An Evaluation of Penetration Testing Methodologies

White Paper

Abertay University

Jack Wilson
1501838
BSc (Hons) Ethical Hacking
25th January 2018
Word Count: 3202

Contents

1 Introduction

With an ever increasing amount (Symantec, 2017) of data breaches and ransomware attacks (due to the WannaCry and Petya ransomware campaigns), the demand for jobs in information security has risen. With this continually expanding sector, penetration testing has increased in popularity.

Penetration testing is a process that involves testing computers, servers, networking equipment and web applications to find and exploit vulnerabilities, with the aim of improving the security of the computer/network/web application based on the findings of the testing.

No network or computer is guaranteed to be 100% hack-proof, and no penetration test will be able to guarantee this. The objective is not to guarantee 100% security, but rather to highlight as many underlying issues with a network as possible. For this reason, various standardised penetration testing methodologies have been developed. The concept behind following a methodology stems from a few ideas:

Standardisation

Using a standardised approach ensures consistency and thoroughness when conducting a penetration test.

Meaningfuless

Many people at different levels of a business will be involved in a penetration test, from system administrators to middle managers and executives. All of these people will likely read the report produced at the end of the testing. For this reason it is important to break down the report into different sections for the various people reading it.

For example; an executive may not have the technical details of a report, but they may want to know how an issue would impact the business, and a systems administrator is more likely to understand the technicalities, but may not be as interested in the business impact of a vulnerability but rather the technical details to be able to reproduce the issue and the details on how to mitigate the vulnerability.

Methodologies will usually discuss pre-engagement, engagement and post-engagement. Generally the engagement phase of methodologies follow a structure in line with the military kill chain that involves:

- Reconnaissance (Research and identification of target(s)).
- Weaponisation (Creating a payload to allow remote access).
- Delivery (Getting the payload to a target (e.g. by phishing email or malicious website).
- Exploitation (Triggering the malicious code inside the target network).
- Persistence (Backdooring the network to maintain persistent access).
- Action on Objective (Proceeding with remainder of attack (e.g. malware infection or data exfiltration).

Commonly found methodologies in the industry include:

- ISSAF
- OWASP
- OTG
- PTES
- OSSTMM
- BSIMM

The aforementioned methodologies will often loosely follow the kill chain process, but there are some variations between each methodology. This paper will investigate the main differences between the Information Systems Security Assessment Framework (ISSAF) and the Penetration Testing Execution Standard (PTES) and evaluate each methodology relating to the planning, management, execution and reporting of a penetration test. The paper will also discuss the legal and ethical aspects mentioned in each methodology to make a well considered, critical evaluation of both methodologies based.

2 ISSAF

2.1 Background

The Information Systems Security Assessment Framework (ISSAF) was originally drafted by the Open Information Systems Security Group and it is a peer-reviewed framework that is designed to break down a penetration test into the various stages and detail each stage in depth to highlight as many potential vulnerabilities and weaknesses within an enterprise as possible.

As per the ISSAF framework, the five main stages of a penetration test are: planning, assessment, treatment, accreditation and maintenance. These stages are detailed in the *analysis* section, below.

2.2 Analysis

2.2.1 Phase 1: Planning

This stage of the methodology involves identifying assets, resources and the IT infrastructure within the organisation that could be targeted during the penetration test. Furthermore, a feasibility study is undertaken to ensure that it is economically viable for the business to pay for a penetration test.

Within the planning stage the management of the penetration test is also discussed and agreed upon. Although the general method of management will be the same, the specific details will vary on a per-client basis. The planning will involve agreeing on the objectives and expected outcomes of a penetration test, agreeing what IT infrastructure is in scope and out of scope and setting milestones within the project (e.g. when testing and reporting must be completed by).

Additionally, key contacts must be established within the organisation for the recommended weekly progress updates on the project as well as in the case of any immediate issues that could arise during the penetration test.

2.2.2 Phase 2: Assessment

The second, and main, section of a penetration test under the ISSAF methodology is the assessment itself. This is broken down into two main categories: Inherent Risk Identification and Controls Assessment.

Stage 1: Risk Identification
The risk identification stage involves discovering company assets and processes that could be targeted within the penetration test. The next part of this stage involves threat and vulnerability identification of the discovered assets/IT infrastructure. All of the results of this stage are subsequently recorded.

