

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Minimizing Legal Risk When Using Cybersecurity Scanning Tools

GIAC GLEG Gold Certification

Author: John Dittmer, jdittmer@prosol1.com

Advisor: Benjamin Wright

Accepted: January 13, 2017

Abstract

When cybersecurity professionals use scanning tools on the networks and devices of organizations, there can be legal risks that need to be managed by individuals and enterprises. Often, scanning tools are used to measure compliance with cybersecurity policies and laws, so they must be used with due care. There are protocols that should be followed to ensure proper use of the scanning tools to prevent interference with normal network or system operations and to ensure the accuracy of the scanning results. Several challenges will be examined in depth, such as, measuring for scanner accuracy, proper methods of obtaining written consent for scanning, and how to set up a scanning session for optimum examination of systems or networks. This paper will provide cybersecurity professionals and managers with a better understanding of how and when to use the scanning tools while minimizing the legal risk to themselves and their enterprises.

© 2017 The SANS Institute Author retains full rights.

1. Introduction

1.1 Why is it Important to Understand How to Minimize Legal Rick While Using Cybersecurity Scanning Tools?

The objective of this paper is to take the lessons of the SANS course ISM 5600, Law of Data Security and Investigations and apply them to minimizing the legal risk of using scanning tools. As part of conducting security audits and continuous monitoring of information systems and devices, the role of scanning tools in gauging the level of cybersecurity for enterprises is becoming increasingly more crucial. Scanning tools are also being used to measure compliance with cybersecurity policies and laws, so they must be used with due care. To ensure accuracy so the scanning results can be used as evidence in courts and legal proceedings there are protocols that must be followed to ensure proper use of the tools. Users of scanning tools also need to take into consideration factors such as receiving prior written authorization, preventing interference with normal network/system operations and to ensure the integrity of the results. This paper is meant to provide cybersecurity professionals and managers with a better understanding of how and when to use the scanning tools while keeping their legal risk to a minimum.

1.1.1 Validity of Security Inspections/Audits

Since security inspections and audits are used to determine the validity of security controls, they can affect determinations of the effectiveness of security programs. This activity can lead to legal and professional implications for an enterprise's senior management. For example, in a government agency, especially in the military, senior leaders may be removed for cause if their commands fail an inspection or if evidence of improper activities was found. For example, in January 2016, Navy Rear Admiral Rick Williams was relieved for cause by the Commander of the Navy's Third Fleet, Vice Admiral Nora Tyson. In a news release, the Navy

© 2017 The SANS Institute Author retains full rights.

said Williams' removal from command was "based on the initial findings of an ongoing investigation into the alleged misuse of government computer equipment," (Myers, 2016). He was later given a letter of reprimand at an Admiral's Mast, a form of a hearing under Article 15 of the Uniform Code of Military Justice (UCMJ) (Steel, 2016). The UCMJ provides the governance for the behavior of active-duty military personnel. According to the investigative report, a team from the Navy Information Operations Command in San Diego discovered the computer violations during a routine security scan of the computers aboard the amphibious assault ship, the USS Boxer (Steel, 2016). During a routine inspection, Williams was found to have looked at pornographic images on his government computer, violating Navy rules that forbid using government furnished equipment to access pornography. The misuse of the computer did not involve any classified material (Myers, 2016).

The inspection team said that they had enough information to say it was not just an innocent mistake. Reviewing the system logs, the investigators concluded that Rear Admiral Williams viewed pornographic web sites over nine hours during two separate instances. He later admitted that he did visit the sites (Steel, 2006). This case is an example how scanning of networks and systems, can have legal implications. In this example, a Navy admiral lost his command and any prospects for future promotion. If he fought the case at a court-martial, he could have potentially been fined or imprisoned for misusing government property and conduct unbecoming an officer. However, if Navy officials decided to go forward either by administrative or legal punishment, the evidence in the form of scanning results must be accurate. Accuracy must also be ensured when conducting security audits and inspections too. Therefore, cybersecurity professionals need to take great care in conducting the scans and handling the results.

© 2017 The SANS Institute Author retains full rights.

Minimizing Legal Risk

In this case, the US Navy has two primary concerns in ensuring that the network scanning was done properly. First, the inspection team needed to ensure that the scanning was thorough enough to find misconduct like using the Navy network and equipment to view pornography. Second, as a government enterprise, the Navy has legal requirements and scanning is a means to discover those who do not comply. Finally, since the military is a unique employer with its own set of laws, it needs to ensure that the scan results can present sufficient evidence to hold up in legal proceedings in case the military member is taken to court-marital for their misconduct.

The legal and regulatory basis of cybersecurity within the Federal Government is the Federal Information Security Management Act of 2002 (FISMA). FISMA is a federal law in the United States enacted in 2002 as Title III of the E-Government Act of 2002 (NIST, 2016). This law recognizes the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source (NIST, 2016).

FISMA requires agencies to conduct annual reviews of an agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to be delivered to Congress to demonstrate the agency's compliance with the act. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and OMB to strengthen information security systems (OMB, 2006). FISMA requires each agency to implement policies and procedures to reduce security risks for information to an acceptable level on a cost-effective basis. Examples of the law assigning such responsibilities include the

© 2017 The SANS Institute Author retains full rights.

law's provisions requiring an asset inventory, risk assessments, and the categorization of systems by risk level (NIST, 2016).

Once the system documentation and risk assessment are completed, agencies must review and certify that the system's controls are functioning appropriately. Based on the certification process results, the information system is accredited. The certification and accreditation process is defined in NIST Special Publication 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems" (NIST, 2014). Through accrediting an information system, an agency official accepts responsibility for its security and is fully accountable for any adverse impacts to the enterprise if a breach of security occurs. Therefore, responsibility and accountability are core principles that characterize security accreditation. It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems to make risk-based decisions on whether to authorize the operations in those systems (NIST, 2014).

The NIST SP 800-37 specifically cites scanning, especially application scanning, as a testing and evaluation activity that is a part of the accreditation process. (NIST, 2014) While the reasoning for conduction g scanning is based on a series of linked laws and policies, it is used to implement or fulfill the requirements of FISMA. Within many agencies such as the DoD, senior officials have mandated policies and orders that require the use of scanning tools on at least a monthly basis. Currently, there is a movement within DoD to conduct continuous monitoring that will eventually require almost daily scanning. Failure to achieve scanning accuracy and optimization could constitute a violation of FISMA since the law requires system accreditation based on tools and processes, which provide senior leaders with an accurate status of the information systems (OMB, 2006).

© 2017 The SANS Institute Author retains full rights.

1.1.2 Fulfillment of Cybersecurity Service Contracts

Another factor to consider in the legal implications is to confirm the fulfillment of cybersecurity service contracts. An increasing number of enterprises outsource their cybersecurity services. However, due to both industry standards, like Payment Card Industry Data Security Standard (PCI DSS), Version 2.0, and the public-sector laws like FISMA, enterprises need to make sure that their contractors and consultants are fulfilling their contractual obligations to protect their clients' information systems and networks. In the case of PCI DSS, vendors who process credit cards are required by the PCI Security Standards Council to use scanning companies that have been approved to conduct scanning as part of their contract with the major credit card companies and banks that issue payment cards (PCI SSC, 2010). These companies are known as Approved Scanning Vendors. So, in this case, scanning is legally and contractually required to verify compliance with an industry security standard (PCI SSC, 2010).

Compliance with PCI DSS is not currently required by federal law in the United States. However, some US state laws either refer to PCI DSS directly or make equivalent provisions. States that include PCI DSS in their laws in the last several years include Minnesota, Nevada, and Washington State (Minnesota, 2007) (Nevada, 2015) (Washington, 2011).

2. Introduction to Cybersecurity Scanning Tools

2.1 Development of Scanning Tools

The origins of scanning tools can be traced back to the research began in 1989 by a student at Purdue named Dan Farmer, who was working on an academic project under one of his professors, Gene Spafford. This project was intended to create a software tool called the Computer Oracle and Password System (COPS), that was comprised of several small, specialized vulnerability scanners designed to identify security weaknesses in one part of an

© 2017 The SANS Institute Author retains full rights.

UNIX operating system (Associated Press, 1995). After he completed college, Dan Farmer began to work for Sun Microsystems and started to collaborate with Wietse Venema of the Eindhoven University of Technology in the Netherlands. Together, they wrote a paper in 1993 titled, "Improving the Security of Your Site by Breaking into It." In the paper, Farmer and Venema stressed that system administrators and security personnel need to approach their networks as an attacker would (Farmer & Venema, 1993). In other words, they put on paper the concept that learning how to conduct offensive strategies teaches one how to implement an effective defense. In their paper, they discussed security practices, which are much like the Critical Security Controls that were published several years later by the Center for Internet Security. Examples of such security practices that Farmer and Venema described included conducting inventories of hardware and software as well as establishing secure configurations of systems that later were included in the Critical Security Controls. Part of their approach was using early scanning tools such as SATAN (Security Administrators Tool for Analyzing Networks) which Farmer and Venema were developing and later released in 1995 (Associated Press, 1995). Another scanning tool that they recommended was ISS (Internet Security Scanner) which was originally written by Chris Klaus, a student at the Georgia Institute of Technology in 1992 (IBM, 2007). Klaus formed a company also called ISS in 1994 that International Business Machines (IBM) bought in 2007 (LaMonica, 2007). In turn, IBM developed ISS into several other commonly used scanning tools such as Internet Scanner, Proventia, and Enterprise Scanner (IBM, 2007).

Returning to the work of Farmer and Venema with SATAN, it was interesting to note that after they published SATAN, some network administrators, and law enforcement personnel concluded that hackers would use it to identify and break into vulnerable computers. There were

© 2017 The SANS Institute Author retains full rights.

no existing laws nor legal guidelines on the activity. Thus, SATAN was getting a lot of bad publicity, and the name did not help. Consequently, Farmer lost his job with his employer at the time. Clearly, there can be consequences when rules are not established to provide guidance. However, within a few years, the use of vulnerability scanners such as SATAN became an accepted method for auditing computer and network security once most security personnel accepted the approach that Farmer and Venema had discussed in their paper (Associated Press, 1995).

Based on the source code for SATAN, a company now known as the SAINT Corporation developed a scanning tool called SAINT (Security Administrator's Integrated Network Tool) in 1998. Its advantage over earlier tools was that The SAINT scanner screens every live system on a network for TCP and UDP services. For each service, it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information about the network (Stephenson, 2010).

