Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
SANS Practical assignment Version 1.4b – Option 1
Submitted by: Chris Peake
Date: July 16, 2003
Version 1.0

Red Teaming: The Art of Ethical Hacking

By 2003, our economy and national security became fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy—energy (electric power, oil and gas), transportation (rail, air, merchant marine), finance and banking, information and telecommunications, public health, emergency services, water, chemical, defense industrial base, food, agriculture, and postal and shipping. The reach of these computer networks exceeds the bounds of cyberspace. They also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars… A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security… Cyber attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures. - The National Strategy to Secure Cyberspace[1]

> ***security: 1.*** *A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. [JP1]* ***2.*** *With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. [After JP1]* ***3.*** *Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. [JP1] – www.atis.org*[2]

INTRODUCTION

The term "hacker" was initially used for skilled computer enthusiasts that could "hack" their way through technical problems. Today, hackers pose one of the principal threats against our information infrastructure by exploiting vulnerabilities in code and circumventing security measures. Hacking uses a wide variety of techniques with differing intentions and objectives. And in order for security professionals to protect against this threat, we must assess the security of our networks from the perspective of the attacker.

Red Teaming is a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access. This process is also called "ethical hacking" since its ultimate purpose is

[1] "The National Strategy to Secure Cyberspace." February 2003. pg 6 - http://www.whitehouse.gov/pcipb/
[2] Telecom Glossary 2000. Alliance for Telecommunications Industry Solutions. - http://www.atis.org/tg2k/_security.html

to enhance security. Ethical hacking is an "art" in the sense that the "artist" must posses the skills and knowledge of a potential attacker (to imitate an attack) and the resources with which to mitigate the vulnerabilities used by attackers.

Although this paper discusses the methodology and tools used to perform Red Teaming, its purpose is to discusses the overall role of Red Teaming in evaluating a system's/network's security posture. The paper does not intend to be a "how-to" guide to Red Teaming, rather it justifies the need for such methods to provide an accurate situational awareness for network/system security.

BACKGROUND

> *"Information security is a mindset of examining the network's threats and vulnerabilities and managing risk appropriately." – Eric Maiwald*[3]

Information security (Infosec) is the fastest growing area in the Information Technology (IT) industry. Security would be an easy process if all that had to be done is to install a firewall and anti-virus software, but the reality is that securing information requires a multi-layered approach.

> *The Computer Security Institute (CSI) reported that 90% of survey respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months. 80% of these companies acknowledge significant, measurable financial loss as a result of these breaches. - eEye Digital Security Whitepaper*[4]

Information attacks come from all angles and with multiple intentions. Companies are no longer just at risk of being attacked/hacked but are also legally responsible for "allowing" their resources to be utilized by hackers to attack other companies (downstream liability). Good information security is a combination of physical security, communication security, emission security, computer security and network security. Obtaining this requires adopting measures to prevent the unauthorized use, misuse, modification or denial of use of knowledge, facts, data, or capabilities and it requires taking a proactive approach to managing risk (threat + vulnerability = risk).

To assist in managing this risk, there are many kinds of Infosec professionals. Two growing fields of these professionals are Red Teams and Blue Teams. Red Teaming is the process of analyzing vulnerabilities on a given system or network by modeling the actions of an adversary. Blue Teaming has the same goals of the red team but functions as a defender that works with those responsible for the network or system operation to mitigate risk. Both of these approaches only identify known vulnerabilities on systems and do not address the requirements for an overarching security infrastructure.

---

[3] Maiwald, Eric. Network Security: A Beginner's Guide. 2002. pg

[4] **eEye Digital Security Whitepaper, "**The Need for Vulnerability Assessment & Remediation: What My CIO Needs to Know." 2003. pg 2.

Recent changes in the business, regulatory and IT environments are increasing the need for comprehensive, enterprise-wide business continuity planning that includes IT practices and processes... A series of legislative and regulatory initiatives - including the Graham-Leach-Bliley Financial Services Modernization Act, the Healthcare Information Portability and Accountability Act (HIPAA) and the European Data Privacy Directive - demands better execution in the areas of security and privacy, and raises the legal and financial stakes for enterprises that fail to meet their standards. These changes in the business, regulatory and IT environments also are increasing the need for comprehensive, enterprise-wide business continuity planning that includes IT practices and processes. - Nicolett[5]

Infosec Infrastructure

Infosec consists of much more than security equipment (firewalls, Intrusion Detection System [IDS], Syslog, etc.) it is a process. Two significant components of Infosec infrastructure are policy and personnel. Security policies not only set the guidelines for employee and company behavior but also define the processes and procedures necessary for implementing, updating and managing security. These policies are only as effective as the security professionals who implement and maintain them.

