Creating a Secure and Compliant Digital Forensics and Incident Response Network with Remote Access

Scott Perry

Applying the Critical Security Controls to a Digital Forensics and Incident Response Lab Network

GIAC GSEC Gold Certification

Author: Scott Perry, perry.sans@gmail.com

Advisor: Adam Kliarsky

Accepted: April 25th 2016

Abstract

Digital Forensics and Incident Response (DFIR) teams in the United States need to expand their capabilities to meet the continually growing data size and complexity of emerging cases. An effective solution is to provide investigators remote access to forensic networks hosted in a secure, accredited lab. Remote access allows greater access and flexibility while providing expandable and capable networks, but comes at the cost of increased vulnerability. This paper will apply the Critical Security Controls (v6) to a DFIR network operating with remote access.

1. Introduction

News stories involving data breaches, cybercrime, and conversely, crimes solved with digital forensics, are becoming daily occurrences. Cybercrime is becoming so common and widespread that over 594 million are affected by cybercrime globally (Norton Cybersecurity Insights Report, 2016, p. 4). With the rise of cybercrime, the need for and subsequent growth of digital forensics incident response (DFIR) teams is growing proportionally. Because of the ever increasing need for cybersecurity, DFIR labs also need to be secure; lest those labs become victims of cybercrime themselves. There is a myriad of guidelines, books, publications, and paid services available to help secure a DFIR lab network. Overly complicated solutions contribute to the problem more than it helps. The Center for Internet Security (CIS) Critical Security Controls (CSCs) can provide straight-forward guidance in designing and implementing strong security practices to ensure a DFIR lab can stay secure. The CSCs are effective because they are derived from private companies and government organizations sharing real-world information about cyber-attacks and defenses (Center for Internet Security, 2015). This information is correlated, analyzed, and then distilled into fundamental principles and guidelines which make them easy to understand and apply to cyber security, such as securing a DFIR lab network.

But what is DFIR? Digital forensics can be defined generally as “the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data” (Kent, Chevalier, Grance, & Dang, 2006, p. 11). Digital forensics is only one part of the equation for a DFIR lab; there is also the action of incident response. The definition of an incident can vary dramatically in different situations and organizations. For the purposes of this paper, an incident will be defined as “any unlawful, unauthorized, or unacceptable action that involves a computer system…and any other electronic device…that operates on a computer network” (Luttgens & Pepe, 2014, p. 2). Incident response can be defined as “a coordinated and structured approach to go from incident detection to resolution” (Luttgens & Pepe, 2014, p. 2). Combining digital forensics and incident response into one unit, operating on a shared lab network, creates a very potent and capable investigative unit. The lab network supporting DFIR investigators also needs to be very capable, and most importantly, secure.

Scott Perry;perry.sans@gmail.com

With the very dynamic nature of DFIR investigations more and more labs require remote access for their investigators and analysts. DFIR members need to deploy outside of the lab environment to conduct their investigations and analysis. Even with proper preparation and having equipment ready with everything an incident responder may need (Security 401 security essentials bootcamp style, 2015, p. 142); that investigator will inevitably need to access the DFIR lab network for additional support and tools. Having remote access to the DFIR lab will enable the responder to access the support he or she needs. But that access has to be secure, and the CSCs can assist in making remote connections secure.

There is also a time and place to use an air-gapped forensic network not connected to the Internet. Malware analysis and investigations involving contraband images should be on an isolated, air-gapped network. Due to their static nature, those networks are easy to secure and made compliant to accreditation standards. Things become much more complicated when a DFIR lab allows remote access.

Not only do DFIR labs need to worry about the integrity of their network, they have to worry about the integrity of their investigations and procedures. In the field of digital forensics, especially the United States, there has been a lot of emphasis on universal accreditation of all forensic science service providers (FSSP), which a DFIR lab is directly affected (National Commission on Forensic Science universal accreditation, 2016). These accreditation programs have been widely available for more than two decades now, but achieving and maintaining accreditation can be cost prohibitive for a DFIR lab, especially smaller labs. This paper is not about accreditation, but some of the requirements of accreditation can, and should, be applied to a DFIR lab of any size as best practices. The critical security controls can complement the ISO/IEC 17025:2005 standards, especially one with remote access.