Another well-known network-scanning tool, Gordon Lyon released Nmap as a simple Linux-only port scanner in September 1997. Over the next 16 or more years, Nmap was used by developers to sprout a myriad of valuable features, including OS detection, version detection, Nmap Scripting Engine, and a Windows graphical user interface, Ncat, Nping, Ndiff, and more (Lyon, 2012). In March 1998, a young Frenchman, Renaud Deraison, wrote Gordon Lyon, asking permission to use some of the Nmap source code to develop a tool called Nessus. Nine days later, Deraison sent Lyon the first widely- used vulnerability assessment scanner called Nessus, which has been the most popular tool among security professionals for the last several years (Piper, 2013). In 2002, Deraison formed a company called Tenable. The next year, Tenable developed a management console for managing Nessus scans and their results called

© 2017 The SANS Institute Author retains full rights.

Tenable Security Center (Piper, 2013). The Department of Defense (DoD) has used a special version of Nessus called the Assured Compliance Assessment Solution (ACAS) since 2012.

Retina was a scanning tool that was developed by a start-up company called eEye Digital Security (now owned by BeyondTrust) under the leadership of Firas Bushnaq and Marc Maiffert in 1998 (BeyondTrust, 2012). Through the years, Retina has evolved into multiple tools such as:

- Retina Network Security Scanner, a vulnerability assessment tool for networks

- BeyondSaaS, a tool that provides both network perimeter vulnerability scanning and a web application security assessment

- Retina Web Security Scanning, an application security testing (DAST) application that identifies cross-site scripting (XSS), SQL injection, and other vulnerabilities across complex websites and web applications.

- PowerBroker Endpoint Protection Platform, a single, lightweight client that replaces multiple security agents, protecting against Advanced Persistent Threats (APTs), known exploits, zero-days, and all other attack vectors (BeyondTrust, 2012).

While there are many other security scanning tools on the market available, this is a brief overview of the history of the major players in the industry. Cybersecurity professionals need to know how the various scanning tools can be useful so they can choose the right tool and procedures to use for the purposes of audits, forensics, network mapping, asset inventories, etc.

2.2 Description of Major Tools in the Market

If security professionals want to manage the legal risk of using cybersecurity-scanning tools properly, they need to understand their essential functionality.

2.2.1 Basic Functions of a Cyber Security Scanning Tool

A vulnerability scanner scans a network or system (such as a computer, mobile device, server or router) and reports back on identified open ports, active Internet Protocol (IP) addresses and log-ons. It will also report on vulnerabilities affecting operating systems, software, and

© 2017 The SANS Institute Author retains full rights.

services that are installed and running. The scanner software performs a comparison on the information it finds against known vulnerabilities located in its database or third-party databases such as CVE, OVAL, OSVDB or the SANS Institute/FBI Top 20 (Lindros and Titttel, 2014).

A scanner tool typically develops priorities on known vulnerabilities as critical, major or minor. The significant value of vulnerability scanners is that they can detect malicious services such as Trojans, which are listening in on the ports of a system (Lindros and Titttel, 2014).

However, not all scanners operate the same way. For example, many inexpensive and free vulnerability scanners only scan a network or system and provide remedial reporting. More feature-rich tools incorporate patch management and penetration testing, among other installed features. However, many scanners – at either the low-end or high-end – suffer from false-positives and false-negatives. False-positive readings usually result in an administrator chasing down information about an issue that does not exist. A false-negative reading is more significant, as it, means the scanner failed to identify or report something that poses a major security risk. Therefore, training security personnel on the use of these tools is important in preventing problems (Lindros and Titttel, 2014).

While conducting research on vulnerability scanners, it is important to learn how they are rated for accuracy (the most important metric) in addition to other factors such as reliability, scalability, and reporting. If accuracy is lacking, security personnel will most likely run two different scanners with the hope that one discovers vulnerabilities that the other may have missed. This remedy adds cost and effort to the scanning process. Not only are security personnel spending double the time on the scanning process itself, they are forced to search through two sets of scanning results to see what is accurate (Lindros and Titttel, 2014).

© 2017 The SANS Institute Author retains full rights.

2.2.2 Categories of Cyber Security Scanning Tools

Software-Based Vulnerability Scanners: These scanners provide targeted reports from various devices. Some of the most commonly known and highly rated commercial vulnerability scanners are Nessus (Tenable Network Security), Secunia CSI, and Core Impact (Core Security). Nessus started as a free tool but Tenable converted the tool to a commercial product, with a more enhanced feature set and higher quality technical support. Secunia is free for use at home and school and it is affordable for commercial use. Core Impact is pricey ($40,000 and up) but offers terrific value for the money since it conducts more thorough scans than similar products (Lindros and Titttel, 2014).

Vulnerability scanning products generally includes configuration auditing, target profiling, penetration testing, and detailed vulnerability analysis. They are designed to integrate with Windows products, such as Microsoft System Center, to provide intelligent patch management; some work with mobile device managers. They can scan not only physical network devices, servers, and workstations, but they also can extend to virtual machines such as Bring Your Own Device (BYOD) mobile devices and databases. Some of the products, such as Core Impact, integrate with other existing scanners, enabling security personnel to import and validate scan results (Lindros and Titttel, 2014).

Software-based scanners also require much less administration than their counterparts from 10 years ago, do, or what are considered the low-end tools of today. This improvement is due to greatly- improved user interfaces and targeted analysis reports with clear remediation actions. Reporting functionality lets one sort on many different criteria, including vulnerability and host, to see trends in changes over time (Lindros and Titttel, 2014).

© 2017 The SANS Institute Author retains full rights.

Cloud-Based Vulnerability Scanners: This type of scanner provides security personnel with continuous, on-demand monitoring. A newer type of vulnerability scanner is then delivered as an on-demand Software as a Service (SaaS). Products such as Qualys Vulnerability Management provide continuous, hands-free monitoring of all computers and devices on all network segments (perimeter to internal). They can also scan cloud services such as Amazon EC2. With an on-demand scanner, there is no installation, manual integration or maintenance required – a subscription to the service is required and then the scans should be configured (Lindros and Titttel, 2014).

2.3 Proper Procedures in the Use of Scanning Tools

Since scanning networks and systems is an important part of assessing their security status, due care must be given in the planning and execution phases of network scanning.

2.3.1 Develop a Scanning Plan

Developing a scanning plan is an essential part of cybersecurity activities. For example, in the DoD, inspection teams are required to submit a formal plan before they can scan a military command's networks and systems. As background information on the DoD processes as an example, the networks and systems that are the responsibility of a military command or agency that are usually referred to as enclaves. The security of the enclave is the responsibility of the military commander or agency head. Therefore, the inspection teams need to submit a formal plan for scanning before they arrive on-site or perform the scans remotely. The plans usually include following elements:

- Dates and times for scanning
- Range of Internet Protocol (IP) addresses to be scanned

© 2017 The SANS Institute Author retains full rights.

- Names of systems and networks to be scanned. Make sure that the scanning tools do not probe other connected networks without prior permission.
- Listing of scanning tools to be used
- A listing of personnel conducting scans and their qualifications should be provided. Security certification organizations such as GIAC now have professional certifications such as GPEN. This type of certification demonstrates that personnel are qualified and understand the consequences of their scanning activities. In some jurisdictions and circumstances, the forensic investigators are required to be licensed Private Investigators, especially if the scanning is done for forensic purposes.
- If scanning is to be done remotely, a listing of IP addresses of the scanning origin (so the enclave's security personnel will not mistake the scanning for a cyber-attack or a gathering intelligence on networks and systems prior to a breach attempt) must be provided.
- List potential damage that could happen to systems to make the System Owners aware of the risks (Rasch, 2013).

With such a plan in place, both the inspecting team and the enclave are kept informed of the activities taking place, which can prevent misunderstandings that could affect the inspection. Thus, all parties involved are managing their operational and legal risks. Organization make similar provisions internally as a part of their operational plans so that security scanning does not interfere with the normal operations of the Information Technology functions of an enterprise. This is especially true as many organizations conduct daily scanning as part of the continuous monitoring of networks and systems.

2.3.2 Obtain Written Consent of the System Owner

An important aspect of a cybersecurity scanning plan is obtaining the written consent of the System Owner. This is an important from a legal standpoint for a couple of reasons. First, the written consent provides the legal cover that scanning personnel has written consent to perform their scanning activities if someone might dispute it later. Second, the written consent demonstrates that the scanning was not part of any cyber-attack or other illegal activities.

© 2017 The SANS Institute Author retains full rights.

Finally, if there is any dispute over the results of the scanning, the scanning plan serves as evidence on how the activities were conducted and what the security personnel's intentions were when he or she did the scanning. Since the results of the scanning may drive how the enterprise's level of security is perceived, especially in terms of compliance with standards or policies, the scanning plan is an important document (Rasch, 2013).

3. Proving the Accuracy of Scanning Tools

Since the results of a security scan are heavily dependent on the accuracy of the scanning tools, measuring and maintaining the accuracy of the tools is extremely important as described below:

3.1 Analogy - Intoxilyzer Test for Detecting Drunk Drivers

A law enforcement analogy for the importance of the accuracy of cybersecurity scanning tools is the accuracy of the Intoxilyzer test for people suspected by the police of driving while impaired (DWI) or under the influence (DUI) of alcohol. Normally, when a police officer pulls over a driver suspected of driving intoxicated, the driver would routinely be given a field sobriety test. If the driver fails the field sobriety test, then he or she will be brought to the police station for the Intoxilyzer test while will measure their Blood Alcohol Level (BAL) per commonly accepted law enforcement practices. If the driver's BAL was above the legal standards, they would be formally arrested and charged for either DWI or DUI.

In the above situation, defense attorneys will routinely examine the evidence of what happened in the apprehension process, including the Intoxilyzer test. They will look to see if the testing machine was properly calibrated and maintained. They will also see records about the previous arrests using that device to see if there were problems with the machine in the past. The

© 2017 The SANS Institute Author retains full rights.

motivation for this research by defense attorneys is to see if there is good reason to have the Intoxilyzer results thrown out as evidence against their clients. Thus, police departments should make accurate and detailed records of the Intoxilyzer machine calibration and maintenance. In much the same way, if a computer scanning results in a legal case, defense attorneys will examine how the scanning tools are operated and maintained as if they would examine the Intoxilyzer in a DWI or DUI case. The purpose of such an examination again is to remove the scanner results as evidence and make the case for reasonable doubt for their clients.

3.2 How Scanning Tools are First Measured for Accuracy in the Laboratory Environment

Just as the function of the Intoxilyzer is subject to legal review and scrutiny, the results of the functions of scanning tools must be scrutinized to ensure they achieve the legal purposes for which they are employed, such as collection of evidence or confirmation of compliance of cybersecurity policies and laws.

3.2.1 What to Test the Tools for

In general, vulnerability scanners are designed to find the following:

- All the hosts that are running on the network
- The open ports on these hosts
- The services that are running on these ports
- If these services are patched with the latest updates
- If the network is properly configured

Thus, any testing of a scanner's capabilities should test against known values such as which hosts are running in a computing environment and which ports are open on these hosts (Nilsson, 2006).

© 2017 The SANS Institute Author retains full rights.

3.2.2 Setting up the Testing Computing Environment

Typically, in a testing computing environment, the scanners run against a laboratory network to find out if they discover known vulnerabilities. A penetration test of the laboratory network should be conducted to see if the scanners could find and warn about vulnerabilities that come from configuration errors or vulnerabilities that are the product of two or more services that are used in the network. The penetration tests would also pinpoint the easiest ways the network could be exposed. A comparison between the scanners reports and the penetration test could give a hint of the quality of the work the vulnerability scanners perform. If the software used in the laboratory network has not been updated for long periods, there should be several vulnerabilities present. Usually, there are many active hosts in the network, which consist of routers, firewalls, and other devices. The hosts are normally using popular operating systems like Red Hat Linux and different Windows versions. In addition, a laptop or a desk with a processor with typical speed of about 2.4 GHz and a good-sized memory of about 4 GBs should be used (Nilsson, 2006).

3.2.3 Conducting the Testing

To discern how well the scanners work, a penetration test or "hack" would be conducted on the lab network. This testing is often done using the same access point that the scanners previously used to scan the network. It is done without using any background knowledge of the lab network, except the IP number to use for connecting to the network. The goal of such a hack is to gain root access to a couple of machines and explore the network for vulnerabilities to see what harm a potential hacker could cause the laboratory network. The goal of the hacking attempt should answer the following questions:

© 2017 The SANS Institute Author retains full rights.

- Can any false negatives be proven?
- Have the scanners missed anything while scanning the network?
- Can any false positives be proven?
- Are the scanners reporting on errors that do not exist?
- Do the scanners really scan as thoroughly as it is stated in the manuals? (Nilsson, 2006)

After this type of test is done, a tester can conduct a variety of experiments to see if the scanning tools can find known vulnerabilities in the network and systems such as applications and devices. When a scanner is tested to confirm it can achieve its legal and security purposes, then the tests need to be recorded so they can be referenced later if there is a legal question. At this point, security professionals need to establish protocols for establishing a credible chain of custody that can h o l d up as evidence in court.

3.3.3 How is Accuracy Maintained in the Operational Environment?

Once a scanning tool active is in the operating environment, there are no specific standards or laws stating how often the scanning tools need to be tested, security personnel would be prudent to run a controlled test as described in the last section at least locally at least on an annual basis and after every software update. This way, security personnel can state in legal proceedings, if necessary, that they have tested the scanning tools on a regular basis to make sure that they worked, as intended.

4.0 Case History Regarding the Accuracy of Scanning Tools

The introduction of the use of scanning tools has brought on some legal debates and even legal cases. The following is a small sampling of the types of legal issues that can arise when scanning tools are being used and their accompanying misunderstandings or debates.

© 2017 The SANS Institute Author retains full rights.

4.1 Sample Case History 1 (Port Scanning)

On the Nmap.Org web site, there is a page devoted to the ongoing debate over scanning network ports. The site advises users that the best way to avoid controversy such as legal disputes over their scanning when using Nmap is to obtain written authorization from the target network representatives before initiating any scanning. There have been cases when system owners have considered people scanning using Nmap on other people's networks to be performing network intrusions. That advice seems consistent with other sources. There is still a chance that Nmap or other network mapping tools might get into trouble with their Internet Service Providers (ISPs) if they notice the scanning (or if the target administrators accidentally submit an abuse report), but this situation is usually easy to resolve. When performing a penetration test as a contractor, the authorization for this test should be in the Statement of Work. When testing on that client's network, the tester should make certain that this activity clearly falls within his or her job description. Security consultants should be familiar with the excellent Open Source Security Testing Methodology Manual (OSSTMM), which provides best practices for these situations (Lyon, 2006).

While security professionals are concerned about civil and (especially) criminal court cases, they are relatively rare in the case of scanning within the United States. Currently, there are no federal laws in the United States that explicitly criminalize port scanning. A much more frequent occurrence is that the target network will notice a scan and send a complaint to the originator's ISP. Most network administrators do not seem to care or notice the many scans bounce off their networks daily, but a few complain. The scan source ISP may track down the user corresponding to the reported IP address and time, then admonish the user or even block them from the ISP. Port scanning without authorization is sometimes against the provider's

© 2017 The SANS Institute Author retains full rights.

acceptable use policy (AUP). For example, the AUP for the huge cable-modem ISP Comcast says:

> Network probing or port scanning tools are only permitted when used in conjunction with a residential home network, or if explicitly authorized by the destination host and/or network. Unauthorized port scanning, for any reason, is strictly prohibited (Lyon, 2006).

Even if an ISP does not explicitly ban unauthorized port scanning, they might claim that some "anti-hacking" provision applies. Of course, this activity does not make port scanning illegal. Many perfectly legal and (in the United States) constitutionally protected activities are banned by ISPs. For example, the AUP quoted above also prohibits users from transmitting, storing, or posting "any information or material which a reasonable person could deem to be objectionable, offensive, indecent, pornographic, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful" (Lyon, 2006). In other words, some ISPs ban any behavior that could possibly offend or annoy someone. Indiscriminate scanning of other people's networks does have that potential (Lyon, 2006).