For example, most companies currently maintain a computer use policy of some kind. The policy outlines what employees are allowed and prohibited to do on company-provided equipment/computer resources. Although the policy is designed to protect both the company and user, it is only effective if the users are aware of the policy and the company enforces it. Therefore, a good policy must also have an implementer (a security team or department).

In order to provide complete information security services, an organization should have at least the following security policies:

- Information policy
- Security policy
- Computer use
- User management
- System Administration (SysAdmin) procedures
- Incident response procedures
- Configuration management
- Design methodology
- Disaster recovery plans

To support these policies, an organizational structure for the information security professionals in the company or organization also needs to be defined. This often leads to appointing a security officer and security managers (for sites, divisions, or departments) to manage security policies and practices.

Infosec Methodology

The proactive approach to information security identifies vulnerabilities and determines risk and then defines the appropriate countermeasures (as a

[5] Nicolett, Mark (VP, Research Director). "Managing IT Security Risk in a Dangerous World", CSO. - http://www.csoonline.com/analyst/report1332.html

preventative measure to attacks). Infosec is based on the premise of risk management. In order to manage risk, keeping in mind that risk = threat + vulnerability, both threats and vulnerabilities must be identified. Until the current state of risk can be identified it is impossible to implement the appropriate security measures to protect the assets.

Threat and vulnerability assessment is a process that includes system-level vulnerability assessment, network-level risk assessment, organization-wide risk assessment, auditing and penetration testing. These assessments require employee interviews, existing policy reviews and physical inspections. The assessment is an in-depth technical analysis of the information system. In order to perform the assessment, the security assessors must know and understand existing vulnerabilities for multiple systems and have the tools to test for the presence of these vulnerabilities.

An effective assessment tests information confidentiality, integrity, availability, accountability, identification/authentication, and audit services. Identified risks in each area will be managed according to the value the company/organization places on the information. Risk is rated as low, medium or high and to be valuable, risk assessment must identify the costs (time, money, loss of productivity etc.) to the organization if an attack is successful.

Implementing Security Measures

> ***information systems security (INFOSEC and/or ISS):*** *[The] protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [INFOSEC] – www.atis.org*[6]

The principal challenge information security professionals face is implementation of risk mitigation strategies. Vulnerabilities are identified faster than policies can be modified or necessary changes can be completely tested (prior to implementation). However, general security measures can be adopted to manage unknown or unidentified risks.

For example, disaster recovery plans are often cumbersome documents due to the wide range of possible "disasters" they encompass. Effective plans address natural disasters, directed attacks, as well as accidental events. Risks can be minimized if proper procedures are in place when unplanned events occur. The development of an Incident Response Team/Incident Response Plan (IRT/IRP) guides the organization on how to react when a security event takes place. The primary purpose of these procedures is to plan for the unplanned.

Most security professionals focus on identifying vulnerabilities for specific systems rather than implementing security measures for universal threats. Past

[6] "Telecom Glossary 2000". Alliance for Telecommunications Industry Solutions. - http://www.atis.org/tg2k/_information_systems_security.html

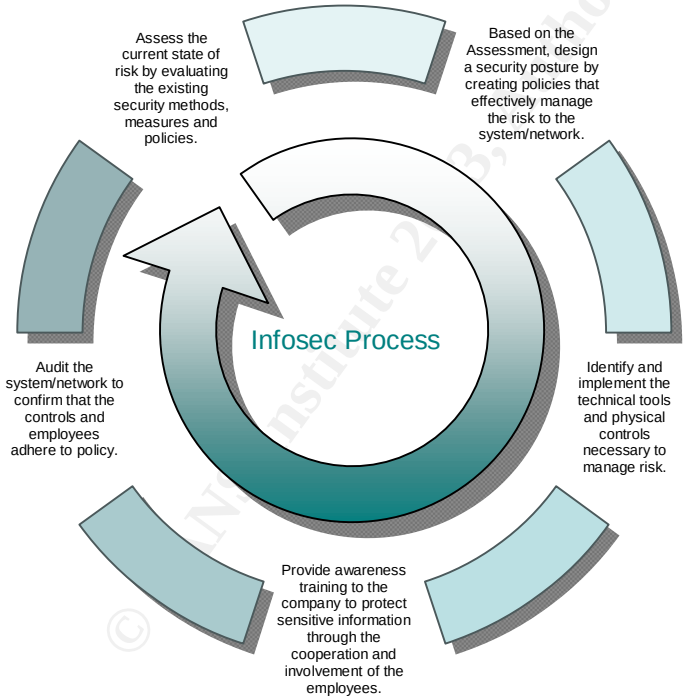
incidents infecting networks, like the infamous "love bug" virus[7], were financially devastating to many companies because they did not have a planned response after realizing their networks were under attack. Information security professionals can help their clients develop these procedures and provide preventative information security measures to protect against future attacks.

> *Nimda, we were told by articles quoting Computer Economics, cost companies $635 million in clean-up and lost productivity. The total sum for the various versions of Code Red was $2.62 billion, SirCam leeched $1.15 billion out of corporate coffers, and the unlovely Love Bug cost $8.75 billion to exterminate. - Delio[8]*

The Role of Red Teaming in Infosec

Red Teaming is just one component of the evaluation of a network's/system's overall security. As stated above, information security is a mindset and a revolving process. This is partially due to the dynamics of the IT industry but also due in part to the continuous discovery of new exploits and vulnerabilities in code. Staying up to date with these vulnerabilities is a full-time job and therefore, so is the field of Infosec.

The Infosec process looks like this:



© Chris Peake, 2003

[7] "CERT® Advisory CA-2000-04 Love Letter Worm", CERT Coordination Center. May 2000 - http://www.cert.org/advisories/CA-2000-04.html

[8] Delio, Michelle. "Find the Cost of (Virus) Freedom" Wired News - http://www.wired.com/news/infostructure/0,1377,49681,00.html

Following the Infosec process does not guarantee protection; it provides guidelines security professionals can take to manage the risk to systems and networks. The process must balance the three principal Infosec services (confidentiality, integrity and availability) without compromising one to protect another.

Red Teaming falls under the assessment stage of the Infosec process. Security professionals have to determine the risk to the system/network before the appropriate security controls can be implemented. To determine risk, vulnerabilities and threats must be identified. The Red Team uses tools to probe for vulnerabilities and can project possible threats based on the scope of the assessment requested by the customer. However, the Red Teaming approach is more in-depth than what most potential attackers follow because those attempting to circumvent security only need to find a single vulnerability, while security professionals need to find all possible vulnerabilities for a given system in order to assess the associated risk. Attackers typically only target a single vulnerability for a specific exploit; to do otherwise would increase the possibility for detection (the more time spent and vulnerabilities probed, the more likely the attacker's actions will be noticed). Nevertheless, Red Teaming should test for all types of attacks (access, modification, denial of service, and repudiation) to provide a complete security assessment.

A thorough Red Team assessment should provide an accurate situational awareness of the security posture of a given system/network. But identifying risk through Red Teaming and other methods cannot provide information security alone; the company/organization must continue through the Infosec process in order to appropriately manage risk and provide security protection.

TOOLS AND METHODS OF RED TEAMING

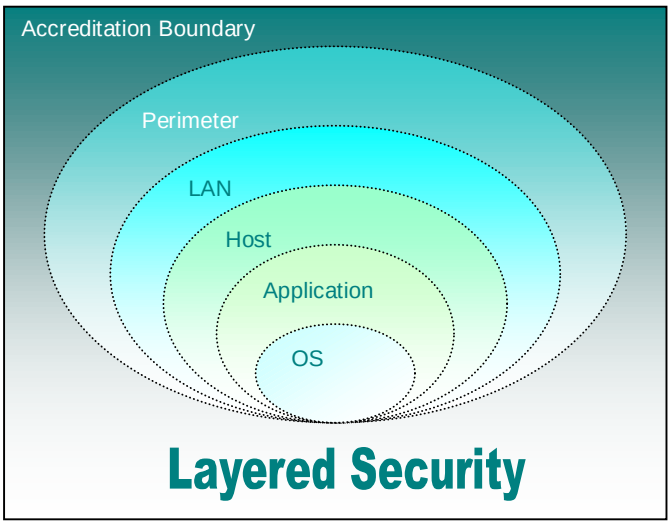
> ***risk analysis: 1.*** *A systematic method of identifying the assets of a data processing system, the threats to those assets, and the vulnerability of the system to those threats. [2382-pt.8]* ***2.*** *In COMSEC (communications security), an organized method of estimating or calculating the probability of compromise. [After X9.49]* ***3.*** *Synonym [in INFOSEC]* ***risk assessment. –*** *www.atis.org*[9]

