technologies)

How can this control be implemented, automated, and its effectiveness measured?

- Devise a list of authorized software
- Deploy software inventory tools
- Evaluate the effectiveness of automated software inventory tools.
- Deploy software white-listing technology that allows systems to run only approved applications and prevents execution of all other software on the system.

Critical Control 3 - Secure Configurations for Hardware and Software on Laptops, Workstations, and servers

- On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way it was delivered.

Critical Control 3 - Secure Configurations for Hardware and Software on Laptops, Workstations, and servers - Tools

- CCM (FDCC) Primary & IP360
- Retina & Blink (eEye Digital Security)
- SecureFusion (Symantec)
- Nessus & SecurityCenter (Tenable)

How can this control be implemented, automated, and its effectiveness measured?

- System images must have documented security settings that are tested before deployment.
- Standardized images should represent hardened versions of the underlying OS and apps.
- Deviations from the standard build or updates to the standard build should be documented and approved in a change management system.
- Government agencies should negotiate contracts to buy systems configured securely out of the box using standardized images
- The master images themselves must be stored securely
- At least once per month, run assessment programs
- Utilize file integrity checking tools on at least a weekly basis
- Implement and test an automated configuration monitoring system
- Provide senior executives with charts showing the number of systems that match configuration guidelines versus those that do not match.

Critical Control 4: Secure Configurations for Network Devices

- Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, the exceptions are deployed, and those exceptions are not undone when the business need is no longer applicable. Making matters worse, in some cases, **the security risk of the exception is never properly analyzed, nor is this risk measured against the associated business need**.

Critical Control 4: Secure Configurations for Network Devices - Tools

- Network Advisor (RedSeal)
- **Firewall Analyzer & FireFlow (AlgoSec)**
- FirePAC (Athena Security)
- Assure-Firewall Compliance Auditor & Network Compliance Auditor (Skybox Security)
- FireMon (Secure Passage)
- Network Configuration Manager - (Solarwinds)

How can this control be implemented, automated, and its effectiveness measured?

- Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization.
- At network interconnection points implement filtering to allow only those ports and protocols with a documented business need.
- Test Network devices that filter unneeded services or block attacks
- All new configuration rules recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
- At least once per quarter, these rules should be reviewed.
- Employ Network filtering technologies
- Use two-factor authentication
- The network infrastructure should be managed across on separate VLANs

Critical Control 5 - Boundary Defense

- Attackers focus on exploiting systems that they can reach across the Internet, which include not only DMZ systems, but also workstation and laptop computers that pull content from the Internet through network boundaries. It should be noted that boundary lines between internal and external networks are diminishing through increased interconnectivity within and between organizations.

Critical Control 5 - Boundary Defense - Tools

- Network Advisor (RedSeal)
- FireMon (Secure Passage)
- While not one of the vetted tools, we do some filtering at our border based on the Dshield blacklist and other sources. You should not rely on this!

How can this control be implemented, automated, and its effectiveness measured?

- Organizations should deny blacklists or limit access to whitelists.
- Periodically, test packets from bogon source IP addresses
- Deploy IDS sensors on Internet and extranet DMZ systems and networks
- On DMZ networks, monitoring systems should record at least packet header information.
- Define a network architecture that clearly separates internal systems from DMZ systems and extranet systems.
- Design and implement network perimeters so that all traffic to the Internet must pass through at least one proxy on a DMZ network. The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a blacklist; and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites.
- Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
- All remote be managed by the enterprise, with remote control of their configuration, installed software, and patch levels.

How can this control be implemented, automated, and its effectiveness measured?

- Periodically scan for back-channel connections to the Internet that bypass the DMZ.
- Devise internal network segmentation schemes to limit traffic to only those services needed for business use across the internal network.
- Deploy filters on internal networks to help stop the spread of malware or an intruder.
- Force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.
- Use built-in firewall session tracking to identify long-term TCP sessions that last an unusually long time.

Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

- Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems were compromised, without protected and complete logging records, the victim is blind to the details of the attack and to the subsequent actions taken by the attackers.

Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs – Tools

- **Splunk**
- Security Blanket (Trusted Computer Solutions)
- Security Manager (Intellitactics)
- Enterprise Security Manager (Arcsight)
- OSSIM (Alienvault)
- Open Log Management (LogLogic)

How can this control be implemented, automated, and its effectiveness measured?

