Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Penetration Testing: Assessing Your Overall Security Before Attackers Do

Copyright SANS Institute
Author Retains Full Rights

SANS ANALYST PROGRAM

June, 2006

Sponsored by CORE IMPACT

Penetration Testing: Assessing Your Overall Security Before Attackers Do

By Stephen Northcutt, Jerry Shenk, Dave Shackleford, Tim Rosenberg, Raul Siles, and Steve Mancini

What is Pen-Testing?

Why Perform Pen-Testing?

Pen-Testing Tools And Reporting

Analysis Of CORE IMPACT

Metasploit Framework 3.0

Contents

Author BIOS 1

Executive Summary 2

What is Pen-Testing? 3

Pen-Testing vs. Vulnerability Assessment 4

How Vulnerabilities Are Identified 4

Why Perform Pen-Testing? 5

Find Holes Now Before Somebody Else Does 5

Report Problems To Management 5

Verify Secure Configurations 6

Security Training For Network Staff 6

Discover Any Gaps In Compliance 6

Testing New Technology 6

Pen-Testing Tools And Reporting 7

Reconnaissance Tools: 7

Nmap 7

Nessus 8

Packet Manipulation and Password Cracking Tools 8

Exploitation Tools 8

Metasploit Version 2.5 8

SecurityForest Exploitation Framework 9

CORE IMPACT (version 5.1) 9

The Penetration Testing Report 10

Analysis Of CORE IMPACT 11

Test Lab Network Diagram 11

Detailed Review Of Test Lab 12

Review Of CORE IMPACT 13

Conclusion 14

Metasploit Framework 3.0 13

ANALYST PROGRAM

Author Bios

Stephen Northcutt: Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer. Stephen is author/coauthor of *Incident Handling Step-by-Step*, *Intrusion Signatures and Analysis*, *Inside Network Perimeter Security*, *SANS Security Essentials* and *Network Intrusion Detection 3rd edition*. He was the original author of the Shadow Intrusion Detection system before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen currently serves as President of the SANS Technology Institute, a postgraduate IT Security College.

Jerry Shenk: Jerry currently serves as Senior Analyst for the SANS Institute and is the Senior Security Analyst for D&E Communications in Ephrata, PA. Since 1984, he has consulted with companies, financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds 5 GIAC GOLD certifications: GCIA, GCIH, GCFW, GSNA and GCFA: all completed with honors.

Dave Shackleford: Dave Shackleford has been involved in information technology, particularly the areas of networking and security, for over ten years. Dave is currently the Vice President of Business Development for Vigilar, a security consulting firm in Atlanta, GA. Dave has also worked as a security architect, analyst, and manager for several Fortune 500 companies and was the first Information Security Manager for AirTran Airways. His areas of specialty include incident handling and response, intrusion detection and traffic analysis, and vulnerability assessment and penetration testing. Dave is also a courseware and exam author for the SANS Institute, where he has taught classes, written multiple courses and exam questions, and also serves as a GIAC Technical Director. Dave has Bachelors degrees in both Psychology and Information Systems and a Masters in Business Administration from Georgia State University. He is the co-author of Hands-On Information Security from Course Technology, as well as the Managing Incident Response chapter in the Course Technology book Readings and Cases in the Management of Information Security.

Tim Rosenberg: Tim is an information security specialist with a strong legal background, Tim is presently responsible for developing and delivering highly focused Information Security courses tailored for his clients. Tim designed and built a portable training network as well as White Wolf Security's fixed learning facility in Lancaster, PA. This portable training network has been used to bring the classroom to the client and teach Information Security tools and countermeasures to a diverse student population including attorneys, executives, systems administrators, members of the Armed Forces and Federal/State law enforcement. Tim continues to design and build new labs for his client's specific needs. Tim has presented material at a variety of international conferences including RSA 2002, and 2003, 2005, InfowarCon, the American Bar Association's Annual Conference, NW3C Economic Crime Summit, the FBI National Academy at Quantico, and the Air Force's Information Warfare Conference. Tim has also been a guest lecturer at the U.S. Military Academy at West Point, the Army War College Center for Strategic Leadership, Villanova University School of Law. Tim has been an Associate Research Professor at the George Washington University where he taught Information Warfare and Computer Security courses as well as an Adjunct for Georgetown University's Security Studies Program. As a founding board member and first President, Tim help establish the Philadelphia Infragard Chapter which grew to one of the largest chapters in the country. Tim now runs White Wolf Security and develops innovative training solutions for his clients. He is also a Research Fellow for the Proteus Management Group.

Raul Siles: Raul is a senior security consultant with Hewlett-Packard. He has implemented numerous security solutions in various industries. Raul's expertise includes security architectures design, penetration tests, incident response, forensic analysis, system and network security assessments and hardening, intrusion detection and information security management. He is one of the few individuals who have earned the GIAC Security Expert (GSE) designation and also holds other SANS/GIAC certifications. Raul is also a SANS Institute course author and instructor. He is a frequent security speaker, has authored a TCP/IP security book and contributed to several security articles, reviews and research projects. He is a member of the Spanish Honeynet Project and loves security challenges. He holds a Masters degree in Computer Science from UPM (Spain) and a postgraduate in Security and E-Commerce.

Steve Mancini: Steve currently works as a Senior Information Security Analyst for the Intel Corporation where he is the technical lead to a business unit's risk management team. In his spare time he volunteers with the Hillsboro Police Department's Police Reserve Specialists and serves as the police department's principle digital forensics examiner and lab technologist. Steve has obtained 3 GIAC certifications over the last several years: GSEC, GCIH, and GSNA (honors).

Executive Summary

With multi-tier network architectures, Web services, custom applications, and heterogeneous server platform environments, keeping data and information assets secure is more difficult than ever. Coupled with this added complexity is the fact that criminal organizations have organized their hacking efforts; it is no longer just "script kiddies" trying to break into your network. In the past several years, it has become apparent that there is real money to be made from criminal hacking, and identity theft is one of the world's fastest growing problems.

Although there are many ways to secure systems and applications, the only way to truly know how secure you are is to test yourself. By performing penetration tests against your environment, you can actually replicate the types of actions that a malicious attacker would take, giving you a more accurate representation of your security posture at any given time. Although most penetration testing methods have traditionally been somewhat ad-hoc, that has changed in the last several years. Robust, repeatable testing methodologies now exist, and high-quality commercial tools can be implemented to ensure that both testing parameters and results are high-quality and trustworthy. CORE IMPACT is just such a tool. In the hands of a properly trained penetration tester, CORE IMPACT provides a stable, quality-assured testing tool that can be used to accurately assess systems by penetrating existing vulnerabilities.

What is Pen-Testing?

Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. If the focus is on computer resources, then examples of a successful penetration would be obtaining or subverting confidential documents, pricelists, databases and other protected information.

The main thing that separates a penetration tester from an attacker is permission. The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report. The goal of a penetration test is to increase the security of the computing resources being tested.

In many cases, a penetration tester will be given user-level access and in those cases, the goal would be to elevate the status of the account or user other means to gain access to additional information that a user of that level should not have access to.

Some penetration testers are contracted to find one hole, but in many cases, they are expected to keep looking past the first hole so that additional vulnerabilities can be identified and fixed. It is important for the pen-tester to keep detailed notes about how the tests were done so that the results can be verified and so that any issues that were uncovered can be resolved.

It's important to understand that it is very unlikely that a pen-tester will find all the security issues. As an example, if a penetration test was done yesterday, the organization may pass the test. However, today is Microsoft's "patch Tuesday" and now there's a brand new vulnerability in some Exchange mail servers that were previously considered secure, and next month it will be something else. Maintaining a secure network requires constant vigilance.

Pen-Testing vs. Vulnerability Assessment

The main focus of this paper is penetration testing but there is often some confusion between penetration testing and vulnerability assessment. The two terms are related but penetration testing has more of an emphasis on gaining as much access as possible while vulnerability testing places the emphasis on identifying areas that are vulnerable to a computer attack. An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem. A vulnerability assessor will stop just before compromising a system, whereas a penetration tester will go as far as they can within the scope of the contract.

It is important to keep in mind that you are dealing with a 'Test.' A penetration test is like any other test in the sense that it is a sampling of all possible systems and configurations. Unless the contractor is hired to test only a single system, they will be unable to identify and penetrate all possible systems using all possible vulnerabilities. As such, any Penetration Test is a sampling of the environment. Furthermore, most testers will go after the easiest targets first.