While legal cases involving port scanning (without follow-up hacking attacks) are rare, they do happen. One of the most notable cases involved Scott Moulton, a consultant who maintained the Cherokee County, Georgia emergency 911 (E911) system. In December 1999, Moulton was tasked with setting up a router to connect the Canton, Georgia Police Department with the E911 Center. Concerned that this connection may jeopardize the security of the E911 Center, Scott Moulton started preliminary port scanning of the networks involved using the Nmap

© 2017 The SANS Institute Author retains full rights.

scanning tool. In the process, he scanned a Cherokee County web server that was owned and maintained by a competing consulting firm named VC3. The company noticed the scan and emailed Scott, who replied that he worked for the E911 Center and was testing security. VC3 then reported the activity to the police. Scott lost his E911 maintenance contract and was arrested for allegedly violating the Computer Fraud and Abuse Act of America Section 1030(a) (5) (B). This law forbids "intentionally accesses a protected computer without authorization, and because of such conduct, causes damage" (and meets other requirements) (Lyon, 2006). The destruction claimed by VC3 involved time spent investigating the port scan and related activity. Scott sued VC3 for defamation, and VC3 countersued for violation of the Computer Fraud and Abuse Act as well as the Georgia Computer Systems Protection Act (Lyon, 2006).

The civil case against Scott Moulton was dismissed before trial, implying a complete lack of merit. The ruling made many Nmap users smile:

> "Court holds that plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of either the Georgia Computer Systems Protection Act or the Computer Fraud and Abuse Act."—Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000) (Lyon, 2006)

This was an exciting victory in the civil case, but Scott still had the criminal charges pending.

Eventually, the criminal court came to the same conclusion, and all charges were dropped. While Scott was vindicated in the end, he suffered six-figure legal bills and endured stressful years battling through the court system. The positive aspect is that after spending so much time educating his lawyers about the technical issues involved, Scott started a successful

© 2017 The SANS Institute Author retains full rights.

forensics services company (Lyon, 2006). Despite his eventual victory, Scott Moulton should have gained written authorization prior to conducting his scanning. It would have saved him years of legal hassles and hundreds of thousands of dollars in legal fees, thus reducing his legal risk. The written authorization should have clearly stated where, when, how Moulton would have conducted the scanning. If he followed the provisions of the authorization, it would have been hard for anyone to press a criminal or civil case against him.

Laws in other nations obviously differ as well. For example, a 17-year-old youth in Finland was convicted of attempted computer intrusion for simply port scanning a bank. He was fined to cover the target's investigation expenses. In Finland, the law in the nation states that the intruder must cover the cost of remediating any security damages. The Moulton ruling might have differed if the VC3 machine had crashed and they could justify the $5,000 damage figure required by the act (Lyon, 2006). At the other extreme, an Israeli judge acquitted Avi Mizrahi in early 2004 for vulnerability scanning the Mossad intelligence service. Judge Abraham Tennenbaum even praised Avi for his technical skills in his ruling (Lyon, 2006).

In 2007 and 2008, broad new cybercrime legislation took effect in Germany and the United Kingdom (UK). These laws were meant to ban the distribution, use, and even possession of “hacking tools.” For example, the UK amendment to the Computer Misuse Act makes it illegal to “supply or offer to supply [a program], believing that it is likely to be used to commit, or to assist in the commission of [a Computer Misuse Act violation]"(Lyon, 2006). These laws have already led some security tool authors to close shop or move their projects to other countries.

© 2017 The SANS Institute Author retains full rights.

Minimizing Legal Risk

The problem with laws that ban certain security tools such as vulnerability scanners is that most security tools is that most security tools can be used by both ethical hackers (white-hats) to defend their networks and black-hats to attack. These dangerous laws are based on the tool author or user's intent, which is subjective and hard to discover. Regardless of the legal status of port scanning, ISP accounts will continue to be terminated if many complaints are generated. The best way to avoid ISP abuse reports or civil/criminal charges is to not conflict with the target network administrators in the first place. Here are some practical suggestions:

Security personnel should ensure that they obtain written permission to scan to minimize the risk to themselves and their employers. Most network vulnerability scanning is non-controversial. People who scan are rarely get into legal disputes for scanning their own personal machines or the networks they administer. The controversy comes when people are scanning networks that belong to other people or enterprises. There are many reasons (good and bad) for them to do this sort of network exploration. Perhaps they are scanning the other systems near them to look for publicly shared files. Alternatively, maybe, they are just trying to find the IP address of a certain printer. Perhaps they are just trying to test connectivity, or maybe they wanted to do a quick security sanity check before handing off their credit card details to that e-commerce company. They might be conducting Internet research. Another possible scenario is that people conducting scanning are really performing initial reconnaissance in preparation for a break-in attempt? The remote administrators rarely know their true intentions, and do sometimes get suspicious (Lyon, 2006).

Target your scan as tightly as possible. Any machine connected to the Internet is scanned regularly enough that most administrators ignore such Internet background noise. However,

© 2017 The SANS Institute Author retains full rights.

scanning enough networks or executing very noisy/intrusive scans increases the probability of generating complaints. So, if you are only looking for web servers, specify port 80 rather than scanning all 65,536 TCP ports on each machine. If people scanning are only trying to find available hosts, then they should do an Nmap ping scan rather than full port scan (Lyon, 2006).

People conducting scans using network connections from work or school should not considered controversial activity. Even though your intentions may be good, you have too much to lose if someone in power (e.g. boss, dean) decides you are a malicious cracker. If an ISP, such as Comcast discussed above, bans any unauthorized port scanning and posting of "offensive" material, then people should not be surprised if they are kicked off for this activity (Lyon, 2006). Gordon Lyon provides the following advice:

- Always have a legitimate reason for performing scans. An offended administrator might write to you first (or your ISP might forward his complaint to you) expecting some justification for the activity. In the Scott Moulton case discussed above, VC3 first emailed Scott to ask what was going on. If they had been satisfied with his answer, matters might have stopped there rather than escalating into civil and criminal litigation. When I scan large portions of the Internet for research purposes, I use a reverse-DNS name that describes the project, run a web server on that IP address with detailed information, and opt-out instructions (Lyon, 2006).
- Remember that a person's ancillary and subsequent actions are often used as evidence of intent. A port scan by itself does not always signify an attack. A port scan followed closely by an IIS exploit, however, broadcasts the intention loud and clear. This factor is

© 2017 The SANS Institute Author retains full rights.

important because decisions to prosecute (or fire, expel, complain, etc.) are often based on events and not just one component, such as a port scan (Lyon, 2006).

Similarly, criminal or civil charges involving port scanning are usually reserved for the most egregious cases. Even when paranoid administrators notify the police that they have been scanned, prosecution (or any further action) is exceedingly rare. The fact that a 911 emergency service was involved is likely what motivated prosecutors in the Moulton case (Lyon, 2006).

In summary, the question of whether port scanning is legal does not have a simple answer. Laws differ dramatically between jurisdictions, and cases hinge on their specific details. People conducting scans need to check the laws of the applicable jurisdictions before conducting scans.

4.2 Sample Case History 2 (War Driving)

Stefan Puffer, a Houston computer security consultant, conducted a "war driving" exercise, with the head of the Harris County's Central Technology Department and a reporter for the Houston Chronicle. Puffer demonstrated that the wireless network for the Harris County Clerk's office was misconfigured to allow anyone to have access to the computing environment. Puffer claims that he stopped the exercise when he saw the misconfiguration. Harris County officials discovered pornography on one of the computers, and after all the County employees deny any involvement, they arrested Puffer for hacking. Tens of thousands of dollars in legal bills later, a jury acquitted Puffer in all of 15 minutes (Rasch, 2013). This case specifically shows how prior written authorization would have probably reduced the legal risk to Puffer by

© 2017 The SANS Institute Author retains full rights.

preventing a criminal case being brought against a security consultant. Just having oral permission or being in the presence of the system owner is not enough.

Another lesson is that security professional should have strict protocols on handling the evidence so they are not accused themselves of illegal activities like Stefan Puffer did. If the protocols in place, it would have reduced for the legal risk both Puffer and Harris County for a couple of reasons. First, following the protocols will help to ensure that there was a chain of custody for possible court case for whoever was really keeping pornographic material on a government computer and helping to ensure that charges would be brought against the correct person who that an innocent party like Puffer cannot sue Harris County for wrong persecution.

4.3 Sample Case History 3 (Announcing Security Risks)

When system administrator Bret McDanel discovered in 2000 that his former employer, Tornado Development, was continuing to advertise a "secure" email service that had a significant vulnerability and a service that the former employer refused to fix, he decided to act. First, he approached his superiors within the company about the security flaws. However, they ignored his warnings. Then, after he left the company, he retained use of his company e-mail account. He used that account to contact users who were customers of Tornado Development telling them about the vulnerability and directed them to his own website for information about the vulnerability. McDanel was not only prosecuted, but he was also convicted and served 16 months in jail. It was only after his jail term that the Department of Justice conceded that the conviction was wrongful (Rasch, 2013).

In this situation, an approach in reducing legal risk would come in different forms for both the company (Tornado Development) and the former employee (McDanel). Tornado

© 2017 The SANS Institute Author retains full rights.

Development should have documented McDanel's findings, suggestions, and their response to them. This way, the company could prove that they were pursing due care of the security of the email service. In addition, the company should have reduced both of its security and legal risks by closing McDanel's e-mail account as soon as he left the firm since he should not be using Tornado Development's resources at that point. In turn, McDanel should have not used his former company's e-mail account since he put himself at legal risk since the company can make the case that he could be misrepresenting himself as a current company employee to the customers. He should have preserved the evidence and shared it with the media instead of sending e-mails to the customers. It would have promoted his argument that he was serving in the role of being a whistle blower.

5.0 Conclusion

Even when facts are nearly identical, different judges and prosecutors do not always interpret the laws in the same way. Security professionals and enterprises should use caution and should follow the suggestions above to reduce legal risks. Specifically, personnel and enterprises conducting scanning should get prior written authorization to scan the networks or systems of other people or enterprises. The parties who sign the authorization must clearly state as to how the scanning will be done, as well as specific roles and responsibilities. There should be precise protocols on how scanning results should be handling, especially if a potential legal case can be foreseen. As case law develops over time concerning this topic, one can safely predict that written authorization to conduct scanning will become more detailed and precisely worded. Finally, training for security professionals in how to conduct scanning and preserve the results as legal evidence will be more extensive as risks become better known as well as the body of how to conduct scanning.

© 2017 The SANS Institute Author retains full rights.