- Validate audit log settings
- Systems should record logs in a standardized format such as syslog entries
- Ensure that systems that store logs have adequate storage space
- devise profiles of common events from given systems
- Log all remote access
- Operating systems should log access control events associated with a user without the appropriate permissions.
- Run bi-weekly reports that identify anomalies in logs.

How can this control be implemented, automated, and its effectiveness measured?

- Network boundary devices should log all traffic arriving at the device.
- Dedicated logging servers should be used
- Organizations should deploy a Security Event/Information Management (SEIM) system tool for log aggregation, consolidation correlation and analysis.

Critical Control 7: Application Software Security

- Attacks against vulnerabilities in web-based and other application software have been a top priority for criminal organizations in recent years.
- Application software that does not properly check the size of user input, fails to sanitize user input by filtering out unneeded but potentially malicious character sequences, or does not initialize and clear variables properly could be vulnerable to remote compromise. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, and cross-site scripting code to gain control over vulnerable machines.
- In one attack in 2008, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

Critical Control 7: Application Software Security -Tools

- Hailstorm (Cenzic) –
- Nessus & SecurityCenter (Tenable)

How can this control be implemented, automated, and its effectiveness measured?

- Deploying web application firewalls
- Use automated static code analysis software to test in-house developed and third-party SW
- For applications that rely on a database, conduct a configuration review to ensure that the database system has been hardened using standard hardening templates.
- Organizations should verify that security considerations are taken into account throughout the requirements, design, implementation, testing, and other phases of the application development life cycle of all applications.
- Software development personnel receive training in writing secure code for their specific development environment.
- Require that all in-house developed software include white-list filtering capabilities for all data input and output associated with the system. These whitelists should be configured to allow in or out only the types of data needed for the system, blocking other forms of data that are not required.

Critical Control 8: Controlled Use of Administrative Privileges

- According to some Blue Team personnel as well as investigators of large-scale Personally Identifiable Information (PII) breaches, the misuse of administrator privileges is the number one method for attackers to spread inside a target enterprise.
- Two very common attacker techniques take advantage of uncontrolled administrative privileges.
- In the first, a workstation user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious web site, or simply surfing to a website hosting attacker content that can automatically exploit browsers. **The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content.** If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data.

Critical Control 8: Controlled Use of Administrative Privileges - Tools

- SMS & Active Directory (Microsoft)
- Security Manager (Intellitactics)
- Security Blanket (Trusted Computer Solutions)

How can this control be implemented, automated, and its effectiveness measured?

- **Inventory administrative passwords and validate** that each person with administrative privileges
- Before deploying any new devices in a networked environment, organizations should change **all default passwords for** applications, operating systems, routers, firewalls, wireless access points, and other systems to a difficult-to-guess value.
- Organizations should configure all administrative-level accounts to require regular password changes on a 30-, 60-, or 90-day interval.
- Organizations should ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis as is done for traditional user and administrator passwords.
- Passwords for all systems should be stored in a hashed or encrypted format.
- Administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.

Critical Control 9: Controlled Access Based on Need to Know

- Some organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information on their internal networks.
- In many environments, internal users have access to all or most of the information on the network. Once attackers have penetrated such a network, they can easily find and exfiltrate important information with little resistance.
- In several high-profile breaches over the past two years, attackers were able to gain access to **sensitive data stored on the same servers with the same level of access as far less important data.**

Critical Control 9: Controlled Access Based on Need to Know - Tools

- CounterAct (ForeScout Technologies)

How can this control be implemented, automated, and its effectiveness measured?

- Organizations should establish a multi-level data identification/separation scheme
- Organizations should ensure that files shares have defined controls
- Organizations should enforce detailed audit logging for access to non-public data and special authentication for sensitive data.
- Periodically, security or audit personnel should create a standard user account on file servers and other application servers in the organization.

Critical Control 10: Continuous Vulnerability Assessment and Remediation

- Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest.
- Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain.
- Organizations that do not scan for vulnerabilities and address discovered flaws proactively face a significant likelihood of having their computer systems compromised.

Critical Control 10: Continuous Vulnerability Assessment and Remediation – Tools

- Nexpose (Rapid 7)
- Retina (eEye Digital Security)
- IP360 (nCircle)
- Vulnerability Manager & Remediation Manager (McAfee)
- **QualysGuard (Qualys)**
- Nessus (Tenable)
- Skybox Secure solution (Skybox security)
- SAINT & SAINTmanager (SAINT)
- SecureFusion (Symantec)
- CounterAct (ForeScout Technologies)

How can this control be implemented, automated, and its effectiveness measured?