Following this, a threat assessment is undertaken to provide the client with an overview of the potential impacts each discovered vulnerability could have on the company, as well as an estimation or measure of the likelihood of the threat.

Stage 2: Controls Assessment
The second stage of the assessment is the controls assessment. This part of the methodology involves looking at the processes a company may have in place to partially or fully mitigate potential security issues and reevaluating the previous risks discovered with the controls taken into consideration. The controls assessment can be further broken down:

Evaluation of Legal and Regulatory Compliance
This part of the assessment reviews the legal and regulatory requirements relating to the IT systems of a business, to ensure the business under assessment is fully compliant with all necessary requirements.

One noteworthy regulation that every business in the UK will have to adhere to is GDPR (the General Data Protection Regulation) which comes into effect on the 25th of May 2018 (Information Commissioner's Office, no date). There are many areas of how a business handles data that fall under GDPR, but the main one that relates to a penetration test would be a data breach.

Companies face heavy fines if they are involved in a data breach, not to mention the reputational damage. Having a penetration test conducted could significantly reduce the risk of a data breach by highlighting any vulnerabilities that could lead to a breach.

Evaluation of Enterprise Information Security Policy
An information security policy within an organisation will be indicative to their stance on information security and should give the penetration testing consultant an in-depth insight into this.

Evaluation of Enterprise Information Security Organisation and Management
The function of this stage of the assessment is to analyse the staff members at an operational level up to a management level to gain an insight into the roles and responsibilities of each staff member. This will allow the assessor(s) to gain a better understanding roles/areas of the organisation that may be understaffed or lacking, which could result in security issues.

Assessment of Enterprise Information Systems Security and Controls
This section of the penetration test involves actively targeting IT infrastructure and the physical security with the intentions of compromising the network/business. The assessment covers the following areas:

- Physical & environmental security (e.g. door, building security and placement of CCTV cameras).
- Technical Controls:
  - Network security (networking equipment and servers).
  - Host security (desktops, laptops, etc. on the network).
  - Application security (an evaluation of any software applications running on the network).
  - Database security.
- Evaluation of Security Awareness through methods such as:
  - Interviews.
  - Observation.
  - Structured walkthrough.
  - Social engineering (both using a physical presence pretending to be someone else, or through digital methods such as phishing attacks).

The technical controls evaluation will typically follow the military kill chain process mentioned earlier, involving reconnaissance (gathering information about the IT infrastructure and conducting a vulnerability assessment), followed by weaponisation and delivery based on the gathered vulnerabilities (selecting an exploit and getting the exploit to the target device). This is followed by the exploitation phase (where the previously created exploit is ran on the target network).

The installation, command & control and action on objectives phases of the kill chain will depend on the scope of the penetration test, but a penetration tester may try to create a backdoor for persistence, exfiltrate documents from the network or escalate privileges to a higher level (e.g. local administrator or domain administrator).

Evaluation of Enterprise Security Operations Management
This evaluation is often ran alongside the assessment of enterprise information systems security and controls that gives the penetration tester an insight into the operational capabilities of the IT team. This covers the whole spectrum of IT including:

- Capacity management.
- Vulnerability management.
- Release management which includes:
  - Patch management.
  - Configuration management.
  - Change management.
- Enterprise incident management which includes:
  - Event logging & monitoring.
  - Security incident management.
  - Operation event management.
- User management (e.g. disabling accounts for employees who leave).
- Certifications & accreditation.

Evaluation of Enterprise Business Continuity Management
A business continuity evaluation ensures that the business is prepared for any incidents that could affect the day-to-day operations of the business. Having a solid business continuity plan will help the business run its day-to-day business at a basic level until disaster recovery measures can be implemented (in an event such as malware spreading cross the network or a hardware failure in a server).

Manage Residual Risks
Residual risks are risks that are not covered by the security and controls procedures that were previously discussed and assessed. These risks will vary business-to-business, but they should be reviewed frequently to ensure the risks have not became more critical.

2.2.3 Phase 3: Treatment

The treatment section refers specifically to residual risks. The residual risks should be reviewed with safeguards and plans put into place with proper documentation. This allows executive management to make a decision on how to manage the risk(s).

2.2.4 Phase 4: Accreditation

Once the above is completed, approved auditors from OISSG would (optionally) complete a test of the business following the ISSAF methodology to ensure all necessary criteria are met, then a report would be provided detailing where any criteria to meet the ISSAF framework was missing. If the business was found to be compliant with the ISSAF framework after an assessment, a certification of compliance would be issued to the business.

2.2.5 Phase 5: Maintenance

As part of being ISSAF certified, a business must demonstrate they are continually compliant with the framework, which involves continuous, regular reassessment. The frequency of reassessment varies dependant on the size of the company and the scope of the compliance.

Outside of the practical aspects of the assessment, there are dozens of considerations relating to best practices, legal and ethical considerations to be undertaken. This includes ensuring that non-disclosure agreements are signed, that only items within the scope are tested and that there is liability in case of an incident during the penetration test.

2.3 Summary

The ISSAF methodology is a good framework/methodology for conducting a penetration test, however it is far from complete. The methodology is incredibly in-depth, with the current draft being over 1200 pages in length details each stage of the methodology. It also includes templates for a lot of the forms/paperwork that may be required during a penetration test.

The largest downside to this methodology is that it is incomplete. At the time of writing the latest version was draft 0.2.1. The majority of the content is still present, but some areas of the methodology (such as sections of penetration testing a Windows host) are missing or there is placeholder text present.

3 PTES

3.1 Background

The Penetration Testing Execution Standard (PTES) is a methodology that was developed to cover the key parts of a penetration test. From the initial contact phase, working through the stages of the cyber kill chain (e.g. vulnerability analysis, exploitation and post-exploitation) and finishing with the reporting phase.

The PTES standard itself does not specify exactly how to conduct a penetration test, but rather the steps that should (typically) be followed. Technical guidelines were developed to accompany the PTES, however it is noted at the beginning of the technical guidelines (correctly so) that the guidelines should not be followed exactly, they are an approximation of the steps that should be followed, and an actual penetration test will vary on a client-to-client basis.

3.2 Analysis

As mentioned above, the PTES methodology has several main sections. These are detailed below:

3.2.1 Section 1: Pre-engagement Interactions

The pre-engagement interactions detail everything that should be covered & discussed before a penetration test begins. This includes agreeing on a scope (what should and should not be targeted), an agreement of the timescale, an agreement on the payment details of a penetration test, defining rules of engagement and the expected outcomes of the testing.

This section also briefly touches on legal considerations when conducting the penetration test. One example that is provided is if a penetration tester was to compromise a VOIP system and listen to/record phone calls. Some countries would consider this wiretapping and it could potentially be illegal regardless of if permission is given from the subject of the penetration test.

3.2.2 Section 2: Intelligence Gathering

Open-Source Intelligence (OSINT) involves using information that is in the public realm and easily available (both digitally and physically) to gather information about a company and its employees that could be used to contribute to the success of a penetration test.

One excellent example of this is finding photographs of employees on social media where work ID badges are visible in photos. This would allow a penetration tester to easily replicate an ID badge which would aid in believability when executing a physical penetration test.

The PTES methodology breaks information gathering down into multiple levels, dependant on the client/company being tested. For example, a medium-large sized enterprise would require less OSINT gathering than a government where a nation state may use advanced techniques to gather information.

Level 1 information gathering may involve running automated tools to gather information, where a level 3 information gathering task may involve heavy manual analysis of a company/government and its subcontractors/subsidiaries.

3.2.3 Section 3: Threat Modelling

Threat modelling involves using information gathered from OSINT combined with a list of company assets to determine a list of potential threats to the business and the level of impact each threat poses. There are several common threats that could impact a business:

- Intentional Threats

  - Targeted: A group or individual specifically targeting an organisation or its infrastructure for a variety of reasons including (but not limited to) stealing company secrets, stealing/leaking customer data, installing ransomware for extortion purposes. This could come from a disgruntled ex-employee, a rival company or a nation state actor.
  - Non-Targeted: This threat occurs when a worm/virus is on the internet targeting any computer device, regardless of the organisation it affects. One such example would be the `WannaCry` virus (National Audit Office, 2017), which targeted any vulnerable computer on the internet and infected the computer with ransomware.

- Unintentional Threats
  - Unintentional threats often come from within the organisation itself in the form of untrained employees (e.g. trying to install software and inadvertently installing a virus) or a hardware failure with a business-critical server that could lead to downtime/data loss due to poor redundancy measures.
  - Additionally, an excessive social media presence by company employees (especially due to poor privacy configurations) can increase the effectiveness of a targeted spear-phishing attack by an adversary.