A Red Team assessment evaluates various areas of security in a multi-layered approach. Each area of security defines how the target (system/network) will be assessed. Following the concept of Defense in Depth[10], the target must be tested at each layer of possible intrusion/attack.

The layered approach of Defense in Depth:

[9] "Telecom Glossary 2000". Alliance for Telecommunications Industry Solutions. - http://www.atis.org/tg2k/_risk_analysis.html

[10] Batongbacal, Mike (Developer Solution Specialist). "Security and eGovernment." April 2003. Microsoft - www.microsoft.com/usa/presentations/DD.ppt



© Chris Peake, 2003

This concept of layered security involves implementation of security controls at each layer. An identified vulnerability at one layer may be protected at another layer minimizing the associated risk of the vulnerability. The Red Team tests policy compliance of the security controls at each layer. And the control is tested in a manner specific to the area of security to which it applies. The following table lists the vulnerability assessment testing areas.

Vulnerability Assessment Testing Areas:[11]

Internet Security • Network Surveying • Port Scanning • System Identification • Services Identification • Vulnerability Research • Internet Application Testing • Router Testing • Firewall Testing • Intrusion Detection System Testing • Trusted Systems Testing • Password Cracking • Denial of Service Testing • Containment Measures Testing	**Information Security** • Document Grinding • Competitive Intelligence Scouting • Privacy Review **Social Engineering** • Request Testing • Guided Suggestion Testing • Trust Testing **Wireless Security** • Wireless Network Testing • Cordless Communications Testing • Privacy Review • Infrared Systems Testing
Communications Security • PBX Testing • Voicemail Testing • FAX Review • Modem Testing	**Physical Security** • Access Controls Testing • Perimeter Review • Monitoring Review • Alarm Response Testing • Location Review • Environment Review

Each of the vulnerability testing areas uses unique methodology and tools to evaluate the level of risk. Regardless of the methodology used, the Red Teaming process is standardized throughout the assessment.

[11] Herzog, Pete. "OSSTMM," Version 2.0, Feb 2002. Pg 13.

The Red Teaming Process

There is an overarching methodology or process to perform Red Teaming assessments. As stated in the title of this paper, Red Teaming is "ethical hacking". As such, it must be carried out with the utmost confidentiality, discretion, and clarity.

Typically, Red Teams are third-party entities hired to make an impartial assessment of the network or system. The customer sets the scope of the project to specify the area of information to be assessed. Before the Red Team can proceed, several legal considerations must be addressed. The team must have explicit and direct permission to perform the test from the customer. This should also include a waiver of repercussions in the event a disaster should occur in the process of testing. The Red Team is responsible for supplying the customer with a detailed plan as well as a list of methods and tools that will be used during the evaluation. Any testing performed outside the scope stated by the customer, can be considered an unwarranted attack by the Red Team. The customer maintains all rights to proprietary data and information and at no time should the Red Team purposefully destabilize the confidentiality or availability of that information.

Jessica Lowery's paper "Penetration Testing: The Third Party Hacker"[12], discusses many of the reasons to outsource security assessments. Most importantly, outsourcing demonstrates an unbiased assessment of a company's security to its clientele. The paper also outlines some of the pitfalls or cautions companies need to consider when hiring a Red Team. Companies should make sure that the Red Team is insured and will allow the company oversight during the tests. Companies need to be cautious when outsourcing security assessments; the right team can greatly benefit the security efforts of the company while the wrong team can potentially cause great damage to security, reputation and IT infrastructure.

The Open-Source Security Testing Methodology Manual (OSSTMM)[13] by Pete Herzog is a thorough and well-recognized document describing the security testing process.