- Organizations should run automated vulnerability scanning tools
- Organizations should ensure that vulnerability scanning is performed in authenticated mode
- Vulnerability scanning tools should be tuned to compare services that are listening on each machine against a list of authorized services.
- Security personnel should chart the numbers of unmitigated, critical vulnerabilities, for each department/division.
- Security personnel should share vulnerability reports indicating critical issues with senior management to provide effective incentives for mitigation.
- Organizations should measure the delay in patching new vulnerabilities
- Critical patches must be evaluated in a test environment before being pushed into production on enterprise systems.
- Organizations should deploy automated patch management tools and

Critical Control 11: Account Monitoring and Control

- Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers.
- Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

Critical Control 11: Account Monitoring and Control – Tools

- SMS (Microsoft)
- Security Blanket (Trusted Computer Solutions)
- Security Manager (Intellitactics)

How can this control be implemented, automated, and its effectiveness measured?

- Disable any account that cannot be associated with a business process
- Systems should automatically create a report on a daily basis
- Establish and follow a process for revoking system access by disabling accounts
- Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
- Organizations should monitor account usage to determine dormant accounts that have not been used for a given period, such as 30 days. After a longer period, such as 60 days, the account should be disabled.
- On a periodic basis, such as quarterly or at least annually, organizations should require that managers match active employees and contractors with each account belonging to their managed staff. When a dormant account is disabled, any files associated with that account should be encrypted and moved to a secure file server for analysis by security or management personnel.

Critical Control 12: Malware Defenses

- Malicious software is an integral and dangerous aspect of Internet threats, targeting end-users and organizations via web browsing, email attachments, mobile devices, and other vectors. Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block its execution.

Critical Control 12: Malware Defenses

- Blink (eEye Digital Security)
- SMS & Active Directory (Microsoft)
- Not on the vetted list but any of your AV vendors. ANOTHER PLUG FOR APP WHITELISTING!!

How can this control be implemented, automated, and its effectiveness measured?

- Organizations should monitor systems for active, up-to-date anti-malware protection with anti-virus, anti-spyware, and host-based Intrusion Prevention System functionality.
- Organizations should employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis.
- Organizations should configure systems so that they will not auto-run content from USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, Firewire devices, external SATA devices, mounted network shares, or other removable media.
- Organizations should configure systems so that they conduct an automated antimalware scan of removable media when it is inserted.
- To verify that anti-malware solutions are running
- Deploy honeypots or tarpits as detection mechanisms.
- Organizations should deploy Network Access Control (NAC) tools to verify security configuration and patch level compliance before granting access to a network.

Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services

- Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and DNS servers installed by default on a variety of different device types, often without a business need for the given service.
- Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled.
- Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.

Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services - Tools

- CCM (nCircle)
- FireMon (SecurePassage)

How can this control be implemented, automated, and its effectiveness measured?

- Host-based firewalls or port filtering tools should be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- Services needed for business use across the internal network should be reviewed quarterly via a change control group, and business units should re-justify the business use. Sometime services are turned on for projects or limited engagements, and should be turned off when they are no longer needed.
- Periodically, a secure version of an authorized service should be activated on a relatively unimportant system to verify that the change is flagged by the configuration and vulnerability testing tools in the environment.
- Operate critical services on separate physical host machines, such as DNS, file, mail, web, and database servers.

Critical Control 14: Wireless Device Control

- Major data thefts have been initiated by attackers who have gained wireless access to organizations from nearby parking lots, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying travelling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization.
- Still other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network.
- Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.

Critical Control 14: Wireless Device Control - Tool

- Retina & Blink (eEye Digital Security)

How can this control be implemented, automated, and its effectiveness measured?

