A Small Business No Budget Implementation of the SANS 20 Security Controls

GIAC GCIA Gold Certification

Author: Russell Eubanks, securityeverafter@gmail.com
Advisor: Rob VandenBrink

Accepted: August 10th 2011

Abstract

A consensus of defensive and offensive security practitioners developed the SANS 20 Security Controls. In their implementation of this program, the United States Department of State demonstrated a substantial reduction in vulnerabilities in its first year alone. Given their overwhelming success, other organizations have begun to adopt this approach and have achieved similar results. Small businesses do not have to be excluded from this program. They too can use practical and often no cost ways to leverage existing security and administration tools to bolster their information security capabilities. Each control is paired with pragmatic ways for small business to rapidly deploy a continuous monitoring program at little to no cost. By leveraging and leaning into existing tools, the small business can develop a robust continuous monitoring program that is positioned to better recognize and respond to threats.

1. Introducing the SANS 20 Security Controls

The SANS 20 Security Controls were developed in 2009 to help businesses large and small embrace a framework that would promote continuous monitoring and increase network awareness (SANS, 2011). Initially labeled as the Consensus Audit Guidelines, it was birthed by a partnership of government, public and private organizations and has garnered national attention due to the successful implementation by the US Department of State. A greater than 88% reduction in vulnerabilities in the first year alone is a key highlight of this work (Streufert, 2010).

An accurate awareness of what is happening on a network is critical to the success of an information security program. It is important to do this with automation. "We need timely, targeted, and prioritized information to drive security. Without it, we are driving "in the rear-view mirror" (U.S. Department of State, 2011).

With an automated means to know what is on the network, it would be easier to determine if specific activities are authorized. Some security vendors have already embraced these controls. Tenable Network Security has published a white paper about how its products contribute to the successful implementation. The paper notes that Tenable products can help address each of the SANS 20 Security Controls using their core product offerings (Gula, Fennelly, 2011).

2. Why the Small Business?

According to the United States Small Business Administration, small businesses represent over half of all employees in the private sector and represent 44 percent of all payroll in this sector (US Small Business Administration). It is commonly believed that large businesses are better equipped to have a dedicated and full time monitoring team and that small businesses have little to no security monitoring. What if the information security staff in small business was able to tune and better leverage the existing tools around a consensus based framework designed specifically to address their gaps in coverage? Could the act of embracing this framework be an impetus to guide an organization of any size from being more compliant to being more secured? By adopting the SANS 20 Security Controls, small businesses can serve as role models for larger organizations by using automation to develop, sustain and enhance a robust continuous monitoring program.

3. What Are These Controls You Speak Of?

3.1. SANS 20 Security Controls

3.1.1. The individual controls contained in this framework guide the security practitioner towards continuous monitoring by establishing broad categories that guide and shape behavior. The first fifteen controls can be completely automated. The last five can be partially automated, but have certain components that are unable to be fully automated at this time. The guiding principles of the SANS 20 Critical Controls include focusing the defense on the most common and damaging attacks, invoking automation and continual measurement along with applying technical activities to produce a more consistent defense against attacks that occur on a frequent basis (Tarala, Cole, 2009).

3.1.2. The following are the SANS 20 Critical Security Controls:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations of Network Devices Such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know

10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Training to Fill Gaps

4. Inventory of Authorized and Unauthorized Devices

The first control is Inventory of Authorized and Unauthorized Devices. When first considering this control, it is tempting to dismiss the value of this opportunity to have near real time awareness of all devices on your network. This is the first of several creative ways to lean into your existing tools to help solve the problem of knowing what is on your network at all times. The following is an attempt to provide several ways to know what devices are on the network using existing or no cost means.

An effective way to implement this control includes the use of the SourceFire RNA product to provide constant automation. This is accomplished with the New Host and New MAC found alerts. These are located in Policy & Response, Responses, Alerts section of the administrative console. It is valuable to have an alert to an IP address change for given MAC address.

Encourage the use of a standard naming convention for your host names. Should a host that stands out appear on the network, it will be noticed more readily. Use device names in all help desk support cases. Finally, seek out the person responsible for purchasing new computers. Review an invoice to see if a MAC address is listed on the documents. Ask them to notify you about all new purchases going forward.

5. Inventory of Authorized and Unauthorized Software

Control 2 focuses on knowing all software that is installed on workstations and servers throughout your organization. Like Control 1, this may seem overwhelming at first. However, once you have started to gain momentum, this control should not be difficult to maintain and any exception will become readily apparent. Start with an initial assessment from these tools to begin the process of realizing what software is installed.

Ways to implement this control often involve leveraging existing tools in interesting ways. An example of this is found in the software inventory report in the Kaspersky Anti Virus tool. This report lists each software package and version where this software agent is installed. Configuration for this option can be found in the Administration Server at Reports and Notifications and then Server Applications. This report can be generated and emailed on a daily basis.

Qualys BrowserCheck can be used to identify web browsers and associated plug-ins that need to be updated. The free Business Edition generates a unique address that if used by all computers in the company, will generate aggregate reports of all devices that have used this website.

Microsoft System Center Configuration Manager (SCCM), formerly known as Systems Management Server (SMS) as well as Dell Kace KBox provide capabilities to inventory each software package. Of particular value are the software versions that are installed on all systems. This list can be compared to the current versions available.

The free Splunk application for Linux hosts, Splunk *NIX, includes a standard report package named Latest Packages by Host that can also be automated and emailed daily. This detailed information can be found within the Splunk application at Configs --> OS Packages --> Latest Packages by Host.

Windows includes a fascinating tool, Windows Management Instrumentation Command-line (WMIC) that allows the administrator to determine up to date information on a given Windows system. The WMIC command to list the software installed on Microsoft Windows is discussed at Command Line Kung Fu Blog (Skoudis, Medin, Pomeranz, & Matheson, 2010).

The psexec tool from Microsoft can be used to perform a software inventory, particularly for applications that do not use the standard windows installer. An example of this is to create the batch file on the C drive named baseline.bat and invoke it weekly with scheduled tasks. This command will use psexec to look for all executables and send the output to a file named ExeFound.txt

```
@echo off
psexec dir *.exe > %computername%_ExeFound.txt
```

Perfecting and adding this information to an automated baseline script is an excellent way to periodically list the packages installed on a given system. This script, when distributed to all systems can be invaluable in determining changes to your servers and workstations.

These reports are good candidates to also send to junior team members. It will let them become involved in securing the network as they begin to gain understanding of what software should be installed and learning from you the proper response when something unexpected is found.

6. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

Control 3 builds on the previous two controls, Inventory of Authorized and Unauthorized Devices and Inventory of Authorized and Unauthorized Software. The intent of this control is to develop secure configurations for all systems and monitor for any deviation from this standard. To implement this control, time must be invested in some manual work in making configuration standards for these devices. Once this is in place, perform regular and automated comparisons to these standards using readily available tools.

The real work in this control starts by reviewing configuration guides from several expert sources, such as the Center for Internet Security and the National Security Agency. These resources have detailed guides that explain the security considerations of each setting. It is a considerable amount of effort to review these documents in detail; however going through this process will cause you to better understand the system settings. It will also undoubtedly make you more aware of the importance better protecting your systems from attackers.

These templates should be used as a sound starting point in developing a secure system. Once configured, regular audits against this standard can then be performed to note any variance in system state. Revert to the known good standard and try to determine how this setting was changed. If needed, adjust the template to reflect the changing needs of the business.

The free Microsoft Baseline Security Analyzer (MBSA) tool can be used to help determine the security status of Windows operating systems. It can be run from the graphical or command line interface and can show previous test results for comparison purposes.

Also available are several security templates for Microsoft operating systems. Several default configuration types are provided and serve as a good place to begin customizing a template for your environment. These should be deployed to all systems and enforced by Group Policy, if a domain controller is available. To complete this in Windows 2008, type gpedit.msc in the Start menu to open the Local Group Policy Editor. Expand Computer Configuration and then Windows Settings and finally Security Settings. Configure the policy here and then Export the custom policy and apply it to other systems in a consistent manner.

System baselines are a critical component of meeting this control objective. Configuring automated baselines of all operating systems before a change occurs allows a comparison to be made against the former know good state. These baselines can be created for both Windows and Linux systems (SANS, 2011). Baselines should be run daily, but certainly should occur after any changes to the system or applications that depend on them.

SANS provides Intrusion Discovery Cheat Sheets for both Windows (SANS) and Linux (SANS). Use the information provided in these guides to develop automated system baselines. Should an unintended change occur, having the previous known good configuration will prove to be invaluable in the event of a compromise or unauthorized change.