> *The concept of this manual has and always will be to create one accepted method for performing a thorough security test. Regardless of the credentials of the security tester, the size of the security firm, financing, or vendor backing, any network or security expert who meets the outline requirements in this manual is said to have completed a successful security scattershot… The tester following the methodology within this manual is said to have followed the standard model and therefore if nothing else, has been thorough. – OSSTMM*[14]

The process expands on the vulnerability testing areas and explains the desired results from assessing each area. The OSSTMM also provides a project timeline

[12] Lowery, Jessica. "Penetration Testing: The Third Party Hacker", SANS GIAC practical Exam - http://www.sans.org/rr/paper.php?id=264
[13] Herzog, Pete. "OSSTMM," Version 2.0, Feb 2002.
[14] Herzog, Pete. "OSSTMM," Version 2.0, Feb 2002. Pg 5.

and recommends tools to test for various vulnerabilities. More importantly, it introduces the idea of Risk Assessment Values (RAVs).

> *This manual introduces Risk Assessment Values (RAVs) which will aid in the clarification of this scattershot by quantifying the risk level and allowing for specific tests within specific time periods to cycle and minimize the amount of risk one takes in any defensive posture. – OSSTMM*[15]

Risk must be a measurable or identifiable value to distinguish the severity of the risk. Although risk can be identified as high, medium or low, Herzog explains that a risk assessment is only a snapshot of the vulnerabilities and configuration at a single moment in time. The dynamic elements of the network/system can affect the severity of an individual risk. So the OSSTMM aids security professionals in defining the most severe areas of risk and determining the most effective means to manage risk.

Red Teaming Methodology

The most important requirement for red teaming is customer consent. Because, by definition and purpose, the Red Team takes an attacker-like approach to testing security, to begin an assessment without explicit permission is legally perceived as an unwarranted attack on the system/network. This being said, many Red Team evaluations are purposefully kept from network and system administrators as a means of testing personnel response to security events or to test IDS or IRP. Consent must come from the security stakeholders and decision-makers. Legal counsel may also be involved on both sides for definition of testing scope and adherence to process and confidentiality.

The scope of the Red Teaming assessment can be very general or very specific when defining what the assessment will include or address. The scope of the project depends on time or cost of the assessment and/or on the objective of the assessment as defined by the customer. It may not be financially feasible to assess the security of the entire network/system (due to the time needed to perform the assessment, physical size of the system/network or number of services requiring an assessment) so the customer can limit the scope of the project. For example, if a company is performing a Red Team assessment as part of an annual security audit, they may only choose to test one segment of the network's/system's security (i.e. Internet security, wireless security, social engineering, etc.). The scope will also help define the depth of testing and, to some degree, the expected results. The customer can request a verification of data integrity without checking availability or test confidentiality without accountability. So the results of the Red Team assessment will be tailored to the customer's objectives.

Red Teaming is commonly mistaken as just penetration testing (pen-testing) when in fact, pen-testing is a component of the Red Teaming assessment. Pen-testing uses various methods and tools to gain access, obtain information or to cause damage to a network/system by probing for known vulnerabilities. Pen-

[15] Herzog, Pete. "OSSTMM," Version 2.0, Feb 2002. Pg 5.

testing tests implementation while Red Teaming tests design. By description, pen-testing is an external detailed analysis of a network and associated systems from the perspective of a potential attacker. This method of security testing is useful in the Red Teaming process to test for backdoors and un-patched vulnerabilities. But pen-testing cannot provide a complete security analysis alone. If a system/network is penetrated, the test proves that there is at least one vulnerability that can be used to gain access to the system/network. And if the pen-test was unsuccessful, the test only proves that the person performing the pen-test was unable to find any exploits in the system (it does not guarantee that there are vulnerabilities are not present).

A good rule of thumb for companies to follow when planning Red Team assessments is to identify the weakest areas or the "low-hanging-fruit" and have these areas tested for vulnerabilities. As stated earlier, hackers will target a specific vulnerability to gain access (rather than numerous) to avoid detection. For example, the infamous SQLSlammer[16] worm used a single vulnerability in Microsoft SQL server to infect thousands of computers connected to the Internet. So any database using SQL as a backend could be a target (e.g. a low-hanging fruit).

Ethical hacking must strictly follow pre-approved testing guidelines that are established with the customer. The team must also document all the steps/procedures in testing in order to retrace the team's actions in case of an incident due to testing or for retesting/verification of results if necessary. Upon completion of the Red Teaming effort all results should be submitted to the customer in a final report detailing the vulnerabilities that were discovered and how each was discovered. The report should also make an assessment of the overall level of risk of the network/system in addition to the risk level of each vulnerability. The final report is as important as the testing itself because it will direct the customer to take additional security steps.

Red Teaming Tools and Tricks of the Trade

The ethical hacker is equipped with an extensive toolkit comprised of software, hardware, and technical expertise. The true skill in Red Teaming is knowing how to use these tools and honing the techniques of testing a network's/system's security. Each vulnerability assessment area requires specific tools to inspect the security configuration. The Red Team may have experts in each of these areas. For instance, the skills needed to test for social engineering vulnerabilities are very different from those needed to test communication security. So the team will be made up of several accomplished individuals who are specialists in some of the following areas:

- Developing the Hacker's Mind
- Port Scanning
- Network Surveying

[16] CERT® Advisory CA-2003-04 MS-SQL Server Worm. CERT Coordination Center. January 2003. - http://www.cert.org/advisories/CA-2003-04.html

- System Identification / OS Fingerprinting
- Vulnerability Research and Verification (automated and manual)
- Service Identification
- Internet Application Testing
- Document Grinding (electronic dumpster diving)
- Recognizing security issues within an organization
- Perform legal assessments on remote / foreign networks
- Examining an organization for weaknesses as through the eyes of an industrial spy or a competitor
- Implementing the right tools for each task in security testing
- Competitive Intelligence
- Exploiting vulnerabilities remotely / exploit research
- Determining appropriate countermeasures to thwart malicious hacking
- Firewall & ACL Testing
- IDS testing
- Social engineering
- Trusted systems testing
- Password cracking
- Denial of Service (DoS) testing

These efforts combined will provide the overall security assessment that is Red Teaming.

There are literally hundreds of tools both software and hardware that can be used to assess different aspects of security. Although these tools are typically considered "hacking tools", the reality is the most of them were developed to assist network administrators and security administrators to detect and fix vulnerabilities rather than exploit them. Many of the tools used by security professionals are open-source and available for download on the Internet. However, there are some very powerful tools developed by leading software companies that are highly effective for detecting vulnerabilities which also include report generation capabilities that are beneficial to Red Teams when providing results to customers (these tools cost several thousand dollars and are not used by the "casual hacker").

The OSSTMM has a very comprehensive list of software-based operational tools used for network security[17]. ISECOM separates these tools into functional areas for security assessments. Security professionals typically use one or two tools for each given task because the test objective differs slightly depending on which tool is used. But essentially tool choice comes down to personal preference. Tool selection should also be based on the projected attacker (this would be determined through threat analysis). The Red Team effort should simulate an attack from a potential attacker. If the customer's network/system is a target for a competing company that has healthy financial resources, a more elaborate tool

[17] ISECOM OSSTMM list of tools. http://www.ideahamster.org/projects/operationaltools.htm

may be used to gain access. The casual hacker looking for a vulnerable system would probably use publicly available tools.

Fluke Corporation[18] has a collection of hardware network testing and troubleshooting products. These products are expensive and require physical access to a network but can literally analyze all communications on a given network or system. Sinffer Pro, by Sniffer Technologies, is a multifunctional network sniffer that also has complete security analysis capabilities. But for just under $8,000 it is not readily accessible for the average attacker. Tools of this caliber would typically be used in the Blue Teaming environment where security professionals have direct access to the network/system being analyzed.

Timothy Layton's SANS paper titled *"Penetration Studies – A Technical Overview"*[19] discusses some of the tools used for pen-testing that are freely accessible on the Internet. These tools use basic network functionality as a means of obtaining information about the target which can be use to compromise the target. Basic Internet services like whois, ARIN, and nslookup can tell a great deal about a target without illegal network probing. Additionally, the paper describes how to use some of these tools and demonstrates some of the expected results.

Another extremely powerful tool is the Internet search engine. Yahoo!, AltaVista, Lycos, Dogpile, and, of course, Google have already done most of the work for us in locating bits of information about any target. Every bit of information accessible on the Internet can be used to profile the target. Attackers can use this profile to tailor their approach to gain access. By directing a Google query to search for specific information on a specific site, the search engine becomes a tool to scour a target's website for employee names, phone numbers, email addresses, computer host names, internal resources and even passwords. In a paper entitled *"Google-Knowledge: Exposing Sensitive Data with Google"*[20], the author explains how both security professionals and hackers can use the Google search engine to obtain specific and often sensitive information about a target through publicly available websites.

Profiling a network is not as difficult as it may seem. Firewalking[21] is a technique that uses traceroute-like tools to probe firewalls and screening routers for ports, services, and protocols that are used by the target network. Firewalking can also be used to map hosts behind the firewalls and packet filtering devices. This

---

[18] Fluke Corporation (about us)
http://www.fluke.com/about_fluke/corporation.asp?AGID=11&SID=0

[19] Layton, Timothy. "Penetration Studies – A Technical Overview", SANS GIAC Practical. 2002. - http://www.sans.org/rr/paper.php?id=267

[20] Mowse. "Google-Knowledge: Exposing Sensitive Data with Google." February 2003. - http://www.digivill.net/~mowse/code/mowse-googleknowledge.pdf

[21] "Firewalking - A Traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access Control Lists", Cambridge Technology Partners. - http://www.packetfactory.net/projects/firewalk/firewalk-final.pdf

information is useful to security professionals to verify firewall and router configurations but can be used by hackers to determine which hosts are running certain services and therefore which vulnerabilities can be used to exploit the system/network.

The process of profiling a target based on information gathering is called "document grinding". This process includes much more than just Internet searches for information. It uses several methods to obtain information about what a company does, what it has (data, equipment, money, etc.), the people at the company and system/network structure and design. Both literal and electronic dumpster-diving can provide a potential attacker with all the information needed to direct an attack. Here are some of the things to look for when document grinding:

- Examine web databases and caches concerning the target organization and key people.
- Investigate key persons via personal homepages, published resumes, and organizational affiliations.
- Compile e-mail addresses from within the organization and personal e-mail addresses from key people.
- Search job databases for skill sets technology hires need to possess in the target organization.
- Search newsgroups for references to and submissions from within the organization and key people.
- Search documents for hidden codes or revision data.

Shredding all printed paper documents before discarding them is an Infosec recommended best practice. But protecting one's information from document grinding and electronic dumpster-diving requires several Infosec policies that address all aspects of information handling.

A Word to the Wise

All information is valuable. But not all information can be protected in the same way. The best security practices will help protect information in numerous forms. As security professionals, we have to be aware of what information can be useful to people outside of our organizations and how they might access that information.

The same tools companies use to promote and advertise themselves can be used by competitors to gain insight into the company's business strategies. This concept is called "competitive intelligence".

> *Competitive Intelligence: A systematic and ethical program for gathering, analyzing, and managing external information that can affect your company's plans, decisions, and operations.*
>
> *Put another way, CI is the process of enhancing marketplace competitiveness through a greater -- yet unequivocally ethical -- understanding of a firm's competitors and the competitive environment.*

> *Specifically, it is the legal collection and analysis of information regarding the capabilities, vulnerabilities, and intentions of business competitors, conducted by using information databases and other "open sources" and through ethical inquiry. - SCIP*[22]

Understanding what a competitor is doing will help guide a company to make internal decisions as to the direction it should take. Companies usually post who they are partnered with and major clients on their websites as a marketing strategy. This information also gives competitors an idea of who they should partner with in order to contend for similar clients. This is an example of competitive intelligence in its most basic form.

The point being, the same information used to aid a company can be used to understand and compete with the company. The way to protect this information is to be aware of how it may be used. And determining the goals and intentions of the competitor is the purpose of Red Teaming.

In the spirit of being aware of security vulnerabilities Fred Cohen published the "50 ways Series"[23] which includes:

- 20 Tips on Software Security
- 50 Ways to Defeat Your Firewall
- 50 Ways to Defeat Your PKI and Other Cryptosystems
- 195 Famous Computer Exploits - Bill Wall's List
- 30 Lies About Secure Electronic Commerce: The Truth Exposed
- 50 Ways to Protect Your Information Assets When Cruising the Internet
- 50 Ways to Defeat Your Intrusion Detection System
- 50 Ways to Attack Your World Wide Web Systems

The series is meant to be an educational tool to inform any user about some common ways to circumvent security measures for the purpose of protecting against such workarounds.

At the root of all security is an understanding of what makes systems and networks vulnerable. This understanding comes from training, research and investigation. Red Teaming is a methodical process that evaluates an existing security posture and helps bring understanding of threat, vulnerability and risk in order to improve security practices.