3.2.4 Section 4: Vulnerability Analysis

This section is the first stage where a penetration tester will begin to actively target computers and servers on the client's network. The objective of this phase of the penetration test is to discover potential vulnerabilities on the network through the use of automated tools & scripts and through manual analysis.

The types of tools used will vary dependant on the scope of the assessment but will generally involve vulnerability scanning tools such as Nessus or OpenVAS as well as manual tools such as Nmap and Nikto to gain additional information into the network and potential vulnerabilities to exploit.

3.2.5 Section 5: Exploitation

Once the penetration tester has completed the vulnerability analysis, the next stage is to attempt to exploit the vulnerabilities. The method of exploitation will vary dependant on the severity of vulnerabilities discovered, but will generally involve a penetration tester bypassing access restrictions to gain access to systems on the network.

During the pre-engagement interactions a scope for the assessment would have been established. With the penetration tester now having access to the network, the scope can be acted upon (for example: exfiltrating data from the network). During the exploitation phase the penetration tester should consider stealth and attempt to avoid any intrusion detection systems/antivirus software detecting an attack.

3.2.6 Section 6: Post-Exploitation

If a penetration tester successfully gains access to one device on the network this gives the tester a foothold and the opportunity to pivot across the network to target higher value assets. During the post-exploitation phase the attacker can use this foothold to create persistent network access, compromise more devices on the network or escalate privileges to either local administrator or domain administrator.

Whatever actions a penetration tester takes during the post-exploitation phase should have been agreed upon in the pre-engagement meetings, and should not cause any intentional risk to the operational needs of the client's IT infrastructure (such as a denial of service attack or data loss).

3.2.7 Section 7: Reporting

The most crucial part of any penetration test is the report. A good penetration tester will go unnoticed in a network, so a report may be the only thing a client sees that proves work was actually completed. The report should portray the results of the penetration test in a variety of ways; both to a technical and non-technical (e.g. management/board member) level. The report should contain:

- A concise, executive summary of the findings and the suggested remediations.
- A reiteration of the pre-engagement details established before the testing.
- An in-depth, technical explanation of all results from Sections 2-6 where each vulnerability discovered has the following details:
  - A background to the issue.
  - Details on the impact the vulnerability could have to the business.
  - A list of affected systems/websites/databases etc.
  - A proof-of-concept exploit (with full steps on reproducing the issue.
  - A detailed explanation of the suggested remediation(s) to the issue.
- A conclusion/summary to the report that reiterates key details of the report.

3.3 Summary

The Penetration Testing Execution Standard is an excellent framework that is expansive and detailed. The latest version (1.1, at the time of writing) details a well thought out methodology for the pre-engagement, engagement and post-engagement phases of a penetration test.

As well as the 200+ page document detailing the methodology, the Pentest Standard website has a wide range of technical guidelines for tests that may be conducted during a penetration test. (Pentest Standard, 2012). The technical guidelines are also community-driven, so any member of the information security community can share their knowledge in the technical guidelines.

4 Conclusion

The general structure of both methodologies is similar (e.g. pre-engagement, engagement and post-engagement) that details the general steps that should be taken (e.g. scoping, NDA's, physical and computer security testing and reporting), but there is some variance between the methodologies.

Overall, I believe that the Penetration Testing Execution Standard is a better framework to use. The ISSAF framework has more content in the documentation and a large focus on the risk assessment and identification (before even touching a computer for the penetration test), but the PTES framework is more complete (being out of draft) and has the large, community-driven technical guidelines available to anyone.

Another alternative option (that is fairly common within the industry) is to use an in-house developed methodology. Using this method still ensures the consistency of adopting a methodology, but having a custom-created methodology could ensure the best parts are taken from both the ISSAF and PTES methodologies.

5 References

Pentest Standard (2012) PTES Technical Guidelines. Available at http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (Accessed 19th February 2018).

Symantec (2017) Internet Security Threat Report. Available at https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (Accessed 19th February 2018).

The PTES Team (2017) The Penetration Testing Execution Standard Documentation. Available at https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf (Accessed 19th February 2018).

Open Information Systems Security Group (2006) Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1. Available at http://www.oissg.org/files/issaf0.2.1.pdf (Accessed 19th February 2018).

Information Commissioner's Office (no date) Guide to the General Data Protection Regulation (GDPR). Available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulat (Accessed 19th February 2018).

National Audit Office (2017) Investigation: WannaCry cyber attack and the NHS. Available at https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (Accessed 19th February 2018).