International Journal of Advanced Science and Technology
Volume 8, July, 2009

Penetration Testing for Hire

[1]Debnath Bhattacharyya and [2]Farkhod Alisherov A.

*[1]Computer Science and Engineering Department, Heritage Institute of Technology,
Kolkata - 700107, India.
[2]Department of Multimedia Engineering
Hannam University, Daejeon, South Korea
[1]debnathb@gmail.com, [2]sntdvl@yahoo.com*

Abstract

With the familiarization of the penetration testing, more and more companies look for professionals in penetration testing to perform a penetration test. While professional skills are required in order for the test to be effective, certification of the penetration tester or penetration team is required and is more and more demanded. This paper suggests a methodology in choosing a penetration tester or a penetration testing team, and a brief certification listing is given.

Keywords: *Penetration Testing Personnel, Penetration Testing.*

1. Introduction

In today's digital data arena, where corporate empires are being built with people's personal information, penetration testing is a necessary function for every Security Department. Penetration testing needs to be thought of and discussed. The empires' data needs to be protected. No longer can we rely on firewall implementations as the answer to privacy. Misconfigurations, exploits, updates, patches, backdoors, disgruntled employees - all are driving reasons for the need for penetration testing.

The process of carrying out a penetration test can reveal sensitive information about an organization. It is for this reason that most security firms are at pains to show that they do not employ ex-black hat hackers and that all employees adhere to a strict ethical code. There are also several professional and government certifications that indicate the firm's trustworthiness and conformance to industry best practice.

Some managers have a romanticized image of what a tester does. They envision consultants huddling in an equipment-filled room, trying to break into a network the way a hacker would. In keeping with this view, these managers tell the tester they will not give him any information about their network so they can approach it “realistically,” to find out what a hacker would actually be able to do.

If a tester agreed to this premise, the organization may not obtain a true picture of their environment’s security. Hackers have an unlimited amount of time to probe a network for weaknesses, while a consultant is restricted by a budgeted amount of hours. Also, consider how extensive the IT network is in a large organization. In an environment of, say, more than 500 servers, a hacker could randomly stumble onto a point of entry that might never be discovered by a tester with limited time and not know where the most sensitive information is stored.

A penetration test or vulnerability assessment performed under these conditions could leave the organization with a false sense of security. The wise course of action is for an organization to share with the tester the complete picture of how the network is mapped and how the system is secured. Disclosing this information may help prevent accidents during the testing. For example, some organizations may have old network equipment or may be running old operating-system software that cannot handle the traffic created by port scans or vulnerability scans.

Obviously, it is hard to predict the likelihood of anything going wrong, but some accidents can be avoided by working from a solid foundation of information. The probability of accidents occurring is typically higher in penetration tests. Because these test how personnel respond to potential security threats, some organizations, although not all, choose to perform penetration tests without informing IT personnel. (Vulnerability assessments are usually more extensive in scope and IT personnel are typically informed in advance and prepared for action if a system is in danger of failing.) For penetration tests, it is good practice to at least inform employees from departments such as security, internal audit and IT (most likely the chief information officer). By being informed, the organization will better understand how the tester compromised the system. Later, when the tester has issued a report, internal employees can draw on their knowledge to help interpret and communicate the test results to the organization.

The tester also benefits when department representatives observe his/her work and provide crucial information otherwise unknown to the tester. Knowledgeable employees can help manage the risk by identifying older “legacy” equipment that may be too fragile to scan. In addition, selected personnel can inform the tester about the relative business value of the system or servers. A representative from research and development areas could identify the location of intellectual property data whose security carries a high risk to the organization.

Using this diverse input, the tester will write a more meaningful, persuasive report on the findings. For example, the company would learn whether a Web server with a particular business function was vulnerable to penetration, posing a specific business risk. A representative from Human Resources may be included in planning when a penetration test involves “social engineering” (the tester attempts to trick an employee into giving him access or divulging information that will help him gain access). This would include access to an IT system (getting the employee to divulge a user ID and password) or physical access to the building (slipping in an unsecured entrance and pretending to be an employee). Human Resources personnel can play a role in calming emotions in the test’s aftermath, when employees express hurt feelings about being tricked or fear their job is at risk. Testers should not report individuals who divulge information but instead report the statistics. If 20 employees are contacted, and 15 divulge their password, it is clear that the employees’ behavior is a symptom of a more serious root cause, such as an ineffective training program.

The extent of Internal Audit’s involvement likely depends on whether they sponsored the test or not. Ultimately, it is the IT department’s responsibility to ensure the system’s security; they should not rely on Internal Audit to validate their work. While Internal Audit will not be considered the owner of the controls, it is important for auditors to assume some responsibility for making sure IT has fixed everything that it promised. Ideally, the two departments’ responsibilities complement each other. For example, in a high-risk environment, IT might complete vulnerability assessments on a quarterly basis while Internal Audit reviews IT’s methodology and performs penetration tests to validate that problems have been remediated.

There is often a genuine need for Internal Audit to sponsor its own tests. It is not unusual for consultants to find an IT department running vulnerability assessments each quarter – or even every month – while the security problems identified still are not fixed.[1]

2. Choosing personnel

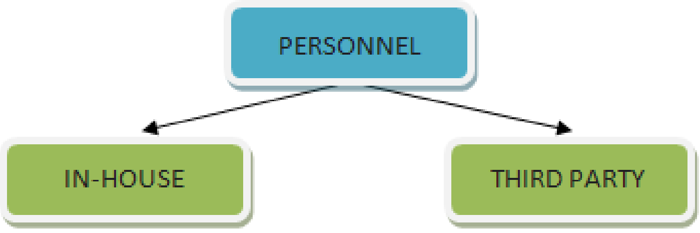

Figure 1. Proposed methodology model

In-house. If the company is hiring a penetration tester into their IT team, then the tester should have the appropriate requirements

- Deep knowledge of application and network penetration testing tools and exploits to identify vulnerabilities and recommend effective corrective actions.
- Excellent report-writing skills.
- Ability to explain technical issues to a non-technical audience after the test
- Outstanding customer relationship management skills
- Knowledge of databases and popular web applications
- Familiarity with more than one operating system (Windows/Linux/*nix)
- Good training skills Minimum 2 years experience in application and network penetration testing
- Understanding of the legalities involved in testing

It is also desirable if the tester has the following competencies:

- Security testing tool development
- Exploit development
- Network design and review experience
- Source code review experience
- SCADA testing experience
- Bluetooth testing experience
- Blackberry testing experience
- Wireless testing experience
- VOIP testing experience
- Visualization experience (VMWare, XEN, UML)

For the third-party penetration testing, to know which supplier is good for the client, the client should ask himself the following questions:

As an absolute fundamental when choosing a security partner, first eliminate the supplier who provided the systems that will be tested. To use them will create a conflict of interest (will they really tell you that they deployed the systems insecurely, or quietly ignore some issues).

- Is security assessment their core business?

- How long have they been providing security assessment services?
- Do they offer a range of services that can be suited to the client’s specific needs?
- Do they perform their own research, or are they dependent on out-of-date information that is placed in the public domain by others?
- What are their consultant’s credentials?
- How experienced are the proposed testing team (how long have they been testing, and what is their background)?
- Do they hold professional certifications, (PCI, CISSP, CISA, and CHECK)?
- Are they recognized contributors within the security industry (white papers, advisories, public speakers etc)?
- Are the CVs available of the team that will be working on the client’s test?
- Do they have a standardized methodology that meets and exceeds the common ones, (OSSTMM, CHECK and OWASP)?
- What is their policy on confidentiality?
- Are references available from satisfied customers in the same industry sector?
- Does the supplier maintain sufficient insurance cover to protect the client’s organization? [2]

3. Certifications

There are many certification that are more and more required by the organizations, that are hiring penetration testing professionals. These certifications are required to separate “amateurs” from “professionals”.

Three certifications have been produced by the International Council of E-Commerce consultants (EC-Council). These included the Certified Ethical Hacker course, Computer Hacking Forensics Investigator program, License Penetration Tester program and various other programs, which are widely available worldwide. These certifications have received endorsements from various American government agencies including the US Federal Government via the Montgomery GI Bill, and the US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) certifying EC-Council Network Security Administrator (ENSA) program for meeting the 4011 training standard for information security professionals.

SANS provides a wide range of computer security training arena leading to a number of SANS qualifications. In 1999, SANS founded GIAC, the Global Information Assurance Certification, which according to SANS has been undertaken by over 20,000 members to date. SANS offers the Security 560 Network Penetration Testing and Ethical Hacking class, which it says is "one of the most technically rigorous courses offered by the SANS Institute." The corresponding certification is the GIAC Certified Penetration Tester (GPEN). SANS also offers the Security 542 Web App Penetration Testing and Ethical Hacking class. The corresponding certification is the GIAC Web Application Penetration Tester (GWAPT).

Government-backed testing also exists in the US with standards such as the NSA Infrastructure Evaluation Methodology (IEM).

For web applications, the Open Web Application Security Project (OWASP) provides a framework of recommendations that can be used as a benchmark. [3]

National Security Agency IAM (Information Assessment Methodology) and IEM (Information Evaluation Methodology): Both of these certifications cover the excellent IEM/IAM methodologies in grueling detail. The certifications involve classroom training, group activities, presentations to peers on assessments (think intelligence briefings), and written exams. These certifications form an impressive foundation for risk assessment skills.

Operating System Specific Certifications such as a MCSE, RHCE, etc. and vendor-specific certifications like CCNA, CCIE are very desirable. The more a candidate knows about the operating systems, devices and applications they are testing, the better.

ISACA has two great certifications that show knowledge of information systems management (CISM Certified Information Systems Manager and CISA Certified Information Systems Auditor).

Familiarity with the Guidelines on Network Security Testing from NIST (The National Institute of Standards and Technology) is an excellent baseline. These guidelines are published in Special Publication 800-42, and are a bit less comprehensive that the OSSTMM model. Testers familiar with 800-42 are typically more knowledgeable about working with regulatory agencies and their specific testing and auditing requirements.[4]

Following chart provides the 3-month moving average for salaries quoted in permanent IT jobs citing Penetration Testing within the UK

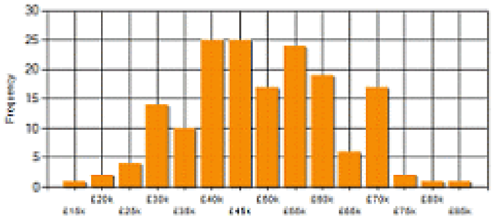

Figure 1. Quoted salaries

The following chart provides a salary histogram for IT jobs citing Penetration Testing over the 3 months to 21 May 2009 within the UK.[5]

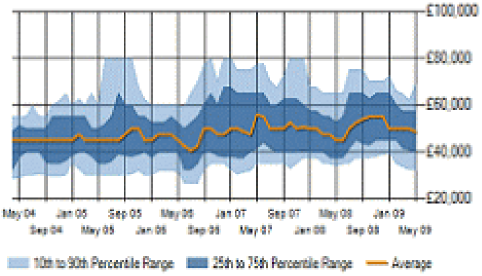

Figure 2. Salary histogram

4. Toolkit

The tester should be familiar with some of the tools, given in the list below:

Footprinting

* Greenwhich

* Whois

* Gnetutil (Network Utilities)

* Itrace (ICMP traceroute)

* Tctrace (TCP traceroute)

* Traceroute

* NSTXD (IP over DNS server)

* Nmap (Network scanner)

Scanning

* Cisco global exploiter (Cisco scanner)

* Cisco torch (Cisco oriented scanner)

* ExploitTree search (ExploitTree collection)

* Metasploit (Metasploit commandline)

* Metasploit (Metasploit console GUI)

* Cheops (Network neighborhood)

* GTK-Knocker (Simple GUI portscanner)

* IKE-Scan (IKE scanner)

* Knocker (Simple portscanner)

* Netenum (Pingsweep)

* Netmask (Requests netmask)

* Nmap (Network scanner)

Analyzer

* AIM-SNIFF (AIM sniffer)

* Driftnet (Image sniffer)

* Mailsnarf (Mail sniffer)

* Paros (HTTP interception proxy)

* URLsnarf (URL sniffer)

* smbspy (SMB sniffer)

Spoofing

* Arpspoof (ARP spoofer)

* Macof (ARP spoofer/generator)

* Nemesis-ARP (ARP packet generator)

* Packit (Traffic inject/modify)

* Nemesis-IP (IP packet generator)

* Nemesis-TCP (TCP packet generator)

* Nemesis-UDP (UDP traffic generator)

* SendIP (IP packet generator)

* TCPReplay (Traffic replay

* Etherwake (Generate wake-on-LAN)

Bluetooth

* BTScanner (Bluetooth scanner)

* Bluesnarfer (Bluesnarf attack)

* Ghettotooth (Bluetooth scanner)

* Kandy (Mobile phone tool)

* Obexftp (Obexftp client)

Wireless

* apmode.sh (Act as accesspoint)

* Airpwn (Client penetration)

* Hotspotter (Client penetration)

* GpsDrive

* start-gps-daemon (GPS daemon)

* stop-gps-daemon (GPS daemon)

* ASLeap (LEAP/PPTP cracker)

* Genkeys (Hash generator for ASLeap)

* Airforge

* Cowpatty (WPA PSK bruteforcer)

* changemac.sh (MAC address changer)

Bruteforce

* ADMsnmp (SNMP bruteforce)

* Guess-who (SSH bruteforc)

* Hydra (Multi purpose bruteforce)

* K0ldS (LDAP bruteforce)

Password cracker

* BKHive (SAM recovery)

* Fcrackzip (Zip password cracker)

* John (Multi-purpose password cracker)

* Default password list

Forensics

* Autopsy (Forensic GUI)

* Recover (Ext2 file recovery)

* Testdisk (Partition scanner)

* Wipe (Securely delete files)

Honeypot

* IMAP

* POP3

* Honeyd (Honeypot)

* IISEmulator (Honeypot)

* Tinyhoneypot (Simple honeypot) [6]

5. Conclusion

While the idea behind the penetration testing is to carry out the test and report the results as effective and complete as possible, the personnel chosal is also very crucial for the client of the test. This paper suggested a methodology to chose tester, whether it will be a penetration tester for the company (to be part of the IT team) or a third-party security assessment organization.

Acknowledgements

This work was supported by the Security Engineering Research Center, granted by the Korean Ministry of Knowledge Economy.

References

[1]What the manager needs to know about planning a penetration test or vulnerability assessment By Scott Laliberte, Protiviti Director and Jeff Sanchez, Protiviti Director http://www.knowledgeleader.com/KnowledgeLeader/

[2] http://www.penetration-testing.com/

[3] http://en.wikipedia.org/wiki/Penetration_testing

[4] http://it.toolbox.com/blogs/securitymonkey/get-hired-as-a-penetration-tester-10224

[5] http://www.itjobswatch.co.uk/jobs/uk/penetration%20testing.do

[6] http://it.toolbox.com/blogs/securitymonkey/get-hired-as-a-penetration-tester-10224