GIAC
CERTIFICATIONS

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.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The Ethics and Legality of Port Scanning:

GSEC Practical Assignment v1.2f
Shaun Jamieson
October 8, 2001

Port scanning is an ideological ambiguity within the computer industry. While usually considered malicious, port scanning is often used by system administrators to diagnose problems on their own network. While most private organizations prohibit the activity, there are currently no state or federal laws that specifically address it. This paper will define and outline the process of port scanning, discuss ethical and legal issues surrounding port scanning, and assert the importance of strictly defining scanning in an organization's policy.

Overview: Definition and Process

Port scanning is a simple process by which a connection is attempted to a range of ports on a range of hosts. The information gathered from the responding ports is used to determine which ports are open and which services are running on those ports. The SANS Intrusion Detection FAQ says, "Port scanning is like ringing the doorbell to see whether someone's at home."[2] TechTarget's searchSecurity.com website defines port scanning as the following:

> *A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.*
> *Types of port scans include:*
>
> - *Vanilla - An attempt to connect to all ports (there are 65,536)*
> - *Strobe - An attempt to connect to only selected ports (typically, under 20)*
> - *Stealth scan - Several techniques for scanning that attempt to prevent the request for connection*

© SANS Institute 2000 - 2005 Author retains full rights.

being logged

- *FTP Bounce Scan - Attempts that are directed through an File Transfer Protocol server to disguise the cracker's location*
- *Fragmented Packets - Scans by sending packet fragments that can get through simple packet filters in a firewall*
- *UDP - Scans for open User Datagram Protocol ports*
- *Sweep - Scans the same port on a number of computers*

[4]

Port scanning is one of the most fundamental techniques that a hacker can use to begin an attack. Many systems can reveal vast amounts of information from being scanned. An attacker can find out a wide variety of information such as services you are running, what versions of those services you are running, and even what operating system the host uses. In many cases, information revealed during a port scan can leave a system highly vulnerable to an attacker.

Port scanning is nearly always considered malicious because of this ability for it to be exploited. Industry professionals consider port scanning an invasive activity that violates the target machine.

Ethics and Legality:

Whether or not scanning is ethical is a delicate tricky question. While scanning is widely held to be a malicious activity, professionals use the technique regularly to diagnose network problems and to detect vulnerabilities on their own network. The legitimacy of a port scan is often determined by the circumstances surrounding the incident in an attempt to establish intent.

A scan is not an attack. In the vast majority of instances, a scan does not cause any damage to its target system. How can an activity that is so passive and non-harmful be considered malicious? While a scan is not any more destructive than "ringing the doorbell to see whether someone's at home,"[2] it is a highly invasive activity. The information taken from a scan can often leave the target system violated and therefore vulnerable. A scan is considered malicious when the intent is to reveal vulnerabilities in the target. Looking for a port of a well-

© SANS Institute 2000 - 2005, Author retains full rights.

known Trojan such as back orifice or subseven is an example of a type of scan that would be clearly malicious. Jim Moore, Security Officer at Rochester Institute of Technology points out another difficulty in determining if a motive is malicious: "Also with the advent of Code Red and Nimda, it is becoming more difficult to distinguish automated scans from worms, from automated scans from people."[6] New viruses perform malicious scans without the knowledge of the user. This establishes yet another ambiguity in trying to determine whether the clearly malicious scan was intentional or the act of a virus.

One of the most powerful tools available to a system administrator in securing a host is the very knowledge that an attacker is attempting to find in a port scan. This makes scanning an invaluable tool for system administrators. In spite of this fact, many individuals have lost their jobs over scanning. The line between scanning maliciously and scanning for administrative purposes is so vague that individuals with benevolent intent have lost jobs because of perceived misconduct.

The evaluation of the intent behind a scan is at best an imperfect science. This makes dealing with scanning in policies difficult and creating laws regarding it nearly impossible.

Law enforcement loosely attempts to address such issues in basic computer crime laws, though scanning is never specifically addressed. Some courts seem to have declared port scanning legal altogether. In the Georgia District Court case of "Moulton v. VC3," the judge declared a port scan in the case legal because it did not "impair the integrity nor availability of the network."[3] The judge found that since the activity performed no damage to the target, it could not be illegal.

Organizations have more ability to enforce this issue than governments. Organizational policies have the luxury of being able to identify specific rights/authorities of specific individuals. This allows an organization to establish exactly who is allowed to scan exactly which systems. Addressing specifics of scanning in a policy is important to extinguish vagaries in authority that can cause issues later. Organizations can also dictate within policy measures for dealing with people who attack other computers

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

from within the organization.

Violations unrelated to organizational duties become more difficult to develop a policy for. Large broadband ISPs are attempting to address such issues in their terms of service. DNSOnline, an ISP in Plymouth, IN, addresses scanning in their Acceptable Use Policy as follows:

> *a. Port Scanning*
>
> *Port Scanning of any DNS computer will be considered a preliminary to a hacking attempt and is therefore expressly forbidden. DNS will immediately terminate the account of any Customer found to be port scanning the DNS system. A first-time offender will be allowed to reopen an account with DNS only after paying a reconnect fee of $50.00. Repeat offenders will not be allowed to reopen an account with DNS; moreover, their names and account status will be posted on a DNS web page for area residents and other ISPs to check.[1]*

While addressing the penalty for scanning their computers, the ISP avoids responsibility for their users actions on third parties. The issue of the third party becomes particularly important in instances of residential organizations. Specifically, individual users on university campuses are often one of the largest groups of violators. How should an educational institution, often responsible for discipline, deal with such ambiguous computer violations? Most universities at the very least provide penalties for violations against their own computers. The Code of Conduct for Computer Use at Rochester Institute of Technology shows no specific mention of scanning. The document does state:

> *8. You must not bypass accounting or security mechanisms or attempt to circumvent data-protection schemes or uncover security loopholes. You must not exploit systems' weaknesses. You must not attempt to modify Institute software, except that intended to be user-customized, without express permission of the systems administrator. [7]*

This would allow port scanning to be penalized under the pretense that it is attempting to uncover security loopholes. Jim Moore says that the policy, "could [be] more clear, and we are working to that end."[6]

© SANS Institute 2000 - 2005 Author retains full rights.

Universities, unlike ISPs, do have the luxury of a judicial and disciplinary process. Even with such luxuries, many educational institutions still have difficulties enforcing such a vague violation.

One solution offered in both residential realms and ISPs is that of user education. Rather than trying to prevent scans and punish them after the fact, people should be educated to a level of security awareness that makes the effect of scanning negligible. On the RIT campus, Moore is working to this end as one means of reaching a solution: "I am going to start a couple of groups on campus on 'personal information security'."[6] Many large ISPs have also started distributing personal firewall software with subscriptions. Earthlink Internet was one of the first providers to start offering this. Users of America Online are often protected from Internet attackers from sophisticated routing and proxies.

Conclusion:

Port scanning is still a fuzzy subject. While clearly the first step in a successful attack, it possesses no damaging payload. In many cases, the scan can be benevolent in nature. Governmental and legal institutions have only begun to deal with issues of computer crime and port scanning is vague enough to slip past many laws. Organizational policies have started to struggle with the issue with some success. As attacks increase, it becomes more important for organizations to protect themselves against attacks to attempt prevention of violations from their members. More clarity is needed in many policies pertaining to individual authority to conduct scans. Ultimately, the effect of port scanning will only be minimized when it is fought on both fronts. In addition to efforts being made to prevent and punish the action, guidelines need to be established for its acceptability. At the same time, users need to be educated to protect themselves from both being scanned and becoming the unwilling victim of scanning worms. Establishing guidelines for proper scanning activity and implementing them into policies is an important and difficult task that needs to be performed by the Information Security community.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Sources:

1. Author DNSOnline, "Acceptable Use Policy",URL: http://www.dnsonline.net/pol3.htm (Access Date: 10/10/01).
2. Author SANS, "SANS Intrustion Detection FAQ", URL: http://www.sans.org/newlook/resources/IDFAQ/port_scanning_legal.htm (Access Date: 10/10/01).
3. Thrash, Thomas W. Jr., "Moulton v. VC3", URL: http://pub.bna.com/eclr/00434.htm (Access Date: 10/10/01).
4. Author TechTarget.com, "port scan – a searchSecurity definition", URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214054,00.html (Access Date: 10/10/01).
5. Malda, Rob, "Judge Says Port Scanning is Legal", URL: http://slashdot.org/articles/00/12/19/149227.shtml (Access Date: 10/10/01).
6. Moore, Jim. Security Officer, Rochester Institute of Technology, 10/08/01, (personal interview).
7. Author RIT, "Code of Conduct for Computer Use", URL: http://www.rit.edu/~620www/Manual/sectionC/C8.html (Access Date: 10/10/01)

© SANS Institute 2000 - 2005 Author retains full rights.