On Linux systems, the application md5sum is typically installed and can be used to create md5 checksums on the contents of a folder and write the results to a file. Md5sum can then be used to compare the current checksums to those stored in the previously generated file. If any files have been changed since the last baseline, it will be noted in the exception report (Medin, & Pomeranz , 2011).

To create initial baselines with md5sum:

```
find /home –type –f | xargs md5sum > md5.txt
```

To compare current md5 checksums to contents of md5.txt:

```
md5sum –c md5.txt > current.txt
```

7. Secure Configurations of Network Devices Such as Firewalls, Routers, and Switches

Control 4 is similar to Control 3 in that it is concerned with maintaining a secure configuration. This time the focus is on network devices. What is the last activity that was performed on network devices? Likely it was to add a rule to permit a new traffic flow. When was the last time verification was made to ensure the configuration is correct? How would you know if it has been changed?

Several authoritative hardening guides exist and are freely available. Choose one of the below and plan to spend a few hours making sure the network device configurations are secure. The National Security Agency (NSA), Center for Internet Security (CIS) Security Benchmarks and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) provide configuration guides for network devices. Compare the current configuration of your network devices to a known good configuration.

Always maintain an updated network diagram by adding this step to the change request form. Change control forms should be completed with appropriate approvals before logging in to the device. Speaking of logging in, strongly consider using Radius authentication for require for named logins. If practical, also consider two-factor authentication. Alert all administrators of every attempted login and rule changes.

8. Boundary Defense

Control 5 builds on Control 4 and is concerned with increased awareness and defense of the network boundary. To defend the boundary means you must be aware of what traffic goes through all network segments. Change control procedures that are strictly followed are also an important step toward successfully implementing this control.

Configuration guides from the firewall and router vendors can be a good place to start a configuration and audit framework. This material paired with hardening guides from the Center for Internet Security and the National Security Agency.

What can be done and where do you start implementing this control to monitor and better manage the boundary defenses? Proper ingress and egress filtering should be in place. What traffic is allowed into your network is just as important as what is allowed to leave. Blacklist known bad sites and white list approved business sites. Once this is done, a careful analysis of what remains will be fruitful.

Always send alerts of successful network device logins and policy changes to every member of the security team. Monitor aggregate data from your NIDS to look for trends or new hosts. A fast and free way to do this is with the free Linux distribution Security Onion (Burks, 2011). This platform is pre-installed and configured with several useful network security monitoring tools.

Security zones must be created and diligently maintained that are based on the different types that traverse your network. All other things being equal, this will help validate that your security efforts are focused on the right network segments.

9. Maintenance and Analysis of Security Audit Logs

Logs are the single most important place to look when it is time to answer the question "what just happened". System and security logs can serve as indications and workings of scanning, recon and attack. The more systems you have, the more impractical it is to review all of the system logs individually. To facilitate this, configure each system to send its logs to a centralized log review and retention solution. This will put all of the logs in one place and also keeps another copy in an alternate location. It is hard to be successful in information security without the use of tools. This control in particular depends on the diligent and effective use of a reliable tool.

Often log review solutions are capable of ingesting logs that are in the form of a text file. This allows more information to be entered and hopefully correlated to data from the other log sources. A good tool not only allows you to search through the logs, but also lets you schedule recurring searches and alert when something is found. The following examples of reports and alerts can serve as the foundation of your indications and warnings of attack and improper configurations.

- Successful (and unsuccessful) logins to firewall and any rule changes
- Daily log volume report for the last several days
- Host has not sent logs over the last 24 hours
- All Remote Desktop Protocol usage
- All two factor authentication system and device usage
- Security log cleared
- New users, especially in privileged groups
- File Integrity Monitoring (FIM) alerts on critical files and folders

Not all tools have to be purchased, however. Martin Holste developed the free Enterprise Log Search and Archive (ELSA). ELSA is a centralized syslog platform that provides a fully asynchronous interface that normalizes logs and makes searching through log data similar to a typical web search. It also includes tools for assigning permissions, email alerts, scheduled queries and graphing. (Holste, 2011).

