Penetration Testing

vs.

Red-Teaming

A Netscylla whitepaper on the differences between penetration testing and red-team engagements.

Version 2.0

Netscylla Cyber Security Ltd
GB 10571639

Address:
Telecom House,
125-135 Preston Road, Brighton,
East Sussex,
United Kingdom, BN1 6AF

Contents

Introduction

At Netscylla we often get asked about the differences about penetration testing and red-teaming.

- Which assessment is most appropriate for my project or organisation?
- Do I really need a red-team assessment?
- What are the advantages and disadvantages of each?

There are many conflicting sources and advice, depending on where you look and who you ask. This whitepaper outlines our belief of good practise for the management of penetration and red-team engagements.

Threat Development

During the past five years, a specific threat category has become much more widely discussed. Advanced Persistent Threat (APT) was originally used to refer to nation-state sponsored attempts to infiltrate military, defence industrial base, and government networks with the specific goal of exfiltrating sensitive data. Today, the term APT is used widely in media and security circles to describe any attack that seems to specifically target an individual organisation, or is thought to be notably technical in nature regardless of whether the attack was actually advanced or persistent.

Common characteristics of an APT include:

- Sophisticated planning
- Specific/sequential targeting
- Effective reconnaissance
- Practiced tool usage
- Social engineering

Modern adversaries have substantial resources and orchestration at their disposal. Regardless of the individual adversary's sophistication, the security incident trends of late 2009 until today are a clear indication that the increased probability of an event and risks are on the rise. The increased sophistication and targeted nature of security threats, coupled with their increasing frequency suggests that—sooner or later— security breaches will affect all users and organizations.

In the current threat landscape, a prevention-only focus is not enough to address determined and persistent adversaries. Additionally, with common security tools, such as antivirus and Intrusion Detection Systems (IDS), it is difficult to capture or mitigate the full breadth of today's breaches. Network edge controls may keep amateurs out, but talented and motivated attackers will always find the means to get inside these security boundaries or gate-keepers. As a result, organisations are all too often ill prepared when faced with the need to respond to the depth and breadth of a breach.

With the evolution of IT and adoption of the cloud, no longer can the boundaries of the enterprise be defined by a network perimeter managed physically or virtually through firewalls. Corporate data, including sensitive data and applications, can be found nearly everywhere: on-premises, in private data-centres, in the cloud, with partners and on a variety of user devices. All of which require different security strategies as well as a shift in the security methodologies utilised by most organisations.

Breach response has always presented many challenges including identifying the scope of breach, timely notification to stakeholders and customers, investigating data loss and recovering compromised assets. Through a combination of today's adversaries and the evolution of IT, breach response has never been more challenging than now. Therefore, rather than the traditional focus on just preventing breaches, an effective security strategy assumes that determined and persistent adversaries will successfully breach any defences.

What is Penetration Testing

Penetration testing has become the means for gaining assurance in the security of an IT system by attempting to breach parts or the whole systems security, using the same tools and techniques as an adversary.

The goal of a penetration test report is to identity technical risks that may impose a threat against a specific part of applications or infrastructure critical to the business.

A well-scoped test can give confidence in products and security controls have been configured appropriately in accordance with good practise and the businesses security policies. Penetration testing is best targeted against individual and specific business components, applications and infrastructure.

Penetration testing usually comes in two flavours:

- White-box testing – where full information about the target is shared with the testers. Additionally, accounts are created with different permissions (including RBAC), to effectively assess the internal vulnerabilities and controls of a given system for known software vulnerabilities and server/software misconfigurations. Privileged accounts, enable the team to potentially debug difficult and challenging vulnerabilities, to aid in vulnerability remediation.
- Black-box testing – where little or partial information is shared with the testers. This type of testing mimics what an external attacker can view, and potentially gain access. This type of testing is more challenging and often split into two kinds of assessment depending on the experience of the testers:
  - Automated scans and vulnerability assessment, where the testers use open-source and commercial tools to scan your targets, and produce a report quickly and at relatively low cost.
  - Advanced targeted attacks, where the more experienced testers, may try to reverse and subject the target to attacks that address specific security concerns. This type of testing is usually bespoke and incurs grater cost when compared to other tests.

What is Red-Teaming

Red-Teaming has recently been viewed as a more advanced form of penetration testing, as penetration testing has devolved into compliance and vulnerability assessments. However, those that have been in the industry for two decades appreciate that red-teaming is very similar to how penetration testing used to be performed, when the cyber security sector was immature and still developing.

The goal of a red-team report is to improve and remedy the businesses internal vulnerabilities and management processes against part of, or the whole business.

Red-Teaming differs from penetration testing in that it is scenario driven. Some may argue that the scenarios must be thriven from collected and processed threat intelligence (such as the CBEST regulated red-team assessments). But in Netscylla's experience good scenario building pays for a good assessment, especially when the threat intelligence can be weak, or not applicable to the customer's specific operating sectors or business. A creative and technically knowledgeable team that is up-to-date on modern attacker's techniques can still adequately build a good red-team assessment without threat intelligence.