Where possible, all of the CSCs should be implemented. But for a DFIR lab network, emphasis should be placed on the five crucial CSCs and a select five additional ones: malware defenses; limitation and control of network ports, protocols, and services; secure configurations for network devices; boundary defense; and data protection. These controls can be applied to a DFIR lab of any size and structure.

Scott Perry;perry.sans@gmail.com

1.1. Labs of Many Sizes

To meet the needs of the mission DFIR labs can be of various sizes and configurations. The exact number of practicing labs can be hard to determine because an individual or company may be operating a lab, and not be counted by the various census and accreditation organizations. However, since 2002, the growing list of over 400 federally funded labs in the United States are tracked by the Department of Justice (DOJ). Labs can be operated at the county, municipal, state, or federal level; they only have to receive federal funds to be counted in the DOJ census. Of those over 400 labs, 30% employ 10 or fewer employees and 34% employ 10 or more (Durose, Walsh, & Burch, 2012). Unfortunately, those statistics can be deceptive as digital forensic requests only account for 1% of reported statistics to DOJ, the vast majority of the reported requests were for forensic biology, toxicology, etc. The 2013 High Technology Crime Investigation Association Cyber Crime Survey narrowed the lab sampling size to only DFIR labs, and lists 66.2% of the reporting labs have one through five analysts and, 27.2% have more than six analysts (2013 HTCIA cybercrime survey, 2013, p. 4). For the purposes of this paper, DFIR labs will be classified as small if they have one through five analysts and large if they have six or more.

1.1.1. Small DFIR Labs

Small, one to five person labs, are the most common DFIR lab because they are the easiest to fund, construct, and operate. Typically characterized as utilizing stand-alone or networked workstations; small DFIR lab networks generally do not have the infrastructure or need for many server-based services such as active directory, DNS, etc. Small DFIR labs will likely have a forensic workstation subnet with attached storage, as either a NAS or a dedicated file server. Ideally, the network will utilize an appliance-based firewall and network intrusion detection system (NIDS), but it is not uncommon for those security measures to be software-based or incorporated into the edge router. For forensic analysis of malware, contraband images, or examinations of sensitive material; DFIR labs will also have an isolated, air-gapped workstation or collection of workstations. Having a network attached forensic imaging device is also a unique feature to a DFIR lab network.

Scott Perry;perry.sans@gmail.com

To enable remote access for personnel connecting to the forensic analysis subnet, or to the DFIR network backbone, the majority of smaller labs will likely utilize remote desktop protocol (RDP), or, ideally, a router with VPN capabilities.

The network diagram below shows some of the common components and structure of a small DFIR lab with remote access.

