Why Black Hats Always Win

Version 1.0.0

Val Smith {valsmith[at]atackresearch.com}

Chris {chris[at]sdnaconsulting.com}

Last modified: 01/08/2010

Table of Contents

Chapter 1

Introduction

1.1 Abstract

From the origins of hacking and black hat hackers a new industry called penetration testing has evolved. Penetration testing is intended to emulate a real attacker in order to uncover what vulnerabilities an organization may have that could put them at risk so they can be fixed. This has led to the term "White Hat Hacker" being used to describe those who perform these tests. However, the goals of a White Hat differ greatly from the goals of a Black Hat, as do the mindsets. This presentation will describe these differences as well as some of the things black hats have to consider that white hats may not even be aware of. This paper will explain why black hats have the advantage over white hats and why the penetration industry has to change. The takeaway from this presentation is that current common penetration methodologies are ineffective in demonstrating the actual risk and threats that exist and provide some insight into how real attacks actually work from the point of view of a black hat.

1.2 Background

The authors of this paper have been involved in security auditing and penetration testing for several years. A common trend among security testers is the use of off-the-shelf software and standardized methodologies to automate the penetration test process. Tools like Nessus[1], Retina[2], CANVAS[3], and Core Impact[4] have replaced manual audits and checklists at many organizations. While these tools do a great job of reducing the time and knowledge requirements of penetration testing, their use can lead to an inaccurate emulation of real attacks, thus reducing the value of a penetration test. Many important attack vectors are missed because they are not implemented by an automated software product.

1.3 Author Bio - Val Smith

Val Smith has been involved in the computer security community and industry for over ten years. He currently works as a professional security researcher on a variety of topics in the security community. He specializes in penetration testing (over 40,000 machines assessed), reverse engineering and malware research. He has worked on the Metasploit Project[5] development team as well as other vulnerability development efforts. Most recently Val Smith founded Attack Research[6] which is devoted to the comprehensive understanding of the methodologies used in attacks against computer systems. Previously Val Smith founded Offensive Computing[7], a public, open-source malware research project.

1.4 Author Bio - Chris

Chris is a Security Consultant and Researcher with Secure DNA[8]. Chris specializes in web-based application development security. He has collaborated with some of the top security researchers and companies in the world and has performed static and dynamic security assessments for numerous companies and government agencies across the U.S. and Asia.

1.5 Acknowledgements

The authors wish to express their thanks to HD Moore for the concepts in Tactical Exploitation[9], and to the numerous unknown black hats whose techniques, activities and goals we can only guess at.

Chapter 2

Overview of White Hat Methodologies

2.1 Goals

White hat penetration testers have several goals when they begin to attempt to compromise a system. The main focus is on achieving the largest number of compromised machines possible. During the course of the engagement, the tester needs to generate sufficient data to fill reports for delivery for the customer. A main area of concern is identifying mitigations for discovered vulnerabilities in order to assist the customer in preventing the attack. Often understanding the vulnerability footprint of an organization, not the strategic penetration of its systems, is the primary goal. Identifying accessible sensitive or critical data is usually a second order goal, if considered at all.

2.2 Information gathering

Penetration tests have a heavy focus on network scans such as massive NMAP[10] port scans, Nessus vulnerability scans, etc. In addition to scans there are some components that overlap with what Black Hat's do during an attack. These components include DNS/Domain lookup records, Google hacking and personnel discovery. The purpose of these for both Black and White Hat's is to understand the infrastructure and the relationship of the people to the organization as well as any unintended information made available to the internet.

There is typically much less concern for being detected by the target with White Hat penetration tests than with Black Hats. Often penetration testers want the target to detect them in order to exercise the organizations incident response elements as a part of the test, and therefore avoid techniques that involve stealth.

2.3 Vulnerability Assessment

White Hat penetration testers typically include a vulnerability assessment as a part of their activities. This almost always involves many automated scans which are both detectable and easy to fingerprint. This results in inferences about potential vulnerabilities rather than absolute knowledge.

The main focus at this stage is on risk and threat analysis. Penetration testers are required to understand and communicate the potential consequences to an organization of every vulnerability. How does this vulnerability hurt the business of the customer? Will the customer suffer a monetary loss or one of reputation? What is the possibility that an attack against a particular vulnerability might occur. These are all questions the penetration tester considers when preparing the report.

2.4 Exploitation

The typical exploitation workflow of a White Hat penetration tester once the vulnerability assessment phase has been completed is to simply download exploits published on any number of websites such as milw0rm[11], Security Focus[12], SecuriTeam[13] and others. These sites often become defunct or unmaintained, rendering their resources stale or unusable. If a penetration testing organization is staffed by individuals with limited skill, the lack of stability in these exploit collection sites can have a serious impact on the quality of their work, and their ability to compete in the industry.

Automated exploitation frameworks which externally update and maintain exploit collections are also frequently used by penetration testing organizations, but these can be costly.

Typically, the results of the vulnerability assessment reflect testing for the existence of a known vulnerability, and then attempting to exploit the vulnerability using the tools made available by the aforementioned methods. Often the exploits themselves are not tested before use but rather run live against the customer, one after the other, until something works, or all options have been exhausted.

2.5 Data Collection

The data collection phase of an attack is typically limited for White Hat testers. It usually consists of screenshots of vulnerable systems or successful compromises along with a small sample of documents or data sufficient to prove that access has been obtained.

The in-depth analysis of attack paths or strategies for prolonged infiltration into the target are not a component of these types of tests. There is no long-term sniffing of network traffic or key logging of user systems because engagements are limited in scope and timeframe.

Chapter 3

Overview of Black Hat Methodologies

3.1 Goals

Black Hat attackers have a wide range of goals when they attempt to compromise a target. Black Hats are much more likely to be focused on the extraction of data, not just access to the targeted systems. This means that they identify strategic data that they want for various reasons and tailor the attack in order to obtain this data, where White Hats simply care about how many systems, they can access with little regard for the data itself.

Black Hat's will often have complex trust targeting objectives and focus on the people who are the weakest link in both security and trust chains.

Access to seemingly unrelated secondary systems may provide steppingstones into primary targets. Some would say that any box on any network is only 6 degrees of separation away from a true target. This contrasts greatly with White Hats who have limited scope and never focus on non-customer owned targets, even if they would provide access to the customer via trusts or other methods.

Another important goal for Black Hats is to gain access to software source code. When a Black Hat gains access to source code they have an opportunity to modify the source in order to introduce vulnerabilities, or to audit the source for bugs. When the target installs or updates the vulnerable package, the attacker has a sure way to compromise the target. Gaining access to source also enables more potential assets. Perhaps the ultimate target does not run the application in question, but a collaborator or trusted website does.

For example, If the target runs wordpress[14] on their website, The Black Hat can compromise the wordpress source repository and then audit the code for vulnerabilities as well as introduce backdoor code to the latest version. This enables surefire compromise of the ultimate target in time, when they upgrade the wordpress software.

3.2 Information Gathering

A Black Hat's approach to information gathering can be quite different to that of a White Hat. Nothing is off limits to the Black Hat. If needed information resides on an unrelated box, such as an ISP's DNS server, a GMail account on Google's servers, etc. it is still "in scope" to the Black Hat. Fake social networking accounts can be set up to gain information about the target’s activities and friends. The target's friends, co-workers, family, even the target themselves can be called up and "social engineered" to give up information useful to the attack.

A Black Hat can scan anything anywhere, upload enumeration code to a website, engage in disruptive effects to cause the target to take revealing actions or any number of strategies not available to a penetration tester. A Black Hat might acquire data from Lexis Nexus, a credit bureau, or a background check service in order to gain more information about the ultimate target. Telephone systems, voice mail, nothing is off limits, giving the attacker a significant advantage and a higher rate of success in the long term.

3.3 Vulnerability Assessment

Attackers often know what is vulnerable ahead of time, either by source code manipulation, code auditing or other means. This eliminates the need for noisy and detectable vulnerability scans, reducing the possibility of raising any alarms. This is a much more efficient method than the White Hat trial and error technique.

Often Black Hats will employ the exploitation of non-traditional vulnerabilities. For example, in one case the authors are aware of, an organization was using an in-house developed, non-commercial, software distribution and licensing application. This application was installed on every computer in the enterprise and ran with domain administrator account privileges. To be able to perform its required functions, it had to have a re-usable password. This provided the attackers with a potential vector on every single system in the network. In order to somewhat mitigate the vulnerability of the static password, it was changed on a time interval on the order of minutes.

The attackers gained access to a binary copy of this application and performed an analysis of its operations. After some examination with a binary disassembler, it was determined that the password changing algorithm potentially stored the clear text password in memory for some period of time. By employing the use of a debugger, the attackers could access the region of memory and acquire the password, gaining domain administrator access, and access to any machine on the network for a short period of time. Through the use of automation, the attackers were able to compromise the entire enterprise.

3.4 Exploitation

Black Hats focus more on 0-day vulnerabilities than White Hats. This is because 0-day exploits are nearly useless to a penetration tester, but gold to an attacker. A penetration tester cannot put into a report that they compromised a system with something the customer was neither aware of, nor was there a patch available for. This is of no value to the customer because there is nothing they can do about the problem.

In the world of the attacker 0days are kept closely held. They are often only used in the case that a public vulnerability fails to work and the need for success is high. Attackers avoid risking "burning" unpublished vulnerabilities if possible. Every time a 0day is used, the likely hood of it getting detected, disseminated and patched grows.

A strategy that is employed is to wait until the moment a vulnerability is public before use. This allows the attacker to blend in with the peak of other malicious traffic, obscuring the fact that they had access to unknown exploits.

3.5 Data Targets

Where penetration testers do not typically target data, attackers have a variety of data categories they go after. These include:

Mail spools - The collection of a targets available email.

Backup files - Backup files often contain all data available on a system, and usually do not have the same file system access controls.

Database dumps - Sites that handle credit cards or other financial transactions, authentication information or other types of sensitive data often store them in databases.

Sniffer logs - If an attacker gains access to a user system or other "behind the firewall" computer, capturing network traffic can help with enumeration, data compromise, etc.

Keystrokes and chat logs - Everything a target type is of potential value, from passwords to account numbers, to communications with other users.

Access tokens - Various types of files or memory allocations which inform a system or network of a particular user's access and authentication status.

Targets of opportunity - During the course of an attack, Black Hats are always on the lookout for trusts that can be exploited, or other systems of value that were previously unknown.

There are a wide variety of techniques that attackers use to try to acquire target data. These include a category of attacks called client injection/exploitation. This involves attacking vulnerable client applications such as vulnerable IRC software which allows the attacker to capture chat traffic, or browser attacks which allow for access to sensitive data in the browser. For example, most web applications that carry sensitive data such as credit card numbers, usernames and passwords are SSL encrypted so that someone cannot eavesdrop as the data is being transported from the user client application to the end point server. Some organizations such as banks even go so far as to use on screen keyboards to protect the client from keyloggers.

These defenses are ineffective because many attackers are now grabbing the data from browser memory or by accessing browser APIs before the data is sent in an HTTPS POST but after it has by typed in something such as an onscreen keyboard. Therefore, the attacker can access the data clear text regardless of these protections.

Chapter 4

Attackers vs. Defenders

4.1 Fundamental Differences

To summarize some fundamental differences between defenders and attackers; defenders have limited resources and time and strict rules of engagement. Defenders have performance-based consequences. If a penetration tester is never able to access a system, then eventually customers lose confidence, and they no longer get hired to perform tests. The motivation of a defender to get into a system is generally based on reporting metrics and demonstrating the threats and risks to their customers.

On the other hand, hackers have unlimited resources from the point of view that they can use any computer, software, network or tool necessary to achieve their goal. They technically have unlimited time in that they can persist against a target for weeks, months or even years, as long as they continue to want to. This offers a significant advantage to the attacker because over a long enough amount of time everything can eventually fall to compromise no matter the sophistication of its security.

If an attacker targets an organization the odds of success increase over time whereas time goes on a penetration tester has less chance of success because the end of the engagement approaches. To an attacker there are no consequences for not gaining access other than they have to try more, where to a defender the consequences are less data for the report, less footholds, a lower access count and over time possibly a reduced reputation.

The motivations for attackers can be varied, complex and difficult to determine. This makes predicting the future actions of an attacker more difficult to predict than the actions of a defender. A defender will likely perform a scan, run some exploits, install countermeasures, and then write a report but what an attacker will do next may be totally unknown.

4.2 Starting Points & Discovery

When a White Hat begins an attack, they are usually assigned a limited block of IP addresses to scan and attack. The penetration tester is legally unable to go beyond the scope of the customer approved list, even if the most efficient way in is on an address not in scope. Customers often provide at least some background about the network, sometimes diagrams and other configuration information. Black Hats usually know one piece of information such as a target name, domain name, IP or email address, etc. and have to expand the sphere of knowledge from there.

Because of the limited starting point of knowledge about the target, Black Hat attackers need efficient techniques for discovering target related IP addresses and client-side application information. They can gain this information in a variety of ways. To gather information about target home IP addresses, mail clients and email addresses an attacker can harvest this information from the headers of news groups and mailing lists which usually have an archive available online to parse. In some cases, outgoing proxy logs are exposed which can allow the attacker to mine information such as how many internal IP addresses there are, what websites the users frequent, operating system types, antivirus and other self-updating applications.

Attackers can use techniques such as backscatter spam in order to gain knowledge about mail gateway configurations, lists, email addresses, allowed file format types and more. Sites such as botsvsbrowsers[15] can provide extensive information about user browser types and operating system versions.

Ex.

```
From stephan.j@atarget.com Sat Apr 26 17:38:24 2009
MBOX-Line: From stephan.j@atarget.com Sat Apr 26 01:28:41 2009
Message-Id:<5.2.0.9.2.20090426102623.025ce3b8@mail.spamcop.net>
X-Mailer: QUALCOMM Windows Eudora Version 5.2.0.9
```

```
In-Replay-To: <16040.65254.766438.720746@host.another.loc>
Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; format=flowed
X-Spam-Status: No, hits=-4.9 required=5.0 tests=IN_REP_TO,
DEAR_SOMBODY version=2.20
X-Spam-Level:
From: Stephan J <stephan.j@atarget.com>
To: pelis AT trusted DOT de
Subject: Re: pelis.org
Date: Sat, 26 Apr 2009 10:28:38 +0200
Dear Walter,
```

The above example demonstrates some of the valuable information that can be gleaned by mining mailing list headers. This selection tells us the mail client type and version, the operating system, the fact that they have some SPAM handling software, what it is, and someone the target is communicating with and likely to expect mail from.

Chapter 5

Analysis of Black Hat Techniques in the Wild

5.1 Profiling

White Hats typically are assigned specific targets. A common occurrence is for the customer to tell the penetration tester to only touch specific hosts and not others which may be critical to operations, live production, or known to be outdated. Frequently a customer will point out several hosts known to be vulnerable which are also designated as off limits. This means that the customer misses out on understanding what an attacker can do to the rest of the network based on the security posture of those "off limits" boxes.

A Black Hat on the other hand chooses his own targets and typically has strategic reasons for doing so. A Black Hat will go after code developers because they are the ones who have access to source repositories that can be mined for vulnerabilities or modified for backdoors. An attacker will also target penetration testers because if they are successful then a good portion of the work is done for them. Penetration testers already have access to some systems and are expected to be attacking therefore hiding the true attackers tracks and activities. Penetration testers also may have access to tools which can be of use to the attacker.

Security researchers are frequently targeted for a variety of reasons, the most common being that they have access to cutting edge information about techniques, 0day's and other attacks which can be leveraged by the Black Hat.

5.2 Environment Modeling and Testing

White Hats and Black Hats go about testing their tools and techniques in somewhat different manners. White hats often test new attacks directly against client systems. During the course of the penetration test they will download whatever new tool or exploit is available and use it.

Black Hats might mirror an entire target environment using virtual machines or equipment purchased from eBay[16]. They will design this environment to match the target as closely as possible and test all tools and techniques against it long before going after the real systems. Attackers will gather information and profile a target until they know the operating systems, hardware, patch levels, applications, and other information until enough is known to build a reasonable model.

This enables the attacker to perfect their methods without the risk of alerting the target, crashing services or making detectable mistakes. In this way once it comes time for the actual attack everything can be planned, timed and automated so that success is rapid and ensured. Attackers can do vulnerability assessment at their leisure, audit code, fuzz, reverse engineer applications and generally gain a high level of preparation. In one case known to the authors a group of attackers spent 18 months modeling and staging in order to exploit the target in less than a minute and spent 5 minutes acquiring the data. No indication was given at the time that the target detected the attack.

Another important difference is exploit development. In general, Black Hats develop exploits for their own use, while White Hats use exploits which have been developed and made available by others.

5.3 Examples

Apache.org

- Attackers used no exploits. Instead, they relied on configuration errors.
- Attackers Used a combination of small bugs leveraged against the system to gain access.
- Attackers gained administrative access to the main source repository.
- Attackers Patiently waited for root to login.
- Attackers Defaced the main web site.

Debian.org

- Attackers used no exploits.
- Misuse of SSH Authkeys by users on a system in Japan and a system in the Netherlands granted access.
- To the administrative account on debian.org.
- SSHD was backdoored.
- Core Debian OS source backdoored.
- Was unknown for 6 months.

Wordpress.com

- Attackers used zero-day vulnerability.
- Backdoored Live web application.
- Accessed chief source code repository.
- Backdoored source code.
- Was quickly noticed and fixed.

Comcast.net

- Attackers used no exploits.
- Attackers Social Engineered Network Solutions into granting them access to Comcast's account.
- Attackers redirected comcast.net domain name to attacker-controlled servers.
- Defaced.

Linux Distribution

- Heard of attacker getting in over months.
- Subtlety backdoored distribution.
    - Introduced bug.
- Matched md5s
- Able to own any system for 6 months.
- Distro NOT the ultimate target

Bank

- Found development host on separate network.
- Attackers used custom vuln in co-located website.
- Read many files via directory traversal.
    - Solaris treats directories like files.
        - Therefore, you can do cat dir/ and get an ls.
- Discovered copy of every transaction goes over email.
- Copied mail spool via targets own website.
- $$$$.

The reoccurring theme in real attacks is that very few exploits are actually used. Often only one exploit is needed to get the initial access and then other methods are used from there. This differs quite a bit from traditional penetration testing techniques. More often attackers use captured / cracked passwords, hijacked trusts or compromised user access as in the case of trojaned SSH clients or stolen / dropped SSH authorized keys.

By using these methods instead of exploits, attackers can appear to be normal users. This is much harder to detect than shellcode or other malicious content across the network. The traffic in this case looks like typical user activity, especially if the attacker is cautious and learns the user's patterns of behavior before acting.

Real attackers treat 0day exploit as priceless and usually save them until they are "1 day" or just recently disclosed. Knowledge of system internals rather than the latest exploit release on milw0rm is the key. Attackers know the playbook used by White Hats, sysadmins, users and security personnel. Black Hats do not do what penetration testers do during an attack unless they want to appear to be a tester.

5.4 Problems

Black Hats suffer from problems that White Hats usually don't have to consider or be aware of. For example, attackers have to be concerned with secure data exfiltration, which is the way they retrieve the data they want without being detected, the data being corrupted, or letting the target know what data they have lost. Penetration testers have little to no focus on data stealing and so they don't have to worry about this.

To combat some of the problems with data retrieval attackers do things using Tor to obfuscate the connection, but tor can be very slow. To adapt to this, attackers use scripts and set up automated downloads over Tor. They also use download managers and use POST's instead of GET's over HTTP to keep commands and other data out of web logs. Attackers have to be concerned with how to get reverse command and control shells without providing an attribution path to forensics and leaking information about themselves during the attack by doing personal email or chat. All of these things can tie the activity back to the attacker, and don't typically concern the White Hat at all.

Attackers also have to watch for dangerous data. Mail spools can be full of viruses that may infect the attacker if they are viewing the mail in a vulnerable client. Some targets are more sophisticated and may watermark or tag their documents with code that calls home in an attempt to uncover the attacker’s location or identity. In other cases, attackers have run across TAR files designed to overwrite home directories which could cause havoc on the incautious attacker’s system.

5.5 Maintaining Control

Attackers have an interest in maintaining control of the assets they have compromised. Intercepting data transfers and network communications is a high priority because it allows the victims to do the hacking for the attacker.

In general, using rootkits to maintain control is not advisable or commonly done by sophisticated attackers because rootkits are detectable, and their intent is unambiguously malicious. Strange behavior in the kernel that promotes stealth almost always indicates a compromise.

A better solution is to ensure re-exploitation of the target as needed through other means or to hide in plain sight and appear like normal user activity. This can be done in a variety of ways from modifying a seemingly innocuous binary to simply making sure to maintain current user credentials on the system.

Black Hats deal with these problems by doing things like constructing a non-network connected system with all the needed readers and data viewers, but no crucial data. Then they write the stolen data to a CD and move it to this stand-alone computer and view it there in relative safety. Some attackers might use a virtual machine as well. Attackers can also introduce subtle bugs instead of backdoor binaries. Modifying the source of a web or other application to simply be vulnerable rather than adding a communications channel is very difficult to detect and leaves the intent ambiguous.

Attackers can also choose to downgrade existing applications to known vulnerable versions. If a sysadmin is used to running VNC for remote access, they won't often check to make sure the version is the same one they installed. If organizations do their own vulnerability scans, however, this may be detected and fixed. Sometimes attackers re-enable common but disabled accounts such as guest or a service account. This kind of activity keeps the sys admins and incident response personnel guessing as to the state of their systems. If a compromise goes awry some attackers will go so far as to flood the box with worms, malware, scans and attacks to try to hide themselves and their real activity in the noise.

5.6 Other Attackers

From time to time a Black Hat may find another attacker on a system they have gained access to too. The first thing they do is to run a full intrusion analysis on the system to understand how the other attacker got there, and what activity they have performed. It is important to understand the other attacker’s reason for being on the box in case a system that didn't appear important turns out to be more valuable.

An attacker then might model their behavior after the other person on the system in an attempt to make their activity appear as if it is the other person doing it. That way if a forensic investigation is performed, they may only detect the one attack allowing the Black Hat to slip away.

Finally, the Black Hat may decide to locate and patch whatever hole the other attacker used and kick them out of the system in order to protect themselves from any mistakes the other attacker might make.

In one case known to the authors an attacker found that someone else had compromised his target and modified the login script to exclude certain hosts from logging. In this particular case the attacker simply added his own hosts to the script and monitored the other person's activity to copy it.

5.7 Anonymity

White Hats don't have to be concerned with anonymity for their attacks. Usually, they are authorized to perform the action and it’s desirable for the customer to know who it is. Often, they provide their IP address ahead of time.

Black Hats on the other hand are very concerned with anonymity. Hijacking available Wi-Fi signals is very common. Many wireless access points are configured with default usernames and passwords and so attackers will hop on the connection, access the WAP, modify the DMZ setting to point to their IP address. This facilitates the ability to receive reverse shells directly from the target.

Another technique is to find existing web shells on web servers that have been hacked by other people. Attackers will use them as launch pads for attacks against other systems and didn't have to hack these systems themselves.

Tor[17] is a system that is commonly used by attackers to remain anonymous while attacking systems. The Tor network carries a large amount of traffic, including porn, pirated software and other attacks. Some attackers will do all the recon of a target over Tor or similar anonymity networks in order to obfuscate where the traffic is coming from. Attackers will change IP's / identities often to keep the target logs from having a discernable pattern. By using 3rd party web-based port scanners and other tools an attacker can hit the target only from Tor, ensuring that attribution will be very difficult.

5.8 Never Caught

This section covers anti-forensics techniques and law enforcement evasion. This is another area that White Hats don't have to consider but which is very important to Black Hats. There is a whole field of study into how to evade being caught by law enforcement, which is beyond the scope of this paper, however a few examples will be given.

There is a concept called "alibiware" which essentially covers using technical means to provide oneself with an alibi while performing an attack. For example, attackers can be caught by their cell phone location and activity, so an attacker might place their cell phone in a desired location far away from where the attack originates from. He could then arrange to have a call made to the phone and the phone answered to "prove" he wasn't in the vicinity of the attack. The use of accomplices, however, can bring complications so one might use an auto-answer program for their smart phone instead.

Another trick is to buy a movie ticket and leave the movie early to go implement an attack. This way the attacker has "proof" that they were somewhere else. Many other scenarios along these lines can be concocted.

As far as anti-forensics goes, one of the most common techniques is to reset every timestamp on a system to the same date. Tools like Encase that are used for forensics rely heavily on file time/date stamps in order to separate malicious activity from normal. If all the dates are the same, no distinction can be made. There are tools to perform this activity such as Timestomp[18] which is part of the Metasploit Framework. Attackers have also been known to include exploits for Encase itself in order to compromise the forensic investigators or prevent them from investigating.

Some attackers will use memory resident only and staged command and control payloads in order to leave no file system traces. These tools can contain just enough code to receive and process the next section of code from the network in order to evade memory analysis. In combination with that they implement true SSL encryption so that an investigator will need full packet capture at the time of the attack as well as to be able to break the SSL in order to get an analysis of the command and control.

Chapter 6

Conclusions

6.1 What does this all mean?

Black hat Attackers can be very determined and will likely not stop in pursing their goals. They are extremely patient and will spend large amounts of time going after a goal. An attacker only has to succeed once where defenders have to always succeed. It is important to understand how attackers think and to realize that attackers test everything. Black Hats are not all powerful but know and use more tricks. Traditional White Hat testers are performing unrealistic tests and providing misleading reports to their customers. They do not emulate what real attacks do. Full scope penetration tests are a more realistic test of security posture, and the best value for the customer.

Bibliography

[1] Nessus - http://www.nessus.org

[2] Retina - http://www.eeye.com/Products/Redina.aspx

[3] CANVAS - http://www.immunitysec.com/products-canvas.shtml

[4] Core Impact - http://www.coresecurity.com

[5] Metasploit Project - http://www.metasploit.com

[6] Attack Research- http://www.attackresearch.com

[7] Offensive Computing - http://www.offensivecomputing.net

[8] Secure DNA - http://www.securedna.com

[9] Tactical Exploitation - blog.attackresearch.com/publications/hdmoore_valsmith_tactical_paper.pdf

[10] NMAP - http://www.insecure.org

[11] milw0rm - http://www.milw0rm.com

[12] Security Focus - http://www.securityfocus.com

[13] SecuriTeam - http://www.securiteam.com

[14] WordPress - http://www.wordpress.com

[15] Bots Vs Browsers - http://www.botsvsbrowsers.com

[16] eBay - http://www.ebay.com

[17] Tor - http://www.torproject.com

[18] Timestomp - http://www.metasploit.com/research/projects/antiforensics