Microsoft provides a description of the security events in windows vista and in Windows Server 2008, including a downloadable list of all security audit events (Microsoft, 2009). Consider which of these events you want to know about and create alerts and reports that indicate when they occur. By understanding what is written to the logs and what actions they represent, more value will be realized by the security and systems administrators

SANS provides a Top 5 Essential Log Reports list that categorizes events that certainly should be addressed in log review. They are broad enough to be valid in all environments and serve as good conversation starters when looking for proper log review and analysis (Brenton, Bird, & Ranum).

- Attempts to Gain Access through Existing Accounts
- Failed File or Resource Access Attempts
- Unauthorized Changes to Users, Groups and Services
- Systems Most Vulnerable to Attack
- Suspicious or Unauthorized Network Traffic Patterns

Ensure that each device uses a trusted time source for NTP to ensure the time of each event on each system can be easily and reliable correlated.

It is a good idea to test that the log alerts are working, particularly if it has been a while since one of them was received.

Splunk is an example of a log review and consolidation tool. Splunk compiles all system, device and application logs into one place and provides a Google-like interface into these logs. Searches can be created, refined and scheduled to run at regular intervals. These can be configured to send an alert if the number of results from this automated search is greater than zero.

10. Application Software Security

Attacks against applications are certainly a growing threat to organizations. Some argue that as system administrators become better at configuring and patching their systems, the application is the next logical target of attack. What can be done at little to no cost to help prevent these threats to your environment?

Take the initiative to learn about the OWASP Top 10 Project (OWASP, 2010). Use this information to create an ongoing workshop for your developers. Help them learn these concepts and be better prepared to avoid them. Meet with your developer and quality assurance teams monthly and review one of the categories each session. With the prevalence of virtualization solutions available, it will be easy to create an environment for them to test these concepts from the comfort of their own cubicles. Leave your ego at the door and you will find this to be a valuable experience for everyone. Recognize that both groups can learn a wealth of information from each other and strengthen existing relationships. It will certainly go a long way at bridging the gap between the developers and security.

A most excellent pre-configured platform to use by your developers and quality assurance teams is Samurai Web Testing Framework (WTF). This free Linux distribution is purpose built for web application penetration testing, includes numerous tools (Johnson, Searle, 2011).

Integrate at least one component of your information security program into each step of the Software Development Life Cycle (SDLC). The key is to get to the point where the developers seek you out. This may have to involve bribery and staying late with them during maintenance, but this partnership is very possible to achieve with some effort.

Look for ways to avoid the 25 Most Dangerous Programming Errors published by Mitre and SANS. Categories of these errors include Insecure Interaction Between Components, Risky Resource Management and Porous Defenses (SANS, 2011).

Institute a peer review program where code is reviewed before it is published by a fellow developer. Consider implementing a nominal reward for each security issue identified before it is released into production. Make the first donation to the fund to show the development team you are engaged in the process. This is not meant to be harassment, rather a tool to engage the developers to lean more into secure operations. Using these very cost effective techniques will go a long way to increase the security posture of your applications.

11. Controlled Use of Administrative Privileges

Gaining access to administrative accounts is often the goal of an attacker. What can you do to ensure that only the appropriately trained and fully accountable people have and maintain administrative access on your systems? This effort must start with an accurate inventory of every account with elevated access and must be strictly maintained. The change control board should approve every new account that requires persistent administrative access. Maintaining strict admission guidelines for administrative access will help curb the desire for everyone to be an administrator. Implement an annual renewal process that requires each administrator to justify his or her continued need for elevated access.

Encourage administrators to maintain different passwords for administrator accounts where clear differences in system type exist, such as on workstations and individual server types. This will help deter unintentional access to collateral systems for which system administrators are not explicitly authorized to use. Encourage this practice by requiring more frequent password expiry and increased complexity rules for these accounts.

Accounts with elevated access must be used only when administrative activities are required. Normal web browsing and email usage should never be permitted from accounts that have elevated access. The damage that could occur is much greater than the convenience gained by allowing a system administrator to check their Twitter account.

Where feasible, require all administrative access to be achieved by elevating their access from a regular user account. Examples to facilitate this to create a Microsoft Management Console (MMC) that includes all tools needed for administration. Open this with a Run As command that uses the credentials of the elevated account. The Windows command prompt can also be run as another user by right clicking the icon and selecting the RunAs option.

Accurate and timely recording and distributing all activities performed by members of elevated access groups as found in system and security logs could help deter misuse and increase accountability. Configure a daily automated report that lists all administrative activities from the previous day to the entire team.

Look for default accounts on workstations and servers that can be removed or disabled. It is up to you to explain and justify every account on your system. The faster you can identify new accounts on the system, the better.

The underling goal must be to do everything in your power to not allow untrained or unauthorized people to gain administrative access on your networks or systems.

12. Controlled Access Based On Need to Know

Simply being an employee should not serve as adequate justification to obtain access to company data. Segregation of logical access must be in place to help deter casual browsing and potential unauthorized data disclosure. Start with broad concepts such as departments and teams as a way to isolate systems and data from those that do not require access.

A data classification program, even if elementary in nature, would be valuable to help achieve the objective of this control. Even if there are broad and limited categories of data types, it would be valuable to know where sensitive data is stored to make sure it is adequately protected from possible misuse.

Successful implementation of this control will certainly require management support. A method to gain this support is to speak with them about sensitive information they use in the company and provide an analysis of everyone who currently has access to this data. This approach may not always work, but it could help raise the importance of implementing this access control model.

Enforce strict role based access for all sensitive resources such as directories and servers and configure the default action to deny for all access that is not explicitly granted. Log failed access attempts and alert the team when failed resource attempts are detected.

Set a monthly calendar reminder to review the access of a small number of employees. Be on guard for access that may no longer be required. This can be a delicate process, so be sensitive to both the real and the perceived needs of co-workers. Enforcing this is particularly difficult with employees with tenure who tend to accumulate access over time.

13. Continuous Vulnerability Assessment and Remediation

Configure a network scanner to perform daily discovery scans on the internal and external networks. Review the output for new hosts and unexpected services. Make certain that these scans are detected by your security controls, such as Network Intrusion Detection (NIDS) and file monitoring tools. This technique is very valuable and will help assess the maturity of the continuous monitoring program.

The free Microsoft Windows Server Update Services (WSUS) provides automated patching of Microsoft products. The administrator can schedule categories of patches and schedule their installation. Also included is a reporting capability. WSUS can send daily reports via email to administrators notifying them of new patch releases and the status of their installation.

Even if in a simple spreadsheet format, track all open vulnerabilities across each system type. If you get to the point where you do not know what task to work on next, this will serve as an excellent guide to direct your attention.

Ensure that after patches are applied that you verify outside the patching tool that the patch has actually been applied. Look for clues such as registry values, installed programs and the last system reboot to help measure this control. This will help move the security program to a more mature state.

14. Account Monitoring and Control

Send automated alerts to any change or attempted change to any group whose membership grants elevated access. Daily alerts and reports of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.

Perform a quarterly review of all accounts on systems and reconcile that to the list of employees from Human Resources and the physical access control system. Often one or more of these systems are not current and is an avenue to potential compromise. Develop relationships with Human Resources in order to have a more prompt employee termination procedure. Working together, a partnership can be created and leveraged when needed.

During internal employee transfers, go through the extra step of revoking all access and then add new access required to perform the new job. This will help avoid accumulation of privileges over their tenure.

Use the Log review solution to create automated alerts for any new account, any new administrator access and also for when any account is locked out. At a minimum you will be able to provide better customer service by knowing about accounts that need to be unlocked. Perhaps these same alerts can be used to serve as indications and warnings to an attack.

15. Malware Defenses

Malware should certainly be considered unauthorized software and addressed using the techniques listed in Control 2. Maintain a listing of approved software and its business need can be readily compared to all software that has been detected.

Malware protection is often packaged within traditional anti virus software. Configure this tool to send its events to the administration tools and event log servers. Carefully review these logs for indications of system compromise. Create alerts specifically for malware infection and respond to these promptly to avoid further damage. Ensure that malware defenses are specifically configured to check for updates every hour and configure the policy to push new defenses to all agents when a new update is found.

Include the Microsoft Malicious Software Removal Tool (MSRT) in the packages distributed by WSUS. The MSRT tool is deployed monthly and is useful to eliminate known and disruptive malware.

16. Limitation and Control of Network Ports, Protocols, and Services

Just as mentioned in Control 5 Boundary Defense, proper ingress and egress filtering should be in place. Diligently maintaining awareness of the traffic that is allowed into and out of your network is critical.