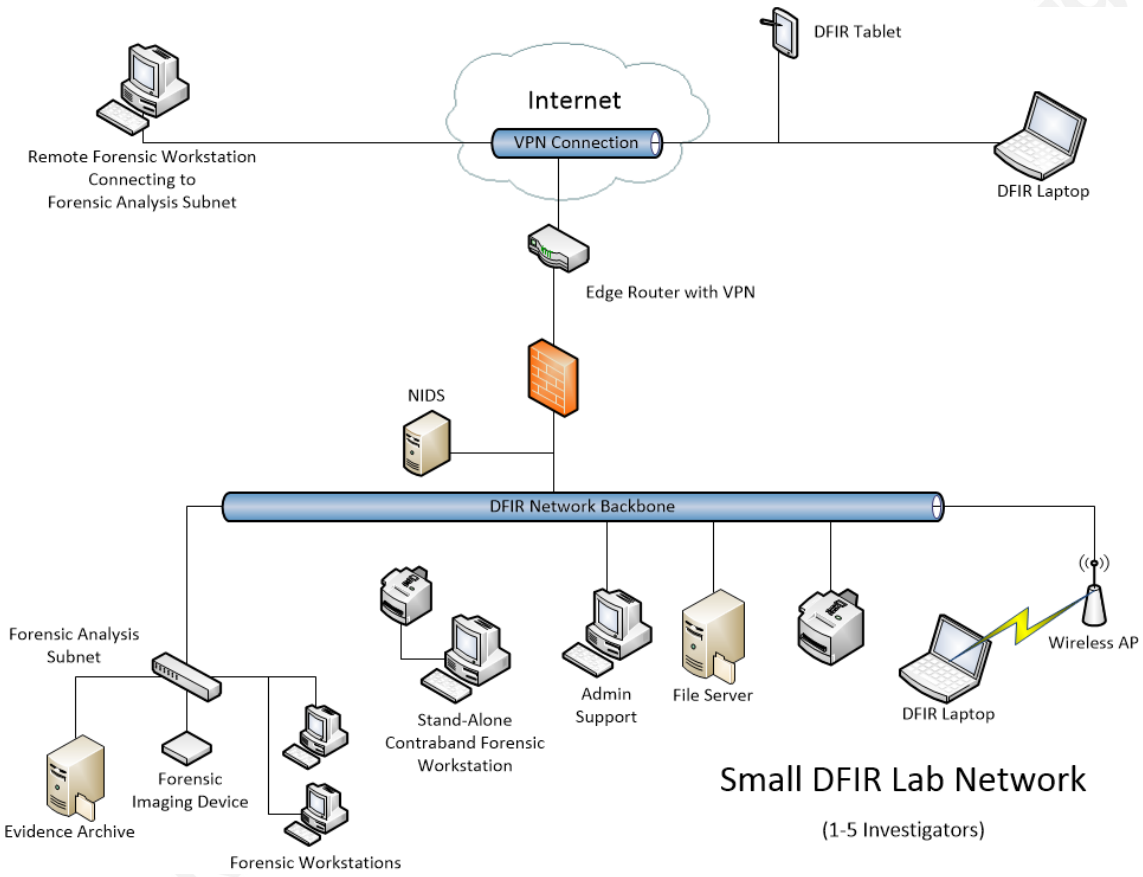

Figure 1 - Small DFIR Lab Network

1.1.2. Large DFIR Labs

In many ways, a larger DFIR lab network is typical of a business network of comparable size. It will have an administrative subnet to host an active directory, anti-malware enterprise server, administrative workstations, and other peripheral devices needed to operate the lab. A semi-public DMZ would also be needed to host a forensic application web review. The DMZ would also host a DNS to help manage the network traffic, and possibly a domain email server to facilitate case management and communication. A larger DFIR lab would have more infrastructure and funding for server-based forensic analysis. This would

be evident in the forensic analysis subnet which would incorporate forensic workstations characteristic of a smaller DFIR lab with the power of a forensic application server, working with an associated database and forensic evidence file server.

In addition to the isolated, air-gapped, contraband forensic subnet, a larger DFIR lab would have an air-gapped subnet for static and dynamic analysis of malware. This subnet could be attached to the network through a data diode or a very restrictive router and firewall, but ideally it would be air-gapped to ensure the malware is contained during testing.

The network diagram below shows some of the common components and structure of a larger DFIR lab network with remote access.

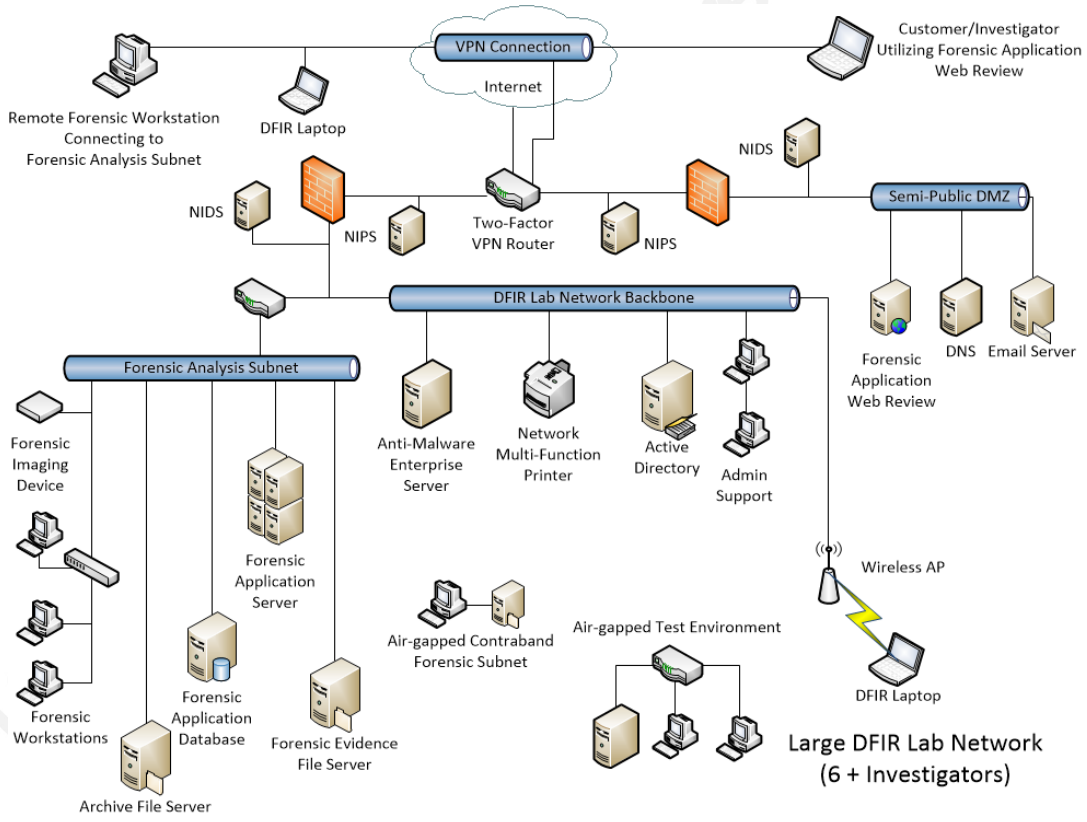

Figure 2 - Large DFIR Lab Network

1.1.3. Physical Layout

Setting up a DFIR lab can be very complicated depending on the size and mission of the lab. This paper focuses on hardware and network aspects, but those components have to be housed in a physical structure. The details and

Scott Perry;perry.sans@gmail.com

requirements for the actual construction of a new DFIR lab, or the modification of an existing building to properly house a lab, would require its own paper. However, in regards to network security, several key components of the physical requirements must be briefly addressed. Whatever network design is used, no matter how large or small, the components of the network must be physically secured. There are many standards which apply to a DFIR lab and its construction and function, below is a brief listing (Watson & Jones, 2013):

• ISO 9000 Quality Management systems series

• ISO 14000 Environmental Management systems series

• OHSAS 18000 Occupational Health and Safety series

• ISO 27000 Information technology, Security techniques, Information security management systems series

• ISO 31000 Risk Management-Principles and guidelines series

• ISO 17025 General requirements for the competence of testing and calibration laboratories.

In physical security, special emphasis must be placed on the LAN/WAN infrastructure. Wireless networks must be deployed in a way to minimize radio signals from going beyond the physical security of the lab to help mitigate eavesdropping and other wireless attacks. Regular audits should be conducted of wired network ports available to users and unused ports should be disabled. If the DFIR lab has a purpose-built server room, there are many design standards which apply. Some of these design standards include (Watson & Jones, 2013):

• ANSI/ TIA 942 Telecommunications Infrastructure Standard for Data Centers (plus the Addenda)

• ANSI/ BICSI 002 Data Center Design and Implementation Best Practices

• CENELEC EN 50173-5 Information Technology-Generic Cabling Systems- Part 5 Data Centers

• ISO/ IEC 24764 Information Technology-Generic Cabling systems for Data Centers

• AS 2834 Computer Accommodation.

Scott Perry;perry.sans@gmail.com

There are many factors and challenges associated with the physical layout of a DFIR lab: HVAC, acoustics, power, back-up power, and a whole host of others, but the primary focus should be on security. Physical access to the lab, and especially the lab network and components should be secured at all times to protect the integrity of the data and components.

2. The Five Crucial Critical Security Controls and how they relate to a DFIR network

The Critical Security Controls have evolved over time as the cybersecurity landscape has changed. The latest evolution stresses five crucial controls which are rightfully a priority in any DFIR network.

2.1. Critical Security Controls 1-3

Having an accurate accounting of all of the devices on a DFIR network is an absolute requirement for cybersecurity. Attackers can easily gain access through a newly attached device which is not correctly configured and patched. Often times the vector of attack is an unknown or unused device connected to the network.

For smaller DFIR lab networks, inventory of devices can be a relatively easy task. A lot of times personnel of a smaller lab can just look around the room, trace wires, and run some basic scans. Larger labs, hosting comparable larger networks, will have to rely on regular automated scanning to detect and catalog devices. Implementing active scans during off-peak hours and passive scans during work hours will help to minimize the impact of these scans on the network bandwidth. Regardless of network size, an inventory of consisting of: network address, machine name(s), the purpose of each system, owner of the device, and the associated department has to be recorded and regularly updated (Center for Internet Security, 2015).

To help mitigate unauthorized devices, a smaller lab with a limited amount of assets can have fixed IP addresses for workstations, file servers, network printers, etc. and easily keep track of those devices through semi-regular scans. Laptops, imaging devices, and other devices where a static IP address is not practical, can be segregated to a different subnet or VLAN where dynamic host

configuration protocol (DHCP) can be implemented and logged. This principle of network segmentation can be scaled to larger networks as well as virtual machines and devices connecting to the network remotely. Likewise, those virtual machines and transient devices can be relegated to a specific VLAN or subnet.

Just like devices, the software on a DFIR network needs to be inventoried and evaluated. The easiest way to accomplish this is to have a policy in place, with accompanying standards, listing authorized software. After establishing a list of authorized software; file integrity checking software and scanning needs to be deployed to ensure compliance. This cataloging of software can be a difficult task in a DFIR network of any size, as tools are constantly being developed, updated, and deployed in support of the mission. The need for introducing new tools and keeping pace with the ever-evolving DFIR landscape has to be managed by an engaged, and active, changed control board.

To facilitate the enforcement of the first three critical security controls, a DFIR lab can deploy standard images on devices. It is a common practice in DFIR labs to begin each case or exam with a standard image or a virtual machine containing authorized and patched software (Shaver, 2008). These standard images, comprised of approved software, can be easily deployed on segregated, air-gaped workstations and servers. DFIR laptops and devices regularly operating outside the network and connecting back remotely should also be wiped and reimaged on a regular basis, such as between each case or assignment. Wiping may seem like an extreme preventive measure, but it ensures each device is deployed conforming to the latest standards and security of the lab.

2.2. CSC 4: Continuous Vulnerability Assessment and Remediation

The fourth Critical Security Control (CSC) is all about automation and verification. Every network with a public facing IP address, and especially a DFIR lab network with remote access, needs to deploy continuous vulnerability assessments and remediation. One way of deploying this is through a scanning program such as the Microsoft Baseline Security Analyzer (MBSA). MBSA conforms with the Security Content Automation Protocol (SCAP) Validation

Program developed by the National Institute of Standards and Technology (NIST) (Cook, Quinn, Waltermire, & Prisaca, 2016). MBSA is an excellent tool because it is free, can be easily deployed on local or remote machines, and it is relatively straightforward and easy to use. These factors make it an excellent choice for small to medium-sized DFIR labs with limited resources. Although MBSA may be free and easy to use, it lacks advanced features to scan for drivers, non-Microsoft software, and network-specific vulnerabilities. ("6 free network vulnerability scanners," 2014). Larger and more diverse DFIR networks should utilize more robust, commercial vulnerability scanners if possible.

Regardless of the type of tool utilized, the scanning program has to utilize the published Common Vulnerabilities and Exposures (CVE) entries, as now managed and published by NIST. There are also commercial vendors who will provide a vulnerability subscription service, if the lab has the budget to pay for it. Automated scanning is an excellent start, but lab personnel must review the results of the scans and compare those results to event logs (Center for Internet Security, 2015). All too often scans are left to run and no one checks the results or bothers to correlate them to logs and previous scans.

2.3. CSC 5: Controlled Use of Administrative Privileges

Based on the nature of work and the tools employed, DFIR personnel usually prefer to use administrator accounts at all times. While this may be convenient to execute programs necessary to accomplish the mission, it is not a very secure practice. Attackers primarily use administrative rights or seek to elevate their unauthorized access to that level. If every user in a network has administrator rights, that makes the attackers job that much easier.

In a smaller lab environment, not commonly running an active directory (AD) to regulate users logging on to each device, the standard image deployed to each workstation should limit the user to a standard role with user access control (UAC) enabled. If applicable to his or her job, that user should be given access to the administrator account, and only use that account for limited purposes. When using the administrator accounts, multi-factor authentication should be employed where available. There should only be one member of the Administrators Group, all other users should be removed. It is also a good security practice to rename the administrator to a unique user name, to help

deter attackers guessing credentials. Additionally, the default local admin and guest accounts should remain disabled. This concept of limiting administrative accounts also applies to network devices and other specialized pieces of equipment such as forensic imagers. It is very easy to have a network attached devices such as a forensic imager connected to a network and still have the default, administrator password. These policies can be enforced with group policy object (GPO) in smaller labs; larger labs should employ AD as it is the best way to manage users in a larger network environment.

3. Other Important Controls for a DFIR Lab Network

If the first five CSCs are considered the foundation of good cybersecurity (Center for Internet Security, 2015), then the remaining fifteen should be viewed as supplemental and complimentary building blocks. It can be correctly argued that all of the CSCs are important to a DFIR lab network, however, this paper will focus on five more CSCs as they are the most applicable.

3.1. CSC 8: Malware Defenses

According to the 2015 Verizon Data Breach Investigation Report, five malware incidents happen every second. This statistic is impressive, but further analysis of those incidents reveals this prolific amount of malware is usually defeated at an organization's outer defenses and network devices (Verizon, 2015). Malware, in this instance, can be used as a generic term used to describe any software that may affect the Forensic Laboratory's information or information processing resources by disrupting operations, corrupting information, or allowing unauthorized access to it (Watson & Jones, 2013).

For a DFIR network of any size; each device, where applicable, needs anti-malware software. However, malware defense needs to be a layered. For smaller DFIR labs, each host needs to have a personal firewall and anti-malware software, and those services must be updated and patched regularly. That is a fairly easy standard to obtain as Windows and other OSs usually come with firewalls and anti-virus/malware software pre-installed or readily available for free. Scans of these systems have to be performed on a regular basis, especially the devices working remotely. Larger DFIR labs can employ

enterprise-level anti-virus and DNS query logging to check for malware attempting to communicate with command and control nodes (Center for Internet Security, 2015).

For a DFIR lab network, malware defense goes beyond deploying and maintaining a defense. DFIR labs are also in the business of studying malware, which means setting up a secure, isolated, air-gaped workstation and/or network segment, or "test lab" to conduct static and dynamic analysis of malware. This test lab can prove invaluable to a DFIR team as it can provide artifacts and behavior analysis to aid in investigations and research (Noel, 2003). All media and network connections to and from the test lab have to be treated as possibly "contaminated". Once hardware is installed in the test lab, it should stay there as part of that segregated network.

3.2. CSC 9: Limitation and Control of Network Ports, Protocols, and Service

The ninth CSC; limitation and control of network ports, protocols, and services; requires a holistic approach to understanding and implementation. The specialized nature of the tools for a DFIR lab necessitates the need to document what services and ports are needed for each program and function. Once a baseline is established, all other unnecessary ports, protocols, and services need to be shutdown. Too often an attacker utilizes an exploit targeted at unnecessary and vulnerable services or ports (Patrick, 2013).

Defense in depth can easily be applied for a DFIR lab network by implementing network segregation for services not requiring a public Internet address, and segregating services between physical hardware where applicable. This can be accomplished by having specialized, processor-intensive services such as distributed processing networks and password-cracking tools segregated to their own subnet. Critical systems also need application firewalls and, where possible, firewalls should be configured for default deny. For the DFIR lab network detailed earlier, these critical systems would be a forensic application processor, an evidence file server, or the forensic application web review server.

Automated port scanning at regular intervals should be used if a DFIR lab is operating with remote access. Some known ports and services will be

required for approved remote access, but labs have to remain vigilant and look for unauthorized remote connections.

3.3. CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

All too often in the course of DFIR investigations, it becomes apparent attackers exploited a network device operating with default configurations. DFIR labs need to take note of this common mistake and make sure their lab networks do not fall victim to the same fate (Engebretson, 2013). The first step in ensuring secure configurations are deployed; is determining what devices are needed on the network. This seems obvious but any organization, especially DFIR labs, deploy a wide variety of unnecessary network devices. These devices may include hastily deployed switches between forensic workstations to facilitate processing; or even a wireless access point to update software. Whatever the rationale, every network device needs to be securely configured before it is deployed. That means the necessity of a change control board, which establishes policy and standards defining what the secure configuration is for each device. Furthermore, the secure configuration should take into account all of the specialized forensic services and associated ports needing network access, such as distributed processing, and blocking everything else. The secure configurations for network devices in a DFIR lab do not have to be elaborate; simply figure out what services and ports the lab needs to function, and then shut off everything else.

The management of the network devices should be conducted with encrypted sessions utilizing two-factor authentication and should be conducted from a workstation specifically deployed for that purpose. The network engineering/configuration workstation should be physically isolated from the network when not in use and only used for configuration purposes (Center for Internet Security, 2015). Additionally, access to diagnostic ports should be restricted and controlled by the Forensic Laboratory IT Department (Watson & Jones, 2013).

Scott Perry;perry.sans@gmail.com

3.4. CSC 12: Boundary Defense

As part of the attack life-cycle (Mandiant, 2013), initial reconnaissance plays a vital role as an adversary probes and scans boundary defenses. As the boundary of any network is usually the first portion that attackers attempt to breach; organizations focus their network defenses only at the boundary of the network. This is a prudent first defense, but it shouldn't be the only defense. The boundary defense can be implemented on internal network boundaries as well as the external boundaries.

In a smaller DFIR lab, the boundary defense could be just a router with a firewall. Even with this meager defense, the router should be configured with a rule set to allow a whitelist of known good IP addresses and a deny a blacklist of known bad IP addresses. Based on the mission and jurisdiction of the DFIR lab this filtering can also be done with geographically assigned IP addresses.

Boundary defense is especially critical for a DFIR lab operating with remote access. Two-factor authentication should be deployed for all VPN and remote access. If the device using remote access is compromised, or the mechanism for remote access is compromised, then the external boundary defense of a DFIR lab network could be completely by-passed. One mitigation is defense-in-depth. Although networks are continually inter-connected and boundaries are blurred, DFIR labs should physically and logically segment their networks wherever possible (Center for Internet Security, 2015) and create protected enclaves of prioritized data. Where possible, boundary defenses should be established at protected enclaves.

3.5. CSC 13: Data Protection

One of the core objectives of most DFIR labs is to provide evidence in support of an investigation. If the integrity of that evidence is called into question because of a data breach, intrusion, or loss of a mobile device or laptop, then the hard work of the DFIR investigator is forfeited. Therefore, data protection for a DFIR lab goes beyond just protecting files on a server. There has to be a policy established, with standards clearly delineating protection of data in place, in transit, and at rest. This policy first begins with an assessment of what data needs to be protected and in what priority. Forensic evidence files and contraband collected in the course of investigations should be the top priority.

Scott Perry;perry.sans@gmail.com

This data can be sitting in an archive drive on a shelf; on a NAS; on a hard drive attached to a workstation; on a server being processed; on a laptop on an airplane; or even in a package being delivered across the country. In short, there are many places a forensic evidence file could be at any given time. The standards employed by a DFIR lab must protect the prioritized data in any form at any point; a challenge to say the least.

Because of the fluid and mobile environment of DFIR investigators working in the field, their laptops and mobile devices need to utilize full-disk encryption (FDE). FDE will protect the data while at rest, outside the protected confines of the DFIR lab. This FDE, with remote-wipe capabilities where available, will ensure the integrity of the data on laptops and mobile devices. Smaller DFIR labs with limited budgets can utilize FDE that is now standard on most OSs. Many times third-party vendors supply FDE as part of their enterprise-level anti-malware software suite that most larger DFIR labs can afford to purchase and deploy.

Another useful technique to ensure data protection is to disable USB and other peripheral devices. Policy should utilize common-sense when detailing how and when to disable USB and other peripheral devices. A DFIR laptop or imaging device deployable in the field should have less restrictions, to allow greater flexibility. However, a forensic workstation or server operating on a protected enclave or segment inside the DFIR lab should have restrictions on what peripheral devices can be attached. Larger labs with more assets can deploy file integrity software to ensure protected data does not leave.

4. Conclusion

The cyber threat landscape is always changing and evolving, using the CSCs to guide policy and procedure allows a DFIR lab network to remain efficient and secure. Utilizing the critical security controls, specifically the first five crucial controls and a handful of selected complimentary controls, a DFIR lab can secure their network. These CSCs follow basic principles: know what is connected to your network; know what software and services are running on your network; never deploy a network device with a default configuration; employ defense-in-depth; and have standards in place which follow a sound policy.

Scott Perry;perry.sans@gmail.com

Scott Perry;perry.sans@gmail.com

References

2013 HTCIA cybercrime survey. (2013). High Technology Crime Investigation Association.

6 free network vulnerability scanners. (2014, April 29). Retrieved from http://www.networkworld.com/article/2176429/security/security-6-free-network-vulnerability-scanners.html

Cook, M., Quinn, S., Waltermire, D., & Prisaca, D. (2016). Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements. doi:10.6028/nist.ir.7511r4

Durose, M. R., Walsh, K. A., & Burch, A. M. (2012). Census of publicly funded forensic crime laboratories, 2009. *ICPSR Data Holdings*. doi:10.3886/icpsr34340

Engebretson, P. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy* (2nd ed.). Syngress.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. doi:10.6028/nist.sp.800-86

Luttgens, Jason T. & Pepe, Matthew. (2014). Incident response & computer forensics, third edition. [Books24x7 version] Available from http://common.books24x7.com/toc.aspx?bookid=72509.

Mandiant. (2013, February 18). APT1. Retrieved March 4, 2016, from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Scott Perry;perry.sans@gmail.com

National Commission on Forensic Science universal accreditation. (2016). Retrieved from Department of Justice website: https://www.justice.gov/ncfs/file/624026/download

Noel, R. (2003). Building a security test environment. *The SANS Institute*. Retrieved from https://www.giac.org/paper/gsec/3248/building-secure-testing-environment

Norton Cybersecurity Insights Report. (2016). Retrieved from Norton Security website: https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt

Security 401 security essentials bootcamp style. (2015). Baltimore, MD: SANS Institute.

Shaver, B. (2008). A discussion of virtual machines related to forensics analysis. Retrieved March 22, 2016, from http://www.forensicfocus.com/virtual-machines-forensics-analysis

Snyder, M., Morin, P., Hutchings, C., & Hutchings, E. (2013). *2013 HTCIA cybercrime survey*. High Technology Crime Investigation Association.

Verizon. (2015). *2015 data breach investigations report*. Retrieved from Verizon website: http://www.verizonenterprise.com/DBIR/2015/

Watson, D., & Jones, A. (2013). *Digital forensics processing and procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements*. Amsterdam, NY: Syngress.

Scott Perry;perry.sans@gmail.com

Last Updated: September 21st, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS London October 2019	London, GB	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS SEC504 Madrid October 2019 (in Spanish)	Madrid, ES	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Cairo October 2019	Cairo, EG	Oct 19, 2019 - Oct 24, 2019	Live Event
Purple Team Summit & Training 2019	Las Colinas, TXUS	Oct 21, 2019 - Oct 28, 2019	Live Event
SANS Santa Monica 2019	Santa Monica, CAUS	Oct 21, 2019 - Oct 26, 2019	Live Event
SANS Training at Wild West Hackin Fest	Deadwood, SDUS	Oct 22, 2019 - Oct 23, 2019	Live Event
SANS Orlando 2019	Orlando, FLUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Amsterdam October 2019	Amsterdam, NL	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS Houston 2019	Houston, TXUS	Oct 28, 2019 - Nov 02, 2019	Live Event
SANS DFIRCON 2019	Coral Gables, FLUS	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS Paris November 2019	Paris, FR	Nov 04, 2019 - Nov 09, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, COUS	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS Sydney 2019	Sydney, AU	Nov 04, 2019 - Nov 23, 2019	Live Event
SANS Mumbai 2019	Mumbai, IN	Nov 04, 2019 - Nov 09, 2019	Live Event
SANS London November 2019	London, GB	Nov 11, 2019 - Nov 16, 2019	Live Event
SANS Dallas Fall 2019	OnlineTXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced