Getting To Know Penetration Testing

A. What is Penetration Testing?

Penetration Testing, pen testing, or ethical hacking is the process of assessing an application or infrastructure for vulnerabilities in an attempt to exploit those vulnerabilities, and circumvent or defeat security features of system components through rigorous manual testing. Those vulnerabilities may exist due to misconfiguration, insecure code, poorly designed architecture, or disclosure of sensitive information among other reasons. The output is an actionable report explaining each vulnerability or chain of vulnerabilities used to gain access to a target, with the steps taken to exploit them, alongside details of how to fix them and further recommendations. Each vulnerability discovered is assigned a risk rating which can be used to prioritise actionable remediation tasks.

B. What Are the Benefits of Penetration Testing?

Penetration testing will reveal vulnerabilities that otherwise would not be discovered through other means such a vulnerability scan. The manual, human analysis means that false positives are filtered out. Furthermore, it demonstrates what access can be gained, as well as what data may be obtained through attempting to exploit vulnerabilities discovered in the way that a real world attacker would. This effectively demonstrates the real risk of a successful exploitation given each vulnerability used to gain access.

Penetration Testing will also test an organisations cyber defences. It can deployed to test the effectiveness of web applications firewalls (WAF), intrusion detection systems (IDS), and Intrusion prevention systems (IPS). When a penetration test is underway, these systems should automatically generate alerts and trigger off the organisations internal procedures resulting in a response from internal security operations teams.

Reference:

https://securitycafe.ro/2015/01/05/penetration-testing-benefits/

Penetration Testing enables organisations to meet regulatory compliance requirements such as PCI-DSS, and also addresses ISO 27001 control objective A12.6.

References:

https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
http://www.itgovernance.co.uk/iso27001_pen_testing.aspx

Finally, penetration testing provides an expert opinion from an independent third party outside of the target organization. This can help internal security teams influence management decisions in their favor and obtain more budget for security enhancements.

C. Who Needs Penetration Testing and Why Do They Need It?

Organizations with an online presence, web or mobile application, or connected digital infrastructure should perform penetration testing. A penetration test should be performed on any type of connected, and even non-connected technology after implementation or development, and prior to its go-live phase. This may include a new web or mobile application, network infrastructure, or hardened kiosk client. It is also recommended to perform a penetration test on a periodic basis and also after changes are made as new vulnerabilities are discovered over time and need to be identified and validated as to how they can be exploited or chained with other vulnerabilities to gain access to a target.

Also, organizations that require to meet compliance standards such as PCI-DSS v.3.0 requirement 11.3 where penetration testing is required on an annual basis or after any significant change also need to perform penetration testing.

D. Why Is It Important to Conduct Penetration Testing?

Organizations should conduct penetration testing for the following reasons:

- To ensure the effectiveness of current controls and how they are implemented and configured.
- In order to develop controls to address weaknesses discovered in the infrastructure, application, or process. (Hardware, Software, and People.)
- To examine the effects of multiple vulnerabilities and how they can be chained together.
- To assess the effectiveness of an application's input validation controls. Where ever user input is entered, rigorous fuzz testing is performed to make sure that it only sanitized input is accepted.
- To improve security response time. A penetration test can be used to identify how different teams respond to an intrusion and improve internal incident response processes and procedures.

E. What is the Difference Between Penetration Testing & Vulnerability Assessment?

Penetration Testing and Vulnerability Assessments should both be part of an organization's security program.

Vulnerability Assessments should be performed frequently across infrastructure and applications. A vulnerability assessment checks for known vulnerabilities and security misconfigurations for which a plugin has been developed in order to perform a specific check it is written to detect. Dedicated software tools such as Nessus and Qualys are used. It does not focus on exploiting vulnerabilities, the results of chaining multiple vulnerabilities together, or have the ability to use information gathered intelligently in order to innovate a customized an attack. The scope of a vulnerability assessment will normally be much larger and include a complete list of known vulnerabilities risked ranked with a CVSS score across an entire range of targets. Also, as a vulnerability assessment does not validate results there is always room for false positives.

Penetration Testing is goal focused. It often targets a specific application or system component within an agreed scope rather than everything as a whole. Unlike a vulnerability assessment, when performing a penetration test the vulnerabilities are discovered through thorough manual probing using a customized toolset that would otherwise not be uncovered in a vulnerability assessment. Often customized scripts are written within the duration of the test in order to uncover security weaknesses. Furthermore, penetration testing requires that the penetration tester actively exploits the vulnerabilities discovered. Often multiple vulnerabilities are exploited in order to successfully gain access. It requires an intelligent and creative way of thinking such that the tester is able to creatively chain vulnerabilities together from exploiting multiple vulnerabilities at the same time, and in symphony, in order to gain access to a target.

F. What Are The Types of Penetration Tests?

Following is a summary of each type of penetration test which all follow different methodologies and utilize different frameworks.

Web Application Penetration Test. These tests focus on the various vulnerabilities found in web application components; including frameworks, server software, API's, forms, and anywhere where user input is accepted.

Mobile Application Penetration Test. A mobile penetration test focuses on trying to exploit how a mobile application accepts user input, how securely it is stored on the phone, how securely data is transmitted across the internet, as well as all the web service vulnerabilities which may be present in the API.

External Infrastructure Test. Checks for ports open on all externally facing ranges, attempts are made to fingerprint and exploit services discovered as well as bypass authentication mechanisms and brute force VPN gateways.

Internal Infrastructure Penetration Test. This will be an attempt to get full system administrator privileges from within the internal network. Checks are done to search for vulnerable services and software, and exploits are used to obtain access. Network traffic is normally sniffed whilst ARP poisoning is executed in order to capture credentials and other sensitive traffic in transit.

Wireless Penetration Testing. At a high level, this involves attempts to crack WEP and WPA encryption in order to obtain access. Other attacks such as Man in the middle (MitM) attacks are attempted, as well as tricking wireless clients into connecting to a dummy access point.

End point / Kiosk PC Penetration Test. These penetration tests attempt to break out of a kiosk PC or other locked down device and gain elevated privileges or access to sensitive data that should otherwise not be accessible.

Penetration Testing Prerequisites

A. Penetration Testing Checklist

Understand Business Requirement. This is the most important part of the engagement. You must have a clear understanding of why the customer requires the penetration test? Is it good practice driven? Part of a new launch? Or compliance driven? The answers to these types of questions will be the dictate how the rest of the engagement is approached.

Define Scope. Define what is in scope and what is specifically out of scope. There also needs to be a clear definition of what is allowed and what isn't allowed in the rules of engagement.

Review Past Threats and Vulnerabilities. Although It is generally good practice to perform a review on what was previously discovered in a penetration test, it is also mandatory as part of PCI requirement 11.3. This review allows you to specifically focus on things that were identified previously and make sure those same issues have either been remediated or not arisen again.

Get Authorization. The actions performed during a penetration test would normally be considered illegal without prior authorization. This can land you in some legal hot water unless you have your "Get Out of Jail Free" paperwork signed off. A good template to use as an example is here: http://www.counterhack.net/permission_memo.html

Penetration Testing Prerequisites

Agree on Timing. There may be certain times in an organisation where the risk of interference or downtime is considered a higher consequence; such as periods of high utilization or when project implementations and upgrades are taking place. Because of this, make sure you agree on an acceptable time window to perform the penetration test.

Whitelist Source IPs. The target organisation of a penetration test should be notified of the source IPs from where you will be performing the test from. There are a number of reasons for this, but in order to properly perform a penetration test without interference from a WAF or an IPS, you should request that your source IPs are whitelisted on such appliances.

Confirm internal contacts available. It's important that you agree on a communication plan and on who your internal contacts will be within the organisation to be available during the penetration test. This is not only so you can get them to support you during the testing process, but it's also a good idea to notify the target organisation immediately if a vulnerability is discovered that you deem to be 'Critical".

Reference:

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

B. Penetration Testing Tools

There are a large suite of penetration testing tools which you may utilize within your arsenal depending on what you are testing. This topic is too big to detail every tool for every type of test. Most of these tools ship with Kali Linux which is considered the penetration tester's Linux distribution. However, the following are are tools you should get to know well:

Penetration Testing Prerequisites

Nmap was traditionally developed as a host discovery and port scanner in order to “map” out the a network. But can now also be used for host fingerprinting, service detection, and vulnerability scanning -- effectively enumerating all services running on any given host(s) including vulnerabilities detected on them.
https://nmap.org/

Netcat. Often referred to as the swiss army knife of the network, Netcat can be used for terminal connectivity, chat sessions, file transfers, port redirection, and as well as for launching forward and reverse shells on connect. An excellent cheat sheet by SANS is here: https://www.sans.org/security-resources/sec560/netcat_-cheat_sheet_v1.pdf

Burp Suite. Burp is a web application intercepting proxy which is capable of spidering and downloading a website, modifying web requests on the fly, fuzzing user input fields and values, analysing session token ID randomness, as well as automatically scanning HTTP requests for vulnerabilities. It is used mainly in web and mobile application penetration tests where web requests are sent to a server.
https://portswigger.net/burp/

Penetration Testing Prerequisites

SQLMap is a full blown automatic database takeover tool. It can be used to identify SQL injection vulnerabilities, and then exploit them in order to download entire databases, launch commands remotely, and spawn a remote OS shell.
http://sqlmap.org/

Nessus is a vulnerability scanner. A vulnerability scanner is often used as part of a penetration test in order to detect missing patches and discover "low hanging fruit." A vulnerability scan will quickly find scan detectable vulnerabilities which can be used as a basis to launch an exploit against in order to gain quick access.
https://www.tenable.com/products/nessus-vulnerability-scanner

Metasploit Framework is an exploit framework used to set up and launch exploits at vulnerable hosts. It can also be used for enumeration tasks as well as a listener for incoming reverse shells and meterpreter shells.
https://www.metasploit.com/

Penetration Testing Prerequisites

Python. It is recommended that you master at least one high level scripting language. If you were only going to learn one language, Python would be it. It is easy to write and well adopted within penetration testing and exploit development circles. https://www.python.org/

Bash. Learning the bash shell and how to script with associated linux command line tools during a penetration test is essential. You should be able to quickly put together custom scripts to filter and format data for presentation or input into another tool.

Google is where you will find open source information that will prove interesting during a penetration test, such as the discovery of potentially sensitive documents that shouldn't be publicly searchable. Johnny Long wrote an excellent book on this topic. There is also a Google Hacking Database (GHDB): https://www.exploit-db.com/google-hacking-database/

Executing Penetration Testing

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

A. Penetration Testing Strategy

It's important to allocated time wisely and not get tunnel visioned attempting to break into one part of a target system. Due to the time constraints of a penetration testing engagement, getting stuck on a red herring will mean that you will miss the opportunity to find other critical flaws that you could have exploited in order to gain access. It's also worth noting that the reporting component will also take a considerable amount of time. For this reason, making sure you have a properly documented process is important. When planning for a penetration test it is worth allocating a fixed amount of time per component or function as well as reporting.

B. Penetration Testing Methodology

It is important to follow an industry methodology as a baseline. You can then build your own processes and procedures for testing on top of that.

OWASP testing guide - Contains a best practice framework and set of tests to perform when conducting a web application penetration test.
https://www.owasp.org/images/1/19/OTGv4.pdf

PCI Penetration testing guide - Provides guidance for conducting penetration tests under PCI requirement 11.3.
https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf

Penetration Testing Execution Standard - A standard put together by a bunch of InfoSec professionals with the goal of developing a common framework for penetration tests.
http://www.pentest-standard.org/

NIST 800-115 - A high level technical guide for conducting information security tests and security assessments.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Penetration Testing Framework - Is a free penetration testing framework and walkthrough covering various phases of penetration testing in detail.
http://www.pen-tests.com/penetration-testing-framework.html

Information Systems Security Assessment Framework (ISSAF) - An excellent reference for penetration testing which covers everything from project management to testing.
https://sourceforge.net/projects/isstf/

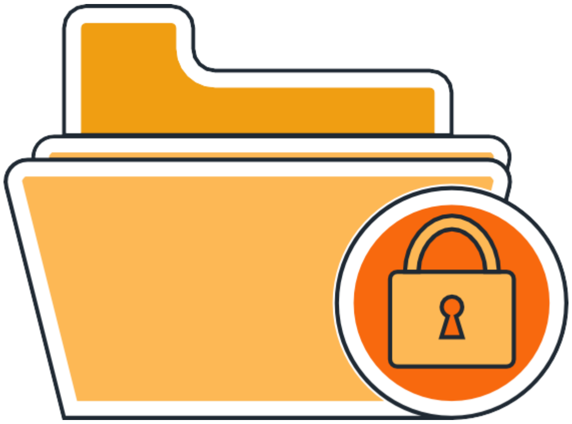
Open Source Security Testing Methodology Manual (“OSSTMM”) - A penetration testing methodology security testing, security analysis, and security metrics, among other things.

C. Penetration Testing Do’s and Dont’s

- ✓ Make sure you do everything as discussed and set out within the agreed scope.
- ✓ Make sure you do get authorization signed off to perform the penetration test.
- ✓ Do not ever perform a penetration test without prior approval.
- ✓ Do not perform testing outside of the agreed scope of the test.

D. How to Organise the Data Collected in Penetration Tests

Detailed notes are important, including lots of screenshots as evidence. For everything you compromise, you will need to explain in detail with screenshots so there will be a lot of cut and paste. Examples of code snippets used should also be included as well as commands entered. You can use a program such as word, or cherrytree for this: http://www.giuspen.com/cherrytree/



The notes and data collected in the course of the penetration testing engagement will be need to be thorough enough so that the attacks can be explained in detail in the final report so that the customer can use to reproduce the attacks themselves.

Post Penetration Testing Questions

A. Interpreting Results of Penetration Testing

Reports should contain risk ranked vulnerabilities with the highest risk rated items at the top of the report. Customers should priorities remediation tasks starting with the highest risks. Risk owners should be identified and assigned items from the report in and given a deadline to remediate based on the risk rating. For example, Critical - 1 week, High - 1 month, Medium - 2 months, Low - 3 months.

B. How to Validate Results of Penetration Testing?

This should have already been done by the penetration tester. The final report should contain details and steps with screenshots showing exactly how certain vulnerabilities were exploited. Thus there should be no false positives in the report.

C. How Often Should Penetration Testing Be Done?

Penetration should be done as part of any secure software development lifecycle, alongside a source code review and secure development standards. It should be performed prior to going live, as well as after going live. Following that, it should be performed periodically on any digital system.

PCI requirement 11.3 requires that penetration testing is performed at least annually and after any significant change.

Post Penetration Testing Questions

D. When should a Re-Test be Done?

At least one re-test should be offered by the penetration tester as part of an engagement. The client should request that a re-test is performed as soon as they have completed remediation tasks. The re-test will test for the vulnerabilities discovered in the initial test in order to validate whether they have been successfully remediated.

Qualifications of Penetration Testers and the Cost of the Service

A. What Certifications Do Penetration Testers Need to Have?

There is currently no requirement for a penetration tester to hold any certifications, however it is recommended that a professional penetration tester holds at least one of the following;

Offensive Security Certified Professional (OSCP) - This would be considered the de facto standard for an entry level penetration tester and recommended as a bare minimum level of skill.

Offensive Security Certified Expert (OSCE) - This validates the skillset of a more advanced penetration tester.

CREST Registered Penetration Tester (CRT-Pen) - We don't believe this one holds too much weight from a technical point of view in comparison to the others but is gaining popularity as a compliance like certification.

The PCI Security Standards Council also lists these certifications as indications of skill level and competence. https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

B. Why Penetration Testing Should be Done by Experts

Penetration testing is a niche skill which takes a lot of hands-on experience to develop. Not only does it require an exceptional attention to detail, but an excellent ability to write high quality technical reports as the report is the deliverable of the engagement.

Qualifications of Penetration Testers and the Cost of the Service

C. How Much Does Penetration Testing Cost?

This varies depending on the type of engagement, scope, and size of what needs to be tested. As such it is best to get quoted accurately. Factors such as complexity of the environment, methodology, experience, and qualifications of the penetration tester, whether the test is performed onsite, and what re-test work is required are all things which will affect cost.