SourceFire RNA Compliance Rules allow the administrator to create rules that mirror the firewall rules and alert when any other traffic occurs. This is configured in the administrative console at Policy & Response, Compliance, Rule Management, Create or open a Group. Select If a flow event occurs and meets the following conditions. Add a condition such as if Payload is AOL Mail. This feature in RNA allows the user to define approved flows and respond to everything not specifically allowed. Policy violations and new traffic flows will become immediately apparent and will be complimentary to the traditional network firewall rules.

Perform daily network discovery scans using nmap. Depending on the complexity of the network, multiple scanners may need to be deployed to ensure complete coverage. List the name of each service running on the network and attempt to justify its business need. Consider an nmap diff scan to identify all hosts and their associated services. Using the diff option, results for the new scan are compared to the previous one, with only the changes being noted.

17. Wireless Device Control

Wireless network access allows for better collaboration and mobility. With this relatively new medium comes an extra risk. Be sure to handle this administratively through the use of policy and user education to set clear expectations of appropriate use. Specific policy reference should be made that prohibits the use of peer to peer wireless networking.

Two major categories of wireless discovery tools exist. Active tools send probe requests periodically, hoping to get a response. Passive tools provide better results, due to the wireless card being placed in monitor mode. Monitor mode can be thought of as being similar to promiscuous mode on an Ethernet interface in promiscuous mode. Examples of active scanners type include Netstumbler and Vistumbler . Popular passive scanners include AirPcap and Kismet (Cache, Wright, & Liu, 2010).

Several popular Linux distributions provide pre configured Kismet. Use these platforms to continually run on old laptops in each office location. For no cost, a continual assessment for wireless activity can be performed. As each access point is identified, white list any approved and neighbor business access point and include them in the Wireless Usage policy. All others must be classified as neighbor businesses or rogues to be investigated and disabled.

Discovery of wireless access points can also be performed using traditional network scanning tools, such as Nessus. Using the plugin 11026, daily complimentary scans can help identify rogue and authorized access points. Combining both wired and wireless scanning tools will help identify wireless usage in the environment.

18. Data Loss Prevention

Data Loss Prevention (DLP) is a new trend in Information Security, but really should not be. DLP may have been a missed opportunity when NIDS was introduced. Is it all of a sudden that data exfiltration has become important? How was this missed as a priority for so long?

Define what is critical data and write regular expression filters on the NIDS that look for this data passed in unencrypted format. Educate users in security awareness training about importance of remaining diligent when handling sensitive information. Critical data should be defined in formal policy and discussed in new employee security awareness training classes.

Snort signatures such as Credit Card Data, Sensitive data credit card numbers 138:2 can be used to specifically look form information that should always be sent securely.

Consider what a data loss prevention incident would look like on your network and design your defenses and alerting to these scenarios. SourceFire Compliance Rules can be configured to alert when the files that are large in size, flows that are long in duration and flows that are new and previously undefined. Once these basic alerts are in place, develop additional data loss scenarios based on recent high profile data loss events and design appropriate controls to detect them. This is a low cost way to get wisdom as cheaply as you can.

19. Secure Network Engineering

Secure networks do not appear by accident. It starts with thoughtful planning and sound engineering principles. Seek out flaws in the current network design as an attacker would and correct all of the faults found in its design. By being intentional and meticulous, a true design can emerge and more importantly it will persist.

A key step to this is creating a document that explicitly lists all approved connections by traffic initiator. This is an excellent source document to audit the firewall rules against each and every quarter. Diligently look for the use of insecure protocols, such as FTP and Telnet in each network segment. When they are found, strongly consider using protocols that do not send their information in clear text format.

Segment networks according to security zones as well as logical departments and divisions. This will allow for more granular firewall rules and a better understanding of the communication paths that are required. Using both color-coded network diagrams and network cables is an excellent visual indicator to the types of traffic and zones being used throughout the environment.

In all monitoring systems that allow it, labeling critical systems within your existing monitoring tools will help reinforce these systems in the monitoring tools. When all else fails, this can help to guide the impact assessment.

It is important to include junior team members in these exercises and discussions. Both teaching and learning will happen for everyone involved and will lead to a more informed and engaged team environment.

20. Penetration Tests and Red Team Exercises

Penetration testing is often confused with vulnerability assessments, as mentioned in Control 10. Penetration testing differs in that it involves attempted exploitation. Just like in Control 10, penetration testing should occur in each network zone to ensure adequate coverage.

Track all open issues and document through confirmed remediation of all issues to be corrected. Determine an effective means to document the core causes of these issues to make sure new development projects are not subject to the same flaws identified in the penetration test.