SUMMARY

> ***risk:*** *The possibility that a particular threat will exploit a particular vulnerability of a data processing system. – www.atis.org*[24]

[22] The Society for Competitive Intelligence Professionals - http://www.scip.org/ci/
[23] Cohen, Fred. "The 50 Ways Series" - http://all.net/journal/50/index.html

As security professionals we must never underestimate the attacker or overestimate our existing security posture. Many companies believe their data is unimportant to anyone but themselves and therefore do not protect it effectively. The truth of the matter is that a company may be a target not just for its information but potentially for its resources, access, recognition, or visibility. Until we understand what threatens our networks and identify where our systems are vulnerable, we cannot possibly protect against an attack; we are at risk.

Risk is never completely removed. Residual risk is managed and constantly assessed. Assessing risk requires an understanding of what threatens a network/system and by taking an attacker-like approach, Red Teaming helps companies first comprehend their risk and then, manage it.

Security professionals are constantly working one step behind the hackers, crackers, and script kids because historically we take a reactionary stance to vulnerabilities. Software patches come out only after a vulnerability has been identified and security measures are adopted immediately following an attack. Modern security efforts have to plan for the unplanned and anticipate attacks before they occur.

The cost of good security implementation is high. It takes people, training, time, research and constant reassessment. To make it more difficult, today's network and system security perimeters are expanding; IT staff have to consider WAN links, remote sites, and even the CEO's home computer when planning the security infrastructure.

Yes, it takes a great deal of effort to implement security, but can we put a price on loss of information, access, reputation, business, credibility? Security may "be a pain" but it is necessary. The trick is to obtain a level of "practical security" or usable security where security does not interfere with doing business.

The role of Red Teaming in security is to provide customers with an awareness of how they could potentially be attacked and why they would be targeted. The only way to anticipate the actions of a hacker is to act like the hacker.

> "Risk is the underlying concept that forms the basis for what we call 'security'. Risk is the potential for loss that requires protection. If there is no risk, there is no need for security." – Eric Maiwald[25]

---

[24] "Telecom Glossary 2000". Alliance for Telecommunications Industry Solutions. http://www.atis.org/tg2k/_risk.html

[25] Maiwald, Eric. Network Security: A Beginner's Guide. Pg .

WORKS CITED

- Maiwald, Eric. Network Security: A Beginner's Guide. City, publisher, date
- **eEye Digital Security Whitepaper, "**The Need for Vulnerability Assessment & Remediation: What My CIO Needs to Know." 2003
- Nicolett, Mark (VP, Research Director). "Managing IT Security Risk in a Dangerous World", CSO. - http://www.csoonline.com/analyst/report1332.html
- "Telecom Glossary 2000". Alliance for Telecommunications Industry Solutions. - http://www.atis.org/tg2k
- Delio, Michelle. "Find the Cost of (Virus) Freedom" Wired News - http://www.wired.com/news/infostructure/0,1377,49681,00.html
- Batongbacal, Mike (Developer Solution Specialist). "Security and eGovernment." April 2003. Microsoft - www.microsoft.com/usa/presentations/DD.ppt
- Herzog, Pete. "Open Source Security Testing Methodology Manual" (OSSTMM), Version 2.0, February 2002. - http://www.isecom.org/projects/osstmm.htm
- Lowery, Jessica. "Penetration Testing: The Third Party Hacker", SANS GIAC practical Exam - http://www.sans.org/rr/paper.php?id=264
- ISECOM – Institute for Security and Open Methodologies website. - http://www.isecom.org/
- Layton, Timothy. "Penetration Studies – A Technical Overview", SANS GIAC Practical. 2002. - http://www.sans.org/rr/paper.php?id=267
- Mowse. "Google-Knowledge: Exposing Sensitive Data with Google." February 2003. - http://www.digivill.net/~mowse/code/mowse-googleknowledge.pdf
- "Firewalking - A Traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access Control Lists", Cambridge Technology Partners. - http://www.packetfactory.net/projects/firewalk/firewalk-final.pdf
- Cohen, Fred. "The 50 Ways Series" - http://all.net/journal/50/index.html
- "CERT® Advisory CA-2000-04 Love Letter Worm", CERT Coordination Center. May 2000 - http://www.cert.org/advisories/CA-2000-04.html
- "The National Strategy to Secure Cyberspace." February 2003 - http://www.whitehouse.gov/pcipb/