Often, the cases cited in this paper were early cases in jurisdictions not used to dealing in cyber law. Both the people scanning and law enforcement personnel had to learn the hard way about the legal implications of scanning and managing their legal risks. Hopefully, in the future, knowledge about how to properly conduct scanning activities and handling the results will be more commonplace.

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

References

Associated Press (1995). *Designer of Satan Software Gets New Job.* Retrieved December 10, 2016 from http://www.apnewsarchive.com/1995/Designer-of-Satan-Software-Gets-New-Job/id-fc57bd48d1ff215be9b289cf4a9a0395

BeyondTrust (2012). *BeyondTrust Acquires Vulnerability Management Pioneer eEye Digital Security.* Retrieved December 14, 2016 from https://www.beyondtrust.com/resources/press-release/beyondtrust-acquires-vulnerability-management-pioneer-eeye-digital-security/.

Farmer, D. and Venema, W. (1993) *Improving the Security of Your Site by Breaking Into it.* Retrieved December 10. 2016, from http://www.porcupine.org/satan/admin-guide-to-cracking.html

IBM Internet Security Systems (2007) *ISS Overview.* Retrieved December 10. 2016, from http://web.archive.org/web/20070521190031/http:/www.iss.net/about/index.html.

LaMonica, M. (2007). IBM to Buy ISS for $1.3 Billion. *CNET.* Retrieved December 16, 2016 from https://www.cnet.com/news/ibm-to-buy-iss-for-1-3-billion/.

Lindros, K. and Tittel, E. (2014). How to Choose the Best Vulnerability Scanning Tool for Your Business. *CIO Magazine.* Retrieved December 16, 2016 from http://www.cio.com/article/2683235/security0/how-to-choose-the-best-vulnerability-scanning-tool-for-your-business.html

Lyon, G. (2012) The History and Future of Nmap. *Nmap.org.* Retrieved December 12, 2016 from https://nmap.org/book/history-future.html.

Lyon, G. (2008) Legal Issues. *Nmap.org.* Retrieved December 20, 2016, from https://nmap.org/book/legal-issues.html.

Myers, M. (2016). Navy Strike Group Commander Fired for Viewing Porn at Work. *Navy Times.* Retrieved November 28, 2016, from https://www.navytimes.com/story/military/2016/01/09/navy-strike-group-commander-fired-viewing-porn-work/78512588/.

National Institute of Science and Technology (NIST) (2016) *FISMA – Detailed Overview.* Retrieved December 1, 2016, from http://csrc.nist.gov/groups/SMA/fisma/overview.html.

National Institute of Science and Technology (NIST) Special Publication (NIST SP) 800-37, Revision 1 (2014) *Guide for Applying the Risk Management Framework to Federal Information Systems.* Retrieved Dec 3, 2016 from http://csrc.nist.gov/publications/nistpubs/ 800-37-rev1/sp800-37-rev1-final.pdf.

© 2017 The SANS Institute Author retains full rights.

Nilsson, J. (2006) Vulnerability Scanners (Note: This is a Master of Science Thesis at the Royal Institute of Technology in Stockholm, Sweden). Retrieved Dec 19, 2016, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7785&rep=rep1&type=pdf.

Office of Management and Budget (OMB) (2006) *FY 2005 Report to Congress on Implementation of The Federal Information Security Management Act of 2002.* Retrieved December 3, 2016, from https://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/reports/2005_fisma_report_to_congress.pdf.

Payment Card Industry (PCI) Security Standards Council (SSC) (2010) *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 2.0.* Retrieved December 4, 2016, from https://www.pcisecuritystandards.org/documents/ PCI%20SSC%20Quick%20Reference%20Guide.pdf.

Piper, S. (2013). Understanding Vulnerability Management. *Definite Guide to Next-Generation Vulnerability Management*. Retrieved December 13, 2016, from http://stevepiper.com/definitive-guide-to-ngvm/.

Rasch, M (2013) Legal Issues in Penetration Testing. *SecurityCurrent Magazine.* Retrieved December 20, 2016 from http://www.securitycurrent.com/en/analysis/ac_analysis/legal-issues-in-penetration-testing.

State of Minnesota Office of the Rivisor of Statues (2007) *Minnesota Session Laws - CHAPTER 108--H.F.No. 1758.* Retrieved December 6, 2016 from https://www.revisor.mn.gov/laws/?id=108&year=2007.

State of Nevada, State Legislature (2015) *Nevada Revised Statutes, Chap. 603A §215.* Retrieved December 6, 2016, from http://www.leg.state.nv.us/nrs/nrs-603a.html# html#NRS603ASec010.

State of Washington, State Legislature (2011) *Washington Revised Code § 19.255.020.* Retrieved December 6, 2016, from http://apps.leg.wa.gov/rcw/default.aspx?cite =19.255.010.

Steel, J. (2016). Admiral is Removed after Investigation Finds He Watched Hours of Porn on Work Computer. *Los Angeles Times.* Retrieved November 29, 2016, from http://www.latimes.com/local/lanow/la-me-ln-admiral-removed-online-pornography - 20160311-story.html.

Stephenson, P. (2010) Penetration Testing: SAINT. *SC Magazine.* Retrieved December 14, 2016, from http://www.saintcorporation.com/wp-content/uploads/ 2016/07/ SAINT_SCinnovator.pdf.

© 2017 The SANS Institute Author retains full rights.