How Vulnerabilities Are Identified

Vulnerabilities need to be identified by both the penetration tester and the vulnerability scanner. The steps are similar for the security tester and an unauthorized attacker. The attacker may choose to proceed more slowly to avoid detection, but some penetration testers will also start slowly so that the target company can learn where their detection threshold is and make improvements.

The first step in either a penetration test or a vulnerability scan is reconnaissance. This is where the tester attempts to learn as much as possible about the target network as possible. This normally starts with identifying publicly accessible services such as mail and web servers from their service banners. Many servers will report the Operating System they are running on, the version of software they are running, patches and modules that have been enabled, the current time, and perhaps even some internal information like an internal server name or IP address.

Once the tester has an idea what software might be running on the target computers, that information needs to be verified. The tester really doesn't KNOW what is running but he may have a pretty good idea. The information that the tester has can be combined and then compared with known vulnerabilities, and then those vulnerabilities can be tested to see if the results support or contradict the prior information.

In a stealthy penetration test, these first steps may be repeated for some time before the tester decides to launch a specific attack. In the case of a strict vulnerability assessment, the attack may never be launched so the owners of the target computer would never really know if this was an exploitable vulnerability or not.

Why Perform Pen-Testing?

There are a variety of reasons for performing a penetration test. One of the main reasons is to find vulnerabilities and fix them before an attacker does. Sometimes, the IT department is aware of reported vulnerabilities but they need an outside expert to officially report them so that management will approve the resources necessary to fix them. Having a second set of eyes check out a critical computer system is a good security practice. Testing a new system before it goes on-line is also a good idea. Another reason for a penetration test is to give the IT department at the target company a chance to respond to an attack. The Payment Card Industry (PCI) Data Security Standard, and other recent security recommendations and regulations, require external security testing.

Find Holes Now Before Somebody Else Does

At any given time, attackers are employing any number of automated tools and network attacks looking for ways to penetrate systems. Only a handful of those people will have access to 0-day exploits, most will be using well known (and hence preventable) attacks and exploits. Penetration testing provides IT management with a view of their network from a malicious point of view. The goal is that the penetration tester will find ways into the network so that they can be fixed before someone with less than honorable intentions discovers the same holes.

In a sense, think of a Penetration Test as an annual medical physical. Even if you believe you are healthy, your physician will run a series of tests (some old and some new) to detect dangers that have not yet developed symptoms.

Report Problems to Management

If a CSO (or security team) has already pointed out to upper management the lack of security in the environment, penetration testing results help to justify the resources to address those needs.

Often an internal network team will be aware of weaknesses in the security of their systems but will have trouble getting management to support the changes that would be necessary to secure the system. By having an outside group with a reputation for security expertise analyze a system, management will often respect that opinion more. Furthermore, an outside tester has no vested interest in their results. Inside a corporation of any size, there will be political struggles and resource constraints. Administrators and techies are always asking for budget increases for new technology. By using an independent third party to verify the need, management will have an additional justification for approving or denying the expenditure of money on security technologies. Similarly, system administrators who know the intricacies of their environment are often aware of how to compromise their network. As such, it is not uncommon for management to assume that without such knowledge, an attacker would be unable to gain unauthorized entry. By using

a third party who operates with no inside knowledge, the penetration testing team may be able to identify the same vulnerability and help convince management that it needs to be resolved. A penetration testing team may also be able to prove that an exploit exists while the internal network staff "knew" it was there but wasn't quite able to pull all the pieces together to demonstrate the exploit effectively.

Remember that ultimate responsibility for the security of IT assets rests with Management. This responsibility rests with management because it is they, not the administrators, who decide what the acceptable level of risk is for the organization.

Verify Secure Configurations

If the CSO (or security team) are confident in their actions and final results, the penetration test report verifies that they are doing a good job. Having an outside entity verify the security of the system provides a view that is devoid of internal preferences. An outside entity can also measure the team's efficiency as security operators. The penetration test doesn't make the network more secure, but it does identify gaps between knowledge and implementation.

Security Training For Network Staff

Penetration testing gives security people a chance to recognize and respond to a network attack. For example, if the penetration tester successfully compromises a system without anyone knowing, this could be indicative of a failure to adequately train staff on proper security monitoring. Testing the monitoring and incident handling teams can show if they are able to figure out what is going on and how effective their response is. When the security staff doesn't identify hostile activity, the post-testing reporting can be used to help them hone their incident response skills.

Discover Gaps In Compliance

Using penetration testing as a means to identify gaps in compliance is a bit closer to auditing than true security engineering, but experienced penetration testers often breach a perimeter because someone did not get all the machines patched, or possibly because a non-compliant machine was put up "temporarily" and ended up becoming a critical resource. In today's heavily regulated environment, many organizations are looking for better ways to continually assess their compliance posture. Most regulations have multiple components specifically related to system auditing and security.

Testing New Technology

The ideal time to test new technology is before it goes into production. Performing a penetration test on new technologies, applications and environments before they go into production can often save time and money because it is easier to test and modify new technology while nobody is relying on it. Some examples might include a new externally facing web server with SOAP enabled, a new wireless infrastructure, or the introduction of mobile messaging gateways.

Pen-Testing Tools and Reporting

There are a wide variety of tools that are used in penetration testing. These tools are of two main types; reconnaissance or vulnerability testing tools and exploitation tools. While penetration testing is more directly tied to the exploitation tools, the initial scanning and reconnaissance is often done using less intrusive tools. Then once the targets have been identified the exploitation attempts can begin.

The line between these tools is very muddy. For example CORE IMPACT is a penetration testing tool but it also has a strong reconnaissance piece. Metasploit 2.5 is clearly a penetration testing tool with almost not reconnaissance functionality but version 3.0 will be adding some reconnaissance features. Nmap is clearly a reconnaissance tool and Nessus is mainly a reconnaissance tool but it has some penetration testing functionality. Many of the single-purpose tools fall more cleanly into either the reconnaissance or exploitation category.

Reconnaissance Tools:

Reconnaissance often begins with searches of internet databases including DNS registries, WHOIS databases, Google, on-line news sources, business postings, and many other on-line resources. The reconnaissance phase often includes print media as well, specifically electronically searchable archives that would be found at a college library or large public library.

Nmap

Nmap is a popular port scanning tool. Port scanning is typically a part of the reconnaissance phase of a penetration test or an attack. Sometimes attackers will limit their testing to a few ports while other times they will scan all available ports. To do a thorough job, a vulnerability scanner should scan all port and, in most cases, a penetration tester will scan all ports. An actual attacker may chose to not scan all ports if he finds a vulnerability that can be exploited because of the "noise" (excess traffic) a port scanner creates.

Another capability of nmap is its ability to determine the operating system of the target computer. Different networking implementations will respond differently to different network packets. Nmap maintains a type of database and will match the responses to make a guess at what type of operating system the target computer is running. This OS detection isn't perfectly accurate but it can help the attacker tailor his attack strategy, especially when coupled with other pieces of information.

Nessus

Nessus is a popular vulnerability scanner that many security professionals use regularly. Nessus has a huge library of vulnerabilities and tests to identify them. In many cases, Nessus relies on the responses from the target computer without actually trying to exploit the system. Depending on the scope of a vulnerability assessment, the security tester may choose an exploitation tool to verify that reported vulnerabilities are exploitable.

Nessus includes port scanning and OS detection, so sometimes a vulnerability assessment will just use Nessus and let Nessus call nmap or other scanners for these components of the test. For a stealthy scan, a security professional or an attacker may choose to run these tools separately to avoid detection.

Packet Manipulation and Password Cracking Tools

There are many other reconnaissance tools within the penetration tester arsenal, but two categories bear special mention here: packet manipulation tools and password cracking tools. The former category includes tools like hping, that allows a penetration tester or attacker to create and send all types of specially crafted TCP/IP packets in order to test and exploit network-based security protections, such as firewalls and IDS/IPS. The password cracking category includes tools like John the Ripper or Cain and Able, which is used to detect and obtain weak password for multiple authentication mechanisms, such as the ones supported by most Unix and Windows operating systems.

Exploitation Tools

Exploitation tools are used to verify that an actual vulnerability exists by exploiting it. It's one thing to have vulnerability testing software or banners indicate the possibility of an exploitable service, but quite another to exploit that vulnerability. Some of the tools in this category are used by both attackers and penetration testers. There are many more exploitation tools than the ones listed here. Many tools in this category are single-purpose tools that are designed to exploit one vulnerability on a particular hardware platform running a particular version of an exploitable system. The tools that we've highlighted here are unique in the fact that they have the ability to exploit multiple vulnerabilities on a variety of hardware and software platforms.

Metasploit Version 2.5

Metasploit is a relatively new addition to the penetration tester's tool belt. It provides attack libraries attack payloads that can be put together in a modular manner. The main purpose of Metasploit is to get to a command prompt on the target computer. Once a security tester has gotten to a command-line, it is quite possible that the target computer will be under his total control in a short time. The currently released version of Metasploit Framework as of June, 2006 is version 2.5. Version 3.0 is expected out shortly. See the sidebar for some information about Metasploit Framework 3.0.

This is a tool that attackers would use to take over, or *own*, a computer. Once an attacker can gain this level of access to a computer, they would often install code that would allow them to get back onto the computer more easily in the future. In some cases, a penetration tester would also install tools on the computer, but often they would simply document the access and what data was available and move on to other testing. This would depend on the defined scope of the testing. The security professional also would want to be careful about causing data loss or server instability that may result in lost productivity. A malicious attacker may be more cavalier about using the computer without regard to lost productivity, though a highly skilled attacker targeting a specific company may be very careful not to damage the system so that they can avoid detection.

SecurityForest Exploitation Framework

Although still technically in Beta version, the SecurityForest Exploitation Framework is another open-source tool that can be leveraged by penetration testers. This framework leverages a collection of exploit code known as the ExploitTree, and the Exploitation Framework is a front-end GUI that allows testers to launch exploit code through a Web browser (similar to Metasploit's Web interface). The Framework is very similar to Metasploit, in fact, with a few key differences. ExploitTree has a remarkable number of exploits included, but the vast majority of these are in pre-compiled format (most likely in a C file) or exist as Perl executables. They are also not natively integrated into the Framework. This framework is not nearly as extensible as some other tools; it primarily functions as a GUI to launch attacks from.

CORE IMPACT (version 5.1)

CORE IMPACT is a commercial penetration testing tool that combines a healthy dose of reconnaissance with exploitation and reporting into one point and click penetration testing tool. The main purpose of CORE IMPACT is to identify possible vulnerabilities in a program, exploit those vulnerabilities without causing system outages, and clearly document every step along the way so that the entire procedure can be verified by another party.

The CORE IMPACT penetration testing tool makes is easy for a network administrator or penetration tester to run tests against a network or host without having a whole suite of security testing utilities. Overall, we found the program to do a good job of scanning the network for vulnerabilities, successfully exploiting them, and reporting on the results.

One really slick feature of CORE IMPACT is the ability to install an agent on a compromised computer and then launch additional attacks from that computer. This proved useful in an actual penetration testing assignment by allowing the tester to compromise one machine and from there run automated scans inside the network looking for additional machines. Those scans weren't quite as good as actually being on-site, but it did allow us to discover internal hosts from outside the network.

For most systems, CORE IMPACT will work well, but as Core Security Technologies states in their documentation, it isn't meant to be a replacement for an experienced penetration tester. One of the areas we ran into some trouble on was when a single IP address had different ports mapped to different servers with different operating systems. Sometimes CORE IMPACT would identify a host as having a given operating system and then refuse to launch a vulnerability against a service that did not match that operating system. In one tested network, a single public IP address was in use by three different computers: an Exchange server, an IIS web server, and a Linux computer running SSH. The OS had been identified as being in the Linux family so an attack against IIS vulnerability wasn't an option. We were able to work around this by re-scanning the machine using only the ports that mapped to the Windows system.

As a commercial vendor, Core Security Technologies does a lot of testing of their exploit code to ensure that it will not adversely affect the target hosts. In testing CORE IMPACT, we found that it was rare for it to crash systems. There was one case where an unpatched Windows 2003 server rebooted a few times in different testing scenarios. Later, the same test was used to exploit the system and gain access to a command prompt. Other than this one test against an unpatched Windows 2003 server, we did not crash any systems.

The reporting feature of CORE IMPACT is quite good. It includes an executive report, a report that lists vulnerabilities and all the machines affected by those vulnerabilities, a detailed report of all hosts and an exhaustive report of every test that was run, when it ran, how long it ran and detailed results of the running. This last report is one that you don't need very often but if you do need it, it has all the details do duplicate a test. Keeping accurate notes is one of the most difficult and time consuming tasks for a pen-tester because often many tests are attempted with small variations to the test. CORE IMPACT makes it easy to go back and find any steps that weren't properly recorded.

The Penetration Testing Report

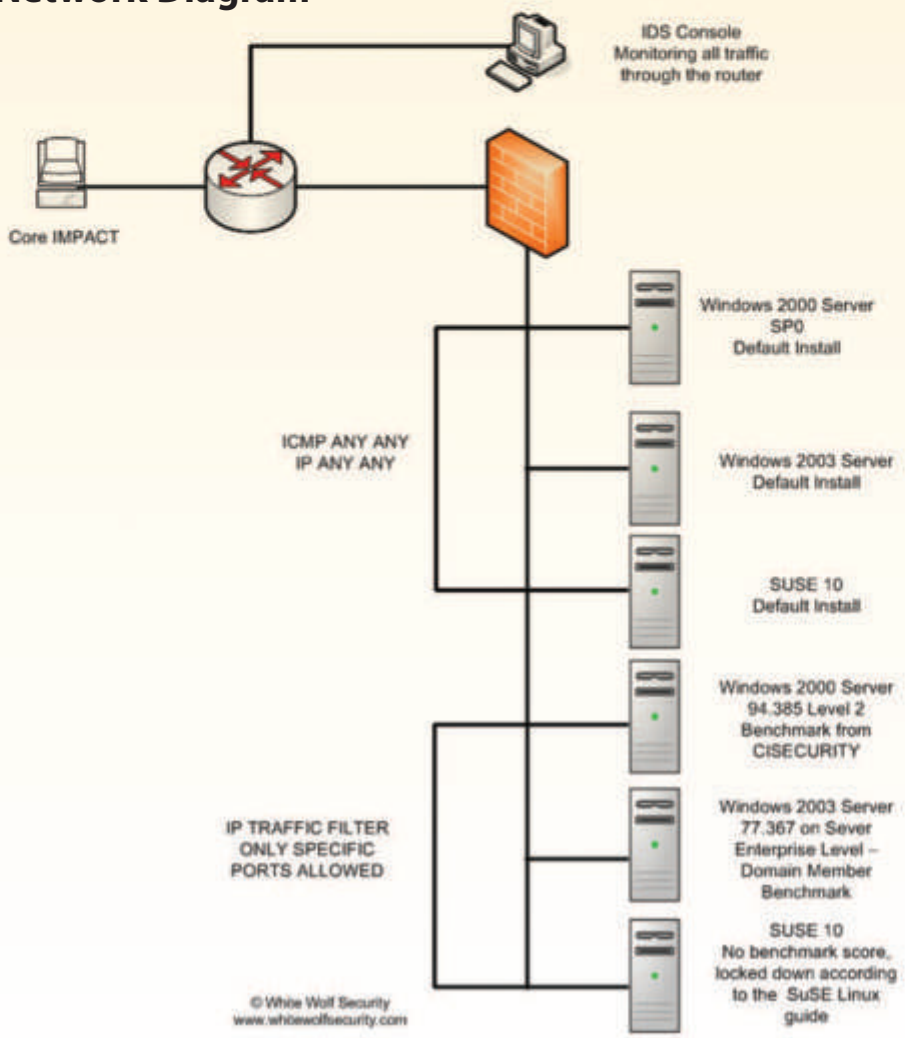
After performing a penetration test, compiling the results from the test into a legible format is key. As many key decision makers are not overly technical, it is critically important to have multiple sections to a report. One common structure for penetration testing reports is to include an Executive Summary, a Management Summary that includes some high-level operational details such as server IP addresses and what needs to be fixed immediately, and a Technical Summary with very specific results and remediation suggestions.

Inclusion of "attack vectors" is important in a thorough penetration test, as well. Given the complexity of most IT environments today, it really does not suffice to indicate that a particular system has a vulnerability. Instead, it is more informative to first demonstrate exactly how this system was accessed, and then explain the vulnerability and exploit. For example, if a DMZ mail server was compromised, and then used as a "jump point" to access other systems, then this entire attack path should be laid out in detail for everyone to understand. The exploitation of trust relationships is a key factor that is difficult to represent by simple "canned" exploits or attack methods.

Analysis Of CORE IMPACT

CORE IMPACT was pulled into the White Wolf Security lab and run against six systems. These systems represent operating systems in one of two states of deployment, default install and no firewall filtering, and locked down behind proper firewall rules. In the case of the default systems sitting behind a firewall that allowed all traffic to/from the systems, each operating system was correctly identified. Upon OS and service identification, the two default Windows systems were quickly compromised using well known exploits. The third default system was a SUSE Linux and not compromised. In the case of the hardened systems behind proper in-bound firewall rules, the OS was correctly guessed, but none of the systems were able to be compromised through the firewall.

Test Lab Network Diagram



Detailed Review Of Test Lab

All the systems were placed behind a Cisco PIX 515E firewall, with varying rules for each of the servers. The three servers that were default installs had no restrictions on the traffic allowed in or out of the firewall. The rules were "ICMP any any" and "IP any any". The three servers that were locked down had rules allowing traffic through the firewall that corresponded with their functions. For example, the Windows 2003 server was an eCommerce web-site. While the site is database driven, only port 80 and 443 were allowed through the firewall to the host. All outbound traffic from all systems was allowed.

CORE IMPACT successfully installed a level(0) agent on each of the Windows 2000 and Windows 2003 default installs, though all attempts to upgrade to level(1) agents failed. The SUSE 10 system was unharmed and not compromised. None of the servers that had appropriate firewall filtering were successfully compromised through the firewall. These systems were also locked down according to their respective CISECURITY guidelines.

At roughly the same time as the CORE IMPACT test was running, the same environment was part of an open game lab for a SANS conference in San Diego, CA. In this environment, we were able to see CORE IMPACT against a group of human penetration testers (we'll refer to them as 'The Contractors'). The Contractors were finally able to compromise the data on the Windows 2003 and 2000 servers. Each of those two servers had MYSQL running with employee and customer databases full of simulated data. The method of compromise was by finding the MYSQL username and password embedded in some PHP pages. Using those credentials, The Contractors were able to use the MYSQL client on the less secure systems to connect over to the locked down OS and perform a database dump.

Review Of CORE IMPACT

In general, I enjoyed running with CORE IMPACT. The integration of the complete attack sequence from information gathering to penetration and clean up makes things much easier. Without an integrated tool, the tester must maintain copious notes and copies of output from one tool to be used as input for the next. Using CORE IMPACT, the tester still needs to take notes, but the bulk of the general information, such as live systems, OS type and running services can all be stored in the tool in a saved session.

Running CORE IMPACT against an infrastructure with IDS was interesting. We used the Cisco NM-CIDS-K9 IDS module in the perimeter router. CORE IMPACT is far from quiet. Alerts were thrown almost from the beginning of the scan. While some would consider this a negative, I disagree. As mentioned earlier in the paper, one of the best uses for a penetration test is to test your organization's ability to detect and respond to an attack. The default settings of CORE IMPACT make for a very loud process to anyone running IDS. If you can get an agent installed without alerting the IT or Security team, then they have a serious deficiency in their practice.

Another advantage to the tool is the safety of the agents. In a previous life, I was an attorney in Pennsylvania. There are very real legal issues associated with doing a proper Penetration Test; not the least of which is the overall safety and confidentiality of the client's data. Using a tool like CORE IMPACT to root a box makes things a bit safer than just downloading someone's exploit and running it. At one end of the spectrum, you have commercial tools such as CORE IMPACT and open source tools such as Nessus and the Metasploit Framework. At the other end of the tool spectrum, you have some code you found on some hacker site that you might want to try. Unless you can do proper code review, you will never know what you are running on the client's system. There is a risk of installing a back door or data swiper that is hidden in the exploit code. With professional tools such as CORE IMPACT, that risk approaches 0. Ultimately, a penetration test is no good and down right dangerous if the tester cannot clean up their activities and ensure that the systems are restored to their 'pre-hacked' states. One of the most powerful feature of CORE IMPACT is the clean up and agent removal function; allowing a tester to get all agent code shut down and off systems.

Conclusion

Penetration testing is like the annual physical at your doctor's office. CORE IMPACT and Metasploit Framework are diagnostic tools, much like a blood test or an X-ray. A blood test will check for many things, but it still takes a doctor to review the data, make inferences, perform additional tests and then reach a diagnostic conclusion. Penetration testing is no different. CORE IMPACT will test for many things, but it will always take a human to review the results and make inferences based on knowledge and experience that you will never be able to put in a tool. That being said, CORE IMPACT is an excellent diagnostic tool. It lowers the barrier of entry for the vast majority of a penetration test through intelligent automation.

Instead of taking a $400 an hour consultant to run nmap, Nessus and Metasploit Framework, it can be done by a junior consultant or an in-house security expert running CORE IMPACT. Physicians manage patients by ordering tests and interpreting the results. This process is made more efficient and accurate through the use of diagnostic tests and support staff such as nurse practitioners. CORE IMPACT helps automate a great deal of the penetration test and provides services and tools to the new penetration testers as well as the seasoned veteran, allowing each to focus on the part of the test they excel at. This creates a business process that allows for the performance of penetration tests in a more efficient and standard way. By offloading the automatic work of scanning, penetration, clean up and reporting to CORE IMPACT, a penetration tester can spend more time doing what humans do best: using their experience to make inferences and taking the penetration testing to places that only a human can go. As a result, the tester can do better work in less time meaning they can secure more systems without sacrificing the overall quality of their testing.

Metasploit Framework 3.0

Metasploit Framework 3.0, a complete rewrite of the 2.0 branch based on the Ruby language, will be released this year. This version includes several impressive features, the main ones being automation and evasion. The new capabilities allow exploit automation through auxiliary scripts, and support automated network discovery and event correlation through reconnaissance modules. The integration of IDS/IPS multi-layer evasion modules, both at the application and protocol stacks, will allow it to perform truly stealthy tests.

From a business perspective, the new version adds multi-user support, for team-based penetration testing, and multi-session support, allowing concurrent exploits and sessions with multiple targets simultaneously. These capabilities, plus support for various databases and new reporting features, make version 3.0 a compelling tool in the security professional arsenal.

Some new exploit features are the capability of using the initially compromised machine as a launch point to attack other targets, and a new framework to escalate privileges once a system has been compromised; both options already exist on the pen-test commercial products. Additionally, the tool offers the possibility of migrating the exploiting code from the originally targeted process to a different process in memory, making the investigator analysis more challenging. Finally, other new built-in capabilities are focused on simplifying the exploit development process through an advanced framework integration, and increasing code simplicity, reusability and flexibility, while providing multiple user friendly interfaces.

This upgrade clearly places Metasploit as a cutting edge exploitation technology, competing with the commercial options.

http://www.metasploit.org/projects/Framework/msf3/

Last Updated: November 29th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defense Initiative 2014	**Washington, DCUS**	**Dec 10, 2014 - Dec 19, 2014**	**Live Event**
SANS Security East 2015	**New Orleans, LAUS**	**Jan 16, 2015 - Jan 21, 2015**	**Live Event**
SANS Brussels 2015	**Brussels, BE**	**Jan 26, 2015 - Jan 31, 2015**	**Live Event**
SANS Dubai 2015	**Dubai, AE**	**Jan 31, 2015 - Feb 05, 2015**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Washington, DCUS**	**Feb 02, 2015 - Feb 09, 2015**	**Live Event**
SANS Scottsdale 2015	**Scottsdale, AZUS**	**Feb 16, 2015 - Feb 21, 2015**	**Live Event**
10th Annual ICS Security Summit - Orlando	**Orlando, FLUS**	**Feb 23, 2015 - Mar 02, 2015**	**Live Event**
SANS Munich 2015	**Munich, DE**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
SANS DFIR Monterey 2015	**Monterey, CAUS**	**Feb 23, 2015 - Feb 28, 2015**	**Live Event**
SANS Secure India 2015	**Bangalore, IN**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
Healthcare Cyber Security Summit	**OnlineCAUS**	**Dec 03, 2014 - Dec 10, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**