Always perform careful screening of potential external pen testers. Make sure the people you engage to perform external testing have to work for their money and do not just point a tool at your network. Force them to articulate the business risk associated with their findings. Identify and resolve as many issues as is possible ahead of their work. Race to see how fast your continuous monitoring program identifies external penetration testers. If they work for long and have not been identified, there are likely gaps in the continuous monitoring program.

BackTrack makes an excellent preconfigured platform to perform penetration tests. BackTrack can easily be used as the primary environment to build and use an internal pen testing program. With so many tools available, it is a good idea to make a weekly task to learn 1 tool in BackTrack per week. Write a small note of what was learned for future reference.

21. Incident Response Capability

Enlist all employees to report suspicious activities to the Incident Response Team (IRT). Create a dedicated phone number and email address they can use to report issues to your team. Security awareness training to enable all employees to contact help desk with suspicious issues

Monthly IRT team member training that covers the steps in the Incident Handling process will be very useful. In this training, demonstrate and practice a single tool that may be used in a real incident. Rotate the training responsibilities of conducting the training as a means to engage the entire team.

After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents. Aggressively look for ways to integrate Lessons Learned from previous incidents into security design.

22. Data Recovery Capability

Develop a written plan that identifies all business owners and the processes needed by them to restore normal operations. Interview the business owners to better understand the dependencies needed to do their normal activities.

Conduct annual tabletop exercises with each business process owner. Use mock scenarios that consider availability loss of people, facilities and technology. Identify and document any gaps identified in the exercise and invite the business process owner to determine if they should be corrected or accepted. Working through this process will help engage the business units as they focus on recovering their operation to a normal state.

Test backup and restore operations on a regular and recurring basis. Create specific procedures that walk the user through how to manually backup and restore data. Just like with Incident Response, this work often occurs during high-pressure moments. Having a written procedure will help ensure critical steps are not missed. Document estimated recovery times for systems and applications. Strive to identify anything that has the potential to keep this from being successful.

23. Security Skills Assessment and Training to Fill Gaps

Is your team well trained or does it lack fundamental and often the advanced skills needed to perform their jobs? Are there team members who are the only ones that know certain functions? What happens when they are not available for good reasons or bad ones? Several avenues for acquiring training are available.

Many large cities have some or all of all of the following security focused groups that foster community and learning new concepts. Attend these meeting and become more involved in the security community.

- OWASP https://www.owasp.org/index.php/Category:OWASP_Chapter

- InfraGard http://www.infragard.net/chapters/index.php
- NAISG http://www.naisg.org/default.asp
- Defcon https://www.defcon.org/html/defcon-groups/dc-groups-index.html
- Security B-Sides http://www.securitybsides.com/w/page/12194156/FrontPage

Do not dismiss the value of setting up a home lab of old equipment or virtualized and ISO distributions to practice hacking and defending your home network. The skills acquired away from work are often the skills that make the biggest difference.

24. Conclusions

According to the US Small Business Administration website, small businesses employ half of all employees in the workforce. These businesses likely are without a foundation of network and security awareness. By learning about and implementing the SANS 20 Critical Controls, small businesses can become not only aware of, but also responsive to threats common to their small business.

Intentional steps towards implementing these controls will enhance the continuous monitoring capabilities of any organization. With intentional planning and continual drive towards these controls, the reader can start to develop a passion for implementing these controls in novel and often no cost ways.

25. References

Burks, D. (2011, July 14). http://securityonion.blogspot.com/2011/07/security-onion-20110714-now-available.html. Retrieved from http://securityonion.blogspot.com

Brenton, C., Bird, T, & Ranum, M. (n.d.). Top 5 essential log reports. Retrieved from http://www.sans.org/info/3766

Cache, J, Wright, J, & Liu, V. (2010). Hacking exposed wireless. McGraw-Hill Osborne Media

Gula, R., & Fennelly, C. (2011, February 22). Real-time auditing for sans consensus audit guidelines. Retrieved from http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/tenable_SANS-CAG_compliance_0.pdf

Holste, M. (2011, July 7). Elsa vmware appliance available [Web log message]. Retrieved from http://ossectools.blogspot.com/2011/07/elsa-vmware-appliance-available.html

Johnson, K., & Searle, J. (2011, June 9). Samurai web testing framework. Retrieved from http://samurai.inguardians.com

Medin, T., & Pomeranz , H. (2011, March 23). Episode #87: making a hash of things [Web log message]. Retrieved from http://blog.commandlinekungfu.com/2010/03/episode-87-making-hash-of-things.html

Microsoft, (2009, July 24). Security audit events for windows 7 and windows server 2008 r2. Retrieved from http://www.microsoft.com/download/en/details.aspx?id=21561

OWASP, (2010). Owasp top ten - 2010. the ten most critical web application security risks. Retrieved from http://www.lulu.com/product/file-download/owasp-top-10---2010-edition/11712679

SANS, (n.d.). Intrusion detection cheat sheet v2.0 for windows. . Retrieved from http://www.sans.org/info/3826

SANS, (n.d.). Intrusion detection cheat sheet v2.0 for linux. Retrieved from Retrieved from http://www.sans.org/info/3831

SANS (2011). Hacker Detection for System Administrators with Continuing Education – Security Architecture for System Administrators (464.1). The SANS Institute

SANS, (2011, June 27). Cwe/sans top 25 most dangerous software errors. Retrieved from http://www.sans.org/top25-software-errors Strand, J. (2011)

SANS, (2011, April 15). Twenty critical security controls for effective cyber defense: consensus audit guidelines (cag).. Retrieved from http://www.sans.org/critical-security-controls Streufert, J. (2010, November 16). Fisma 2.0: toward lower risk, faster patching & higher roi . Retrieved from www.state.gov/documents/organization/156897.pdf

Skoudis, E., Medin, T., Pomeranz, H., & Matheson, S. (2010, June 22). Episode #101: third-party party [Web log message]. Retrieved from http://blog.commandlinekungfu.com/2010/06/episode-101-third-party-party.html

Tarala, J., & Cole, E. (2009). 20 critical controls: planning, implementing, and auditing. The SANS Institute

U.S. Department of State, Information Resource Management, Office of Information Assurance. (2011). Continuous certification and accreditation (c&a) frequently asked questions (faqs) Retrieved from www.state.gov/documents/organization/156899.pdf

US Small Business Administration, Initials. (n.d.). How important are small businesses to the u.s. economy?. Retrieved from http://www.sba.gov/advocacy/7495/8420

26. Appendix 1

List of controls and tools that will help address each:

Inventory of Authorized and Unauthorized Devices	HIDS, Microsoft SMS, Dell Kace, Nessus, nmap, OpenVAS, SourceFire RNA
Inventory of Authorized and Unauthorized Software	HIDS, Kaspersky Anti Virus,Nessus, nmap, OpenVAS, Splunk *Nix Application, Qualys BrowserCheck, WMIC
Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Hardening Guides from Center for Internet Security, Microsoft Security Compliance Manager, MBSA, Nessus, nmap
Secure Configurations of Network Devices Such as Firewalls, Routers, and Switches	NSA Security Guides for Cisco Routers and Switches. Center for Internet Security (CIS) Security Benchmarks, DISA STIGs
Boundary Defense	SourceFire, Security Onion
Maintenance and Analysis of Security Audit Logs	Splunk, Syslog, ELSA
Application Software Security	OWASP Top 10 Project, Samurai WTF
Controlled Use of Administrative Privileges	Sudo, RunAs, Splunk, Syslog
Controlled Access Based On Need to Know	Splunk, Syslog
Continuous Vulnerability Assessment and Remediation	Nessus, nmap, OpenVAS
Account Monitoring and Control	Splunk, Syslog
Malware Defenses	Kaspersky Anti Virus, MSRT
Limitation and Control of Network Ports, Protocols, and Services	Nessus, nmap, OpenVAS, SourceFire RNA, WSUS
Wireless Device Control	Nessus, nmap, OpenVAS, Kismet, Aruba
Data Loss Prevention	SourceFire, Snort
Secure Network Engineering	
Penetration Tests and Red Team Exercises	Nessus, nmap, Metasploit, Core Security, BackTrack
Incident Response Capability	SANS Security 504
Data Recovery Capability	
Security Skills Assessment and Training to Fill Gaps	SANS, Security Podcasts, OWASP, ISSA, InfraGard, B-Sides, NAISG

27. Appendix 2

List of SANS 20 Critical Security Controls User Vetted Tools
http://www.sans.org/critical-security-controls/user-tools.php