- Scenario driven testing aimed at identifying vulnerabilities – The team explores a particular scenario to discover whether it leads to a vulnerability in the businesses defences. Scenarios may include: lost laptops, unauthorised devices connected to the internal network, compromised DMZ hosts, and many others are possible.
- Scenario driven testing for detection and response – This version is driven to assess a business's capability of detecting and managing external threats. Scenarios include, phishing, social engineering, physical attacks, website compromise assessments, evading protection software, lateral movement across networks and many other attacks depending on the complexity of your systems.

Threat Intelligence driven scenarios.

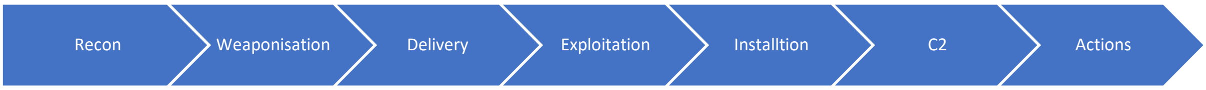
A modern twist to some of the red-team plays, is that they are threat intelligence driven; what is the difference between threat intelligence and open-source intelligence (OSINT)? Threat intelligence amalgamates several intelligence sources such as: open-source (OSINT), human (HUINT), technical (TECHINT) and financial (FINIT).

Data from these sources is then combined and mapped against known threat actors in the industry. The goal is to map between 4-6 different actors (e.g. hacking groups) and their techniques using the groups known patterns from previous incident response and forensically analysing incidents. Some threat actors might then be eliminated due to their differences in targeting sectors, political or financial motivations.

The output of the threat intelligence should be a report providing 3-4 threat actors with their TPP's (Technology, People, & Processes). That outline the possible scenarios for red-teaming.

The ‘Lockheed Martin’ Kill Chain

The Red Team is often a group of full-time staff that focuses on breaching a client’s infrastructure, platform and their own tenants and applications. They are the dedicated adversary (a group of ethical hackers) performing targeted and persistent attacks against Online Services (Customer’s infrastructure, platforms and applications but not end-customers’ applications and data). The role of a Red Team is to attack and penetrate environments using the same steps as an adversary’s kill chain as shown in figure below:



Therefore, researching and understanding industry incidents and threat landscape trends in order to stay on top of the latest attack techniques and tools used by adversaries is a critical part of any Red Team’s approach. The Red Team uses this research and intelligence to not only model but also execute real-world tactics associated with an adversary kill chain.

In addition to research and modelling known adversaries, the Red Team develops and derives their own novel techniques for compromising customer networks using custom-developed penetration tools and attack methods. Just like determined adversaries, the Red Team utilises emerging and blended threats in order to perform compromises and will change tactics when presented with new roadblocks or defences. Since talented and motivated attackers breach perimeter defences, so must the Red Team. Edge controls may keep amateurs out, but persistent adversaries always get inside. Once inside, it is common for the Red Team to acquire insider privileges which they use to pivot laterally to penetrate the infrastructure even deeper. Additionally, like most skilled adversaries, the Red Team establishes a foothold from which to maintain persistence and may continuously modify their approach to evade detection. For example, the Red Team may install custom tools (bots, remote control, etc.) allowing them continual access to a compromised resource and retrieval of information whenever they please. The mechanics of such an attack allow the Red Team to not just exfiltrate sensitive data, but leverage that compromised data.

Due to the sensitive and critical nature of the work, the employees who work on Red Teams at are held to very high standards of security and compliance. They go through extra validation, background screening, and training before they are allowed to engage in any attack scenarios. Although no end customer data is deliberately targeted by the Red Team, they may establish and obtain similar levels of access? These individuals need to be appropriately vetted, and have up-to-date knowledge on privacy laws. In addition, the Red Teams can only attack customer managed infrastructure and platforms; Third parties cannot be included due to contract law.

Summary

Below is a brief summary of the differences of penetration and red-team assessments:

	Penetration Testing	**Red-Teaming**
Scope of engagement	1-2 specific systems	Specific part of (or the entire) organisation
Type of engagement	White/Black box	Scenario driven
Average length of engagement	1-4 weeks	2-3+ months
Cost	£ - ££	£££ - ££££
Permitted Credentials	White box - Yes Black box - No	Initially - No, but credentials may be supplied if testing slows to a state of non-productivity, for the assessment to progress
Reporting timeliness	1 week	1 month
Type of report	Technical against software vulnerabilities	Tactical and strategical management report against business processes, and additional technical report for specific software vulnerabilities identified during the engagement
Tools	Industry standard tools; only use what's available at the present time – tomorrow could hold an unexpected 0-day	Constant R&D, development of new attack strategies based on the release of new tools and new security advisories.
Post breach analysis	Testing generally stops on compromise or successful compromise.	Leverages the breach, for exfiltration of data, or pivot into new systems and launch further attacks.
Production vs Development	Attacks are 90% never in production. Most systems under assessment are pre-production or development environments that don't represent real-world.	Attacks production environments. Attacks all layers of the production stack – may leverage weaknesses in development environments (e.g. shared/static credentials).
Escape and Evade	IDS/IPS systems are usually not enforced or disabled during testing.	Strong emphasis on evasion, best attempts to avoid detection, and circumvent security systems and policies.

References

- https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf