HORNECYBER

SECURE PENETRATION TESTING OPERATIONS: DEMONSTRATED WEAKNESSES IN LEARNING MATERIAL AND TOOLS

PRE-PUBLICATION VERSION FOR CONFERENCE RELEASE | FOR THE FINAL REPORT, INCLUDING CODE AND DETAILED DESCRIPTION OF THE DEMONSTRATED TOOL, VISIT HORNECYBER.COM

WESLEY MCGREW, PH.D.
DIRECTOR OF CYBER OPERATIONS,
HORNE CYBER
WESLEY.MCGREW@HORNECYBER.COM
@MCGREWSECURITY

ABSTRACT

Following previous presentations on the dangers penetration testers face in using current off-the-shelf tools and practices (Pwn the Pwn Plug and I Hunt Penetration Testers), this paper and presentation explores how widely available learning materials used to train penetration testers lead to inadequate protection of client data and penetration testing operations. Widely available books and other training resources target the smallest set of prerequisites, in order to attract the largest audience. Many penetration testers adopt the techniques used in simplified examples to real world engagements, where the network environment can be much more dangerous. Malicious threat actors are incentivized to attack and compromise penetration testers, and given current practices, can do so easily and with dramatic impact.

The accompanying presentation to this paper includes a live demonstration of techniques for hijacking a penetration tester's normal practices, as well as guidance for examining and securing penetration testing procedures. The tool shown in this demonstration will be released publicly (with code) along with the first presentation of this talk.

INTRODUCTION

This paper is a companion piece to the talk of the same title. In both this paper and the correlating talk, previous work is presented, followed by a review of the threats to penetration testers. A study was performed on a large body of penetration testing learning materials, illustrating the lack of secure practices being taught—practices that have been observed to be repeated on real engagements.

Recommendations are made for improving secure processes. Finally, a tool is presented that illustrates the threat that penetration testers face. This is demonstrated live in the corresponding talk, showing how penetration testers' post-exploitation activities can be easily hijacked by attackers.

PREVIOUS WORK

Vulnerabilities in penetration testing tools, techniques, and devices have been explored in two prior talks by the author:

- DEF CON 21 – Pwn The Pwn Plug: Analyzing and Counter-Attacking Attacker-Implanted Devices[1]
- DEF CON 23 – I Hunt Penetration Testers: More Weaknesses in Tools and Procedures[2]

In Pwn the Pwn Plug, an off-the-shelf penetration testing device meant to be hidden and left behind within an organization was analyzed for vulnerabilities that would affect the security of operating it in this configuration. In the "left behind" scenario, the device is uniquely susceptible to tampering and monitoring by third-parties with physical access to the same locations. It was established and demonstrated in this talk that the vulnerabilities were not simply limited to physical access: third party attackers could remotely execute commands on the device through a combination of vulnerabilities in the penetration tester's user interface to the device. In this, the first talk on the subject, the work was presented both in terms of targeting penetration testers, as well as in the context of incident response: performing forensics on malicious threat actors' implanted devices.

In the next talk, I Hunt Penetration Testers, focus was placed on the security of penetration testers that use software and hardware tools on remote and in-person engagements. In this talk, a set of common security tools were examined to determine the inherent safety of their default configurations and options. It was determined that many penetration testing tools lack, at least by default, the capability to secure command-and-control information and sensitive client data both in transit and at rest. Scenarios were described that illustrate why a malicious threat actor would find a penetration testing firm to be an attractive target. Finally, a vulnerability was demonstrated that allows attackers within range of the popular WiFi Pineapple device the ability to remotely gain control of it. This illustrated the risks of operating in hostile network environments with devices that have not been hardened.

This talk, Secure Penetration Testing Operations: Demonstrated Weaknesses in Learning Material and Tools, builds upon the previous work by exploring the root causes of insecure practices in penetration testing, practical demonstration of more vulnerabilities in common procedures, and recommendations for more secure practices for engagements. It is worth mentioning that the closer examination of post-exploitation payloads undertaken as part of the work for this talk reveals that the dangers posed by current practices in the use of these payloads/agents is far worse than was described previously in I Hunt Penetration Testers.

THE THREAT

Previous presentations on this topic have established a description of the threat model for malicious third party actors targeting penetration testers. While the purpose of this talk is not to retread ground, it is worth briefly revisiting some of the major points for the purposes of defining the scope and motivation behind this paper.

In I Hunt Penetration Testers, it was proposed that penetration testing professionals and firms represent attractive targets due to their level of access to client organizations and their position outside of the rules of normal

business operation. Penetration testers are expected to break rules, elevate privileges, and perform exfiltration of sensitive data. For these reasons, a penetration test can serve as an opportunity both for cover and for the opportunity to discover vulnerabilities "over the shoulder" of a penetration tester.

Penetration testers, apart from their clients, might be the target of compromise as well. More advanced testers might be in possession of tools and exploits that are not publicly available and would represent a value to the attacker. As security professionals, a compromise of a penetration tester also represents an embarrassing situation if made public by a hacktivist or other malicious party. While the focus of earlier talks on this topic were on compromising penetration tester tools themselves, the demonstration in this talk, and the questions examined about learning material are focused on weaknesses in procedures opening up access to client systems and data.

WE OPERATE AS WE LEARN – A SURVEY OF PRACTICES IN PUBLICLY AVAILABLE RESOURCES

While some standards documents exist for penetration testing [3,8,9,10], most circumstances and requirements for penetration testing do not currently require rigorous adherence to formal standards. Existing documents of this nature generally describe phases of a penetration test, but stop short of providing hard requirements for all tests. In this way, these documents largely constitute "guidance" (as described in the PCI supplement on penetration testing [10]) more than serving as standards to be met.

This is appropriate in some ways, as the value in a penetration test is only realized when an experienced and talented team is able to use human ingenuity to find vulnerabilities in complex systems where an automated scan simply would not provide value. Current guidance/standards allows for the flexibility needed to do this. The mind's capability to intuit the intended and unintended operation of software written by other humans, recognize patterns in complex data, and apply complex ad-hoc processes to solve problems (i.e. the location and exploitation of vulnerabilities) all contribute to a penetration testing team providing results that cannot be obtained using an automated vulnerability scanning tool. A formal standard for conducting tests would not be able to encompass the breadth and depth of potential activity, and would therefore be counterproductive.

While the lack of a formal standard does not impair the technical value of penetration testing, it does result in a lack of rigor. Without defined expectations for protecting the security of client data and systems, to say nothing of the operations of the penetration testing individual of the firm, there is no control on the low bar for such protection. Without a standardized set of expectations, we fall back upon what is most convenient or expedient to implement. In this work's examination of operational security issues in penetration testing in learning and reference materials, standards documents did address some, but not all issues of security in penetration testing. Out of the standards documents surveyed, the open source Penetration Testing Execution Standard addressed more issues of client and penetration test operational security than the rest, including the protection of client data in transit, client data at rest, operational security during the intelligence gathering phase, communications security for contact with client staff, and the security of client systems during and after the test.

If we look to current and common practices in safely (or, not so safely) conducting penetration testing, it is reasonable to expect that most testers will conduct their tests in accordance to their background and training. There are no requirements for formal education to enter the profession, nor are there very many formal programs that extensively cover offensive security testing. Training programs in penetration testing (taught in a matter of days or weeks)

typically have few pre-requisites. While this paper will avoid bemoaning the minimal depth or breadth of background knowledge required or gained by most new penetration testers, it is safe to say: for many, their tools and techniques will be defined by the learning material they have used without much improvisation or improvement.

If we consider that most penetration testers will tend to operate in a way that is consistent with the material they learned from (and continue to reference), then we can draw conclusions on the security of common penetration testing techniques by examining that material. For this paper and talk, a selection of popular books and training material on penetration testing was examined with the goal of applying a set of feature-extracting questions. These questions are designed to determine the presence and nature of operational security advice for penetration testers that is contained within material used to learn the profession.

The questions are as follows:

1. **[Host Security – Penetration Tester]** Does the work address precautions for preventing penetration testers' systems from being compromised? Describing how to set the Kali/Backtrack password is not, by itself, sufficient for this to be a "yes".

2. **[Host Security – Client]** Does the work address precautions for maintaining the security of client systems during the test? Penetration testing procedures should not leave the tested systems in a more insecure state then they were in when the test began.

3. **[COMSEC]** Does the work address establishing secure means of communicating with the client about the engagement? This would include emergency contact and report delivery, as well as any other email or teleconferencing.

4. **[Client Data in Transit]** Does the work address issues surrounding the transmission of sensitive client data between targets and penetration testers' systems in the course of the engagement? This would include data that is being extracted for proof of impact, as well as information about the hosts that would be transmitted across command-and-control channels.

5. **[Client Data at Rest]** Does the work discuss procedures for securing client data at rest, during and/or after the engagement? This includes data that has been extracted from targets and stored on penetration testers' workstations and penetration testing devices. Procedures might include encryption, hardening, and/or secure deletion.

6. **[OSINT OPSEC]** Does the work address operational security during intelligence gathering phases? This would address confidentiality of the information one might be transmitting about the client in the course of seeking information about the client from publicly available sources.

7. **[Potential Threats]** Does the work address issues with conducting tests against systems over hostile networks, such as the public Internet or unencrypted wireless?

8. **[Insecure Practices]** Does the work demonstrate or teach at least one example of an insecure practice without describing how it might leave the tester or client vulnerable?

OBSERVATIONS FROM EXAMINING LEARNING MATERIAL

This section discusses the results of examining a set of material with the goal of answering the above questions. This set of material included 16 books, four standards/guidance documents, and the publicly-available material for three classes. The stated goal, of all of these works, is to serve as learning or training material for penetration testing. All of the materials used for this study are publicly available outside the context of a paid training

class. Paid training classes' material were not studied as a part of this work due to usage agreements and a lack of easy access (at a reasonable cost) to recent materials for the purposes of this study. This is not seen as a significant loss, however, as it is in the author's experience that such classes do not differ greatly from publicly published material with regards to this study.

This paper does not disclose the titles, authors, or sources of the works examined, as the point of this study is to demonstrate an across-the-board lack of focus on the security of penetration testing procedures in works that many new testers are using to build their skill set, rather than to describe the deficiencies or virtues of one set of material over another. While moving forward, it is important for new material to incorporate secure practices and describe the due care needed in testing, it might be unfair to point out specific works as being "bad" when there was no widespread education/ understanding of the risks at the time the content was created.

METHODOLOGY

The methodology used for this study was to examine how each work addresses the eight questions posed. Standards/ Guidance documents were chosen through internet searches and references to penetration testing standards documents identified and used in other recent work on this topic. Class material was gathered from publicly available materials not encumbered by usage agreements. Books were gathered based on popularity in Amazon searches for penetration testing books. A brief examination of each studied work was made to verify that it directly stated its purpose as being a learning resource for penetration testers. In the results, no distinguishing markings are made for the different types of material (standards/guidance, classes, books), as each, for the purposes of this study, serves the same role as learning materials that penetration testers will implement in practice.

Reading and analyzing every sentence on every page of every targeted work in the context of the eight questions would make the duration of the study prohibitively long. Therefore, the examination of each work was performed in two phases. The first phase took the approach of examining the table of contents to determine sections that seemed likely to contain information that would provide a positive answer to each question, and then examining those sections for the information is being sought.

After this initial phase, to more exhaustively test the remaining questions, each page of the work was briefly examined (in most cases on the order of a few seconds) to seek out text relevant to the security of penetration testing procedures. With the author of this paper's experience in quickly consuming written works, and the ease at which relevant coverage should be identified, this approach, while subjective, should be considered fair. The potential for false negative results should be considered with the justification that coverage of secure penetration testing practices should have been easily located, if that coverage was meant to be effective.

For simplicity in illustrating the point of this paper, a simple "yes" or "no" was recorded for each studied work and each question. The threshold for "yes" was intentionally very low. For example, a single paragraph in a book of over five hundred pages on the topic of encrypting a report for transmitting to a client would be sufficient for a "yes". While this may exhibit positive results for studied works that do not provide an extensive coverage of these topics, it causes the results of the study as a whole to more effectively demonstrate the negative case: that a large amount of resources available to learn penetration testing techniques do not have any coverage at all of these concerns.

RESOURCE	1 - HOST - PENETRATION TESTERT SECURITY	2 - HOST SECURITY - CLIENT	3 - COMSEC	4 - CLIENT DATA - IN TRANSIT	5 - CLIENT DATA - AT REST	6 - OSINT OPSEC	7 - POTENTIAL THREATS	8 - INSECURE PRACTIICES
1	Y	N	N	N	Y	N	N	N
2	N	N	N	N	N	N	N	Y
3	N	N	N	N	N	N	N	Y
4	N	N	N	N	N	N	N	Y
5	Y	Y	Y	Y	Y	Y	Y	N
6	N	N	N	Y	Y	N	N	Y
7	N	N	N	N	N	N	N	Y
8	N	N	N	N	N	N	N	Y
9	N	Y	N	N	Y	N	N	Y
10	N	N	N	N	N	N	N	Y
11	N	N	N	N	N	N	N	Y
12	N	N	N	N	N	N	N	Y
13	N	Y	Y	Y	Y	Y	N	N
14	N	N	N	N	N	N	N	Y
15	N	N	N	N	N	N	N	Y
16	N	N	N	N	N	N	N	Y
17	N	N	N	N	N	N	N	Y
18	N	N	Y	Y	N	N	N	Y
19	N	Y	N	Y	Y	N	N	Y
20	N	N	N	N	Y	N	N	Y
21	N	N	N	N	N	N	N	Y
22	N	N	N	N	N	N	N	Y
23	Y	N	N	Y	Y	N	N	Y

This chart represents the results of applying the study methodology to the resources selected. For questions 1 through 7, “Y” indicates that the topic was addressed in the work (and is colored green as a positive result), “N” indicates that it was not (colored red as a negative result). For question 8, “Y” indicates that vulnerable practices were taught without disclaimer, and those cells are colored in red, opposite to the rest of the columns (as the “Y” response is negative in this context). For question 8, “N” indicates that no vulnerable practices were taught. If the “N” for question 8 is colored yellow, the resource did not cover any technical matters of penetration testing and focused only on procedural issues.

ANALYSIS

As a whole, it is straightforward to look at the chart and come to the conclusion that concerns about the security of penetration testing operations are not a well-covered part of most available learning resources. Out of 23 works studied, 14 works did not address any of the basic issues put forward in the questions. Only four works addressed more than two.

Almost every single work in the study describes practices that, if conducted across the public Internet or other hostile network, could result in the disclosure of client information, systems, or the penetration tester's system to malicious third parties. By simple "yes"/"no" results, three works did not describe weak practices. The one color coded in green followed descriptions of potentially dangerous actions with a warning about performing those actions across unencrypted networks. Of the two that are color coded in yellow, one did not cover technical practices, only focusing on procedure. The other did not discuss insecure practices by virtue of being fraudulent: a self-published Kindle book that consisted only of material on terminology that appeared to be from various online sources, with no instruction whatsoever on technical or operational matters of penetration testing.

The most common insecure practice described was the usage of post-exploitation payloads (especially those built into Metasploit, since it is so popular) that allow for third-party monitoring and hijacking. The Metasploit project contributors are aware of (and have discussed publicly) the potential for these kinds of attacks, and have developed new functionality for the Meterpreter payload to secure its command-and-control [7]. With "paranoid mode" Meterpreter functionality only being added within the past year, it was not unexpected to see many works describe insecure practices for command-and-control of client systems. It is, however, not impossible and would have been desirable to have seen discussion of the risks, along with guidance for conducting tests locally, over VPNs, or other secure tunnels. The demonstration in the companion talk to this paper demonstrates hijacking post-exploitation command-and-control.

Beyond what was expected, a number of books described practices that represent an even clearer danger to the security of communications and client systems than was expected. Anecdotally, the following notably insecure practices were described in the context of penetration testing:

- The use of online hash cracking services
- The use of plaintext FTP services opened up on penetration testers' systems for transferring payloads and the exfiltration of client data
- Persistent netcat listeners running on client systems, backed by shells, without authentication, and left open for later access by penetration testers
- The use of unencrypted web shell backdoors to maintain access to target systems
- Plaintext command-and-control between penetration testers' workstations and devices left behind in the target's physical/network space
- The use of Tor and/or public proxy lists found through search engines to find proxies through which attacks could be anonymized.
- Enabling a Windows telnet daemon for continued access to a system

A single resource addressed all of the questions, and did not present any technically insecure practices without also having some description of the risks inherent to those practices. While for the overall purpose of this study, the titles and authors of the works are not disclosed, in this specific case it is worth pointing out that *Professional Penetration Testing, Second Edition, by Thomas Wilhelm* [12] is the work that managed to address each point (row 5 in the chart). While this is not a book review, and the work was not read thoroughly for its overall quality, it is commendable that there is at least some mention of the potential problems that penetration testers face with security.

CONDUCTING SECURE PROFESSIONAL PENETRATION TESTS

Practices can be adopted to minimize the risk that penetration testers face with regards to the security of their own operations, as well as the operations, communications, and data security of their clients. The following recommendations relate to the questions posed in this paper's study and are described such that, with an expected degree of effort, they can be integrated into the workflow of a professional penetration testing firm.

CLIENT COMMUNICATIONS SECURITY IN SCOPING, PROGRESS UPDATES, EMERGENCY, AND DELIVERY

Initial meetings to discuss and scope upcoming penetration tests should establish secure means by which clients and testers can communicate. If both parties already have the capability, end-to-end encrypted email would be recommended. If the capability does not already exist with the client, a secure HTTPS file sharing solution hosted by the penetration tester could be used by both parties to transfer sensitive network information for scoping, as well as reports later on. For emergency contact, mechanisms that are out-of-band from the client network are necessary, such as a mobile phone, though when possible and as time and circumstances allow, sensitive data should be exchanged through more secure means.

OPEN SOURCE INTELLIGENCE GATHERING OPERATIONAL SECURITY

During open source intelligence gathering efforts, careful consideration should be given to the set of search terms being used, and where they are being submitted. While company names and other non-sensitive information can serve as appropriate search terms, testers should be careful as they branch out using information they've derived from a combination of sources. Note that search terms typically passed along to sites as part of the referral URLs provided by the web browser. Take measures to prevent the nature of your search from being apparent to the sites that you visit. If the identity of the penetration testing firm can be deduced from the IP address performing OSINT, information that ties that firm to a current engagement with a client can leak out, as well.

Carefully consider what actions are taken over TOR or other proxy systems. Do not search for or view information over such systems that you would not want the unknown operator of an exit node or proxy to also view. In most cases, it should be understood by the target organization that you will be conducting operations using your own resources, so it may not be necessary (or appropriate) for you to proxy activities over third party connections.

POTENTIAL THREATS, CLIENT DATA IN TRANSIT, AND INSECURE PRACTICES

All members of the penetration testing team need to be aware of the network environment in which they are operating. In tests that are conducted across the Internet, unencrypted wireless, or other transports that are not under penetration tester or client control, those networks must be assumed to have malicious threat actors participating in them. The penetration tester and the target do not exist in a vacuum.

When tests occur over these uncontrolled networks, care must be taken to ensure that when command-and-control is established, that it cannot be monitored or hijacked. If client data is the target for exfiltration, that data must be transferred over a secure channel. If tools that are naturally insecure (as described in I Hunt Penetration Testers) are used, all attempts should be made to tunnel that tool over a more secure protocol.

This solution is not perfect, in that a third party might identify the initial vulnerability by which a tester compromised a system. In some cases, this may be unavoidable when the end goal is to identify all of the vulnerabilities an attacker might be able to exploit. It is recommended, however, that when circumstances allow, the test should be conducted from a position on the network that is as close as possible to the client being tested. Performing a test on-site is one option, though a similar result can be obtained by using an appliance designed to "phone home" securely back to the penetration testers, allowing them to conduct their test over a VPN connection to appropriate points just outside of (or within) the client network.

PENETRATION TESTER HOST SECURITY

Penetration testers should be aware of the attack surface that their tools represent. Many penetration testing tools act as servers for agent software, exposing to a third party attacker an interface that they can interact with. Many tools are primarily developed as proof-of-concepts for vulnerabilities, and have not been designed with the goal of providing security, reliability, and resilience in operational use by penetration testers. Penetration testers should routinely examine their own systems, tools, and practices to determine what opportunities a third party would have to subvert them.

CLIENT HOST SECURITY

Penetration testers should take great care in not creating more vulnerabilities in target systems than already exist. The necessity of persistence mechanisms should be determined as a balance between the need to maintain access to systems balanced against the stability of re-exploiting certain vulnerabilities. While memory corruption attacks have the potential to crash a system when exploited many times in succession, most web-based vulnerabilities are much more reliable. While it should be needless to say that access and persistence mechanisms should only be accessible by the penetration tester, and not third parties that happen to find them, it is clear from this paper's study that it does need to be stated.

CLIENT DATA AT REST

After exfiltration, data gathered from clients should be stored on penetration testers' systems in a controlled way. In addition to the controls recommended for securing penetration testing workstations, devices that are outside the physical control of testers should not be used to store client information for any longer than is necessary. Such devices can be physically compromised, or become the targets of remote compromise (as disclosed in the two previous talks on this subject).

After an engagement, it is recommended that only a minimum amount of information about the client should be kept long-term. This is something that must be discussed with a client prior to an engagement to set appropriate expectations. There will certainly be something left, if only agreement documents proving the test actually occurred, alongside the report. More may be stored if there if engagements are meant to be on-going or recurring periodically. Any remaining data should be protected with encryption and access controls, and anything that is to be discarded should be wiped securely.

DEMONSTRATING ATTACKS ON PENETRATION TESTERS

This section describes a tool that part of the live demonstration of the talk that corresponds to this paper. The attack that is demonstrated by this tool illustrates threats to penetration testing operations that, while known to be technically feasible,

are not normally considered during an engagement. While one should not feel ashamed to find enjoyment in seeing or presenting something being hacked on stage, these demonstrations and tools serve the additional goal of raising awareness and, hopefully, forcing the issue of increased rigor in penetration testing learning material, operations, and client expectations.

TO DOWNLOAD THIS TOOL AND THE LATEST COPY OF THIS WHITEPAPER WITH MORE DETAIL ON ITS USE, VISIT HORNECYBER.COM.

Snagterpreter – Hijacking HTTP and HTTPS Meterpreter Sessions

Metasploit is the most featured and mature free platform for the development of exploits as well as operationally conducting a wide variety of penetration testing activities [4]. The most fully featured post-exploitation payload for Metasploit is the Meterpreter agent, which provides many more features than the typical reverse shell payload used by traditional stand-alone exploits. Meterpreter has features that provide resilience for the connection between the penetration tester and their target, evasion of both host and network based detection, and a rich set of post-exploitation and exfiltration capabilities [5]. Given their capabilities, stability, and ease of use, the combination of Metasploit and the Meterpreter payload are a ubiquitous part of most testers' training, no matter how brief.

Meterpreter sessions frequently take place across hostile networks, including the public Internet. Such sessions are valuable to a third party attacker that would seek to seize control of the same systems that have been compromised by the penetration tester. Such sessions might be the result of more than direct exploitation of external-facing systems, in the case of post-exploitation pivoting or social engineering, and therefore represent more than just an extension of existing and accessible vulnerability that a third party could exploit in parallel to the tester's activities. For these reasons, Meterpreter sessions must be considered as part of the attack surface that a malicious threat actor "shadowing" a penetration tester would seek to compromise.

Meterpreter sessions operate using a Type-Length-Value (TLV) protocol for issuing commands and responses, and can operate over a variety of transport mechanisms. The most common means configured for a Meterpreter agent to communicate to a penetration tester's system are direct reverse TCP sessions (using a TCP socket directly), HTTP, and HTTPS. While the "reverse TCP" transport is commonly presented in learning material that predates (or is sourced from material that predates) the addition of HTTP/HTTPS transports to Meterpreter in 2011, the use of HTTP/HTTPS is considered to be generally more desirable for reasons of being more resilient (requests can be broken up among separate stateless HTTP requests) and stealthy (such traffic blends well with "normal" traffic in an organization) [6].

While most common configurations of the Meterpreter agent support obfuscation and encryption of traffic, it is (in these configurations) for the purpose of evading detection, rather than to protect the session from monitoring or hijacking. In this context, exclusive-or obfuscation of traffic is used, as well as SSL sessions that do not require the presence of trusted certificates. The Metasploit developers are well-aware of the security issues (even if the end users are not necessarily as cognizant), demonstrated by a recent change, as of June 2015. Meterpreter can now be configured in a "paranoid mode" that requires the agent to verify the signature of the SSL web server that it is connecting to, allowing the penetration tester to deploy agents that will only complete connections to a verified listener. This mode is not yet widely used, however, due to it being a recent development as well a lack of general understanding of the susceptibility of non-"paranoid mode". A Google search for meterpreter "paranoid mode" on 3/1/2016 resulted in less than 400 hits, the vast majority of which were not relevant to this feature, or reproduced the text of the Metasploit project's description of the feature.

The Snagterpreter tool, developed by the author for this talk, gives an attacker in a position to monitor and modify traffic on a hostile network between the penetration tester and their target the ability to hijack non-"paranoid mode" Meterpreter sessions that have already been established. Snagterpreter supports hijacking Meterpreter sessions using the HTTP and HTTPS transports, and hands over interactive control of the session to the attacker. Once the attacker is done with a session the session can usually be returned to the penetration tester for continued and expected operation.

The attack demonstrated by Snagterpreter can be mitigated most effectively by configuring Meterpreter payloads to use "paranoid mode". Instructions for this can be found in the Metasploit wiki [7]. In the absence of using "paranoid mode" (which is newer than most learning materials used by penetration testers) a reasonable mitigation would be to avoid or minimize situations in which a malicious actor could intercept traffic. No materials reviewed made any reference to the potential or mitigation for attacks of this type.

CONCLUSIONS

In the course of this paper, and the corresponding presentation and demonstration, we have examined previous work in explaining the threats that penetration testers might encounter on engagements, and the risk posed to the testers and their clients. A study was undertaken of the most popular learning and reference materials for penetration testers, and significant shortcomings were found in guidance for securely conducting engagements. Recommendations have been made for improving the security of tests moving forward. Finally, a tool has been developed to demonstrate the very real risk that can be realized by using insecure practices.

For a profession that specializes in reporting on vulnerabilities, it is important that a penetration testing firm should have its own house in order. You cannot have it both ways: you can't report on vulnerabilities exploitable in situations involving malicious actors on the Internet intercepting and modifying traffic without also considering those scenarios in attacks on penetration testing operations. In order to provide secure services for clients, efforts must be made to improve tools, techniques, and processes. In turn, improvements must be made in training and reference material that define standard procedures.

REFERENCES

[1] Wesley McGrew, Pwn The Pwn Plug: Analyzing and Counter-Attacking Attacker-Implanted Devices, DEF CON 21, https://www.defcon.org/images/defcon-21/dc-21-presentations/McGrew/DEFCON-21-McGrew-Pwn-The-Pwn-Plug-WP.pdf

[2] Wesley McGrew, I Hunt Penetration Testers: More Weaknesses in Tools and Procedures, DEF CON 23, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Wesley-McGrew-I-Hunt-Penetration-Testers-WP.pdf

[3] Multiple authors, The Penetration Testing Execution Standard, http://pentest-standard.org

[4] Metasploit: Penetration Testing Software http://metasploit.com

[5] Metasploit Framework Wiki, Meterpreter, https://github.com/rapid7/metasploit-framework/wiki/Meterpreter

[6] HD Moore, Meterpreter HTTP/HTTPS Communication, https://community.rapid7.com/community/metasploit/blog/2011/06/29/meterpreter-httphttps-communication

[7] Meterpreter Paranoid Mode, https://github.com/rapid7/metasploit-framework/wiki/Meterpreter-Paranoid-Mode

[8] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment,

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

[9] ISECOM, OSSTMM 3 – Open Source Security Testing Methodology Manual,

http://www.isecom.org/research/osstmm.html

[10] Penetration Test Guidance Special Interest Group, PCI Data Security Standard – Information

Supplement: Penetration Testing Guidance,

https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

[11] The Penetration Testing Execution Standard, http://pentest-standard.org

[12] Thomas Wilhelm, Professional Penetration Testing, Second Edition

ABOUT THE AUTHOR

Wesley McGrew, Ph.D.

Wesley serves as the director of cyber operations for HORNE Cyber Solutions. Known for his work in offensive information security and cyber operations, Wesley specializes in penetration testing, network vulnerability analysis, exploit development, reverse engineering of malicious software and network traffic analysis.