- Ensure that wireless device connected to the network matches an authorized configuration and security profile
- Manage all wireless devices using enterprise management tools.
- Network vulnerability scanning to detect wireless access points connected.
- Organizations should use wireless intrusion detection systems (WIDS) to identify rogue wireless devices
- Configure wireless access on client machines to allow access only to authorized wireless networks.
- Disable wireless access in the hardware configuration (BIOS or EFI) when no need
- Regularly scan for unauthorized or misconfigured wireless infrastructure devices
- All wireless traffic leverages at least AES encryption used with at least WPA2 protection.
- Use authentication protocols such as EAP/TLS or PEAP
- Use strong, multi-factor authentication credentials
- Disable peer-to-peer wireless network capabilities
- Disable wireless peripheral access of devices

Critical Control 15: Data Loss Prevention

- In recent years, attackers have exfiltrated more than 20 terabytes of often sensitive data from Department of Defense and Defense Industrial Base organizations (e.g., contractors doing business with the DoD), as well as civilian government organizations.
- Many attacks occurred across the network, while others involved **physical theft of laptops and other equipment holding sensitive information**. Yet, in most cases, the victims were not aware that significant amounts of sensitive data were leaving their systems because they were not monitoring data outflows.
- The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

Critical Control 15: Data Loss Prevention - Tools

- RSA (DLP) Suite (RSA)
- Not vetted but we own and are in the process of implementing Symantec (formerly Vontu)

How can this control be implemented, automated, and its effectiveness measured?

- Deploy approved hard drive encryption
- Network monitoring tools should analyze outbound traffic looking for anomalies,
- Monitor network perimeters for certain Personally Identifiable Information (PII).
- Conduct periodic scans of server machines using automated tools to determine whether PII data is present on the system in clear text.
- Use secure, authenticated, encrypted mechanisms for data movement across networks.
- Encrypt data stored on removable, easily transported storage media
- Configure systems so that they will not write data to USB tokens or USB hard drives.

Critical Control 16: Secure Network Engineering

- Many controls in this document are effective but can be circumvented in networks that are poorly designed. Without a carefully planned and properly implemented network architecture, attackers can bypass security controls on certain systems, pivoting through the network to gain access to target machines.

How can this control be implemented and its effectiveness measured?

- Log information about DHCP leases
- Support rapid response and rapid deployment of defensive measures.
- DNS should be deployed in a hierarchical, structured
- Segment the enterprise network into multiple, separate trust zones

Critical Control 17: Penetration Tests and Red Team Exercises

- Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Once they get access, they often burrow deep into target systems and broadly expand the number of machines over which they have control. Most organizations do not exercise their defenses so they are uncertain about their capabilities and unprepared for identifying and responding to attack.

* We want to do this but don't often have the opportunity.

Critical Control 17: Penetration Tests and Red Team Exercises

- **CORE IMPACT Pro (Core Security Technologies)**

How can this control be implemented and its effectiveness measured?

- Conduct regular penetration tests
- Penetration testing should occur from outside
- Organizations should perform periodic red team exercises
- Fully mitigate systemic problems discovered
- Create test bed that mimics a production

Critical Control 18: Incident Response Capability

- A great deal of damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response programs in place.
- Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion.
- Thus, the attacker may have far higher impact on the target organization, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible with an effective incident response plan.

How can this control be implemented and its effectiveness measured?

- Organizations should ensure that they have written incident response procedures
- Organizations should assign job titles and duties for handling computer and network incidents to specific individuals.
- Define management personnel that will support the incident handling process
- Devise organization-wide standards for the time required for personnel to report anomalous events
- Conduct periodic incident scenario sessions for personnel associated with the incident handling team

Critical Control 19: Data Recovery Capability

- When attackers compromise machines, they often make significant changes to configurations and software.
- Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information.
- When the attackers' presence is discovered, organizations without a trustworthy data recovery capability can have extreme difficulty removing all aspects of the attacker's presence on the machine.

How can this control be implemented and its effectiveness measured?

- Ensure that each system is automatically backed up on at least a weekly basis
- Ensure the ability to rapidly restore a system from backup
- Three components of a system do not have to be included in the same backup file or using the same backup software.
- Ensure that backups are encrypted
- Backup media should be stored in physically secure, locked facilities.

Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps

- Any organization that hopes to be ready to find and respond to attacks effectively owes it to their employees and contractors to find the gaps in their knowledge and to provide exercises and training to fill those gaps.

How can this control be implemented and its effectiveness measured?

- Develop security awareness training
- Devise periodic security awareness assessment quizzes
- Conduct periodic exercises to verify that employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller.

So, how are we doing?

Credits

- All of the information contained in this presentation was taken from the SANS website:

  http://www.sans.org/critical-security-controls/guidelines.php
- http://www.sans.org/critical-security-controls/user-tools.php
- Steve Scott Manager, Information Security Operations, University of Utah