bsi.

...making excellence a habit.™

Enhancing your penetration testing regime

A whitepaper

Executive summary

This whitepaper explores how utilizing red-team or objective-oriented penetration testing services can provide increased insight into the security posture of an organization, its susceptibility to varying degrees of attack and its ability to detect and respond to such an attack.

Due to the rising number of high profile cybersecurity incidents and compromises, the need to more accurately simulate the Tools, Tactics and Procedures (TTPs) of the real-world adversary has become more important. Red teaming engagements are not a new concept, but have gained more prominence in recent years with the advent of CBEST (Bank of England), TIBER (De Nederlandsche Bank), iCAST (Hong Kong Monetary Authority) and CREST STAR schemes, the latter of which BSI are a member. All these schemes are similar in nature, and bring a formalized framework to offensive testing techniques which have been around for a long time.

By utilizing this type of enhanced penetration testing, an organization can gain a greater understanding and appreciation of the likelihood of a successful compromise, the types of adversary they may face, and how well they are equipped to respond to and deal with such an incident.

This paper will now explore what we currently know about penetration testing and two ways of enhancing penetration testing efforts and results; objective-oriented assessments and red teaming assessments.

Penetration testing

A typical penetration test would follow a pre-defined and approved methodology during the execution of the assessment, with the end result being a report which highlights all of the security issues and vulnerabilities identified on specific assets.

In order to identify the vulnerabilities present on those assets, a penetration test would often include performing offensive testing techniques against a pre-defined scope of assets. Assets can take on many forms; including web applications, externally facing networks and hosts, internal networks, network devices, cloud infrastructure, mobile applications and APIs, to name but a few.

Penetration testing has formed, and continues to form, a large element of cybersecurity efforts in organizations, primarily due to the value that the results provide and that it gives the organization stable and measureable output relating to the security posture of the in-scope assets at a specific point in time.

However, traditional penetration testing has its limitations. For instance, a client could opt to remove certain assets from scope such as specific hosts, areas of web or mobile applications or physical buildings, to name but a few. The result of such scope restrictions is that testing is done in isolation; the scope may have in-depth coverage of each asset, but could represent a lack of breadth across the organization as a whole.

Objective-oriented penetration testing

An organization can counter those limitations and obtain increased assurance over their security posture by introducing objective-oriented penetration testing alongside their usual testing regime in order to enhance their penetration testing output.

A real-world adversary who is targeting an organization is not concerned with any scope or time restrictions. Adversaries are interested in only one thing; compromising an organization they have targeted, via any means possible.

Objectives

In order to replicate the real-world attacker, the focus of the penetration test can be reviewed; rather than assessing the pre-defined assets with a single specific type of assessment, a more realistic penetration testing scope would be to focus on achieving pre-agreed objectives within a pre-agreed, reasonable timeframe.

With respect to this type of penetration testing, a goal can be defined any number of ways, and can encompass the many domains of information security; such as network security, application security, physical security and user awareness.

As an example, we have tested against objectives such as the following:

- Is it possible to access to card payment data?
- Can personally identifiable information (PII), which could impact on GDPR, be compromised?
- Is it possible to gain access to a specific, high value host on a network or access a segregated or high-security network or physical location?
- Is it possible to achieve unauthorized access to an operational technology (SCADA / ICS) networks from an adjacent IT, corporate network or the Internet?

In order to satisfy those objectives, BSI use the methodologies from each of the corresponding assessment types as applicable, so for example, the "Is it possible to access to card payment data?" objective, the testing team could have combined application testing, network infrastructure testing and perhaps mobile application testing (depending upon the use-case) as the means to achieve that objective. Similarly, for "Is it possible to gain access to a specific, high value host on a network or access a segregated or high-security network or physical location?", the testing team would have employed social engineering techniques in the form of physical security testing to first obtain unauthorized access to the target building, office or object, then, network infrastructure testing to attempt to access the target host or network.

Organizational buy-in

With respect to organizational buy-in, objective-oriented penetration testing would be handled in the same way as a normal penetration test, including engaging and informing all key stakeholders that the assessment is happening ahead of time. The testing team would also require the client to supply the usual information to facilitate the test, such as URLs, IP addresses, email addresses or target building addresses and credentials.

Whilst there are common themes, each engagement is developed in a bespoke manner working closely with the client and the penetration testing team.

By engaging an objective-oriented penetration test, an organization can gain valuable insight into their susceptibility to various types of attacks, increasing their ability to react to and defend against adversaries.

Red team testing

Whilst objective-oriented penetration testing typically combines a number of complimenting assessment offerings with a specific set of objectives in mind, fully fledged red team engagements take those principles and develop them further, emulating the Tools, Tactics and Procedures (TTPs) of real-world attackers. A red teaming engagement is objective-oriented, and will focus around objectives such as the ones outlined in the section above.

However, that is not the only intended outcome, such engagements are intended to provide an organization with insight into their ability to prevent and respond to an advanced persistent threat (APT).

In contrast to a traditional or goal-based penetration test, a red teaming engagement would typically be performed from as close-to-a-zero knowledge perspective as possible, with the offensive team (red team) performing the engagement from a black-box perspective. In-line with that, the organization as a whole is not notified ahead of the engagement, thus removing its ability to prepare for the assessment.

Red teaming objectives

A red team testing objective can be defined in the same way as was explored in the objective-oriented penetration testing section. By setting the objective to reflect a real-world attack scenario, the engagement becomes representative of the specific threats facing an organization. As previously mentioned, however, red teaming is also designed to exercise the internal teams and their procedures for responding to and defending against attacks, as they are not afforded prior knowledge of the test.

Red team vs blue team

As per a typical war game-based scenario, a red team engagement consists of attack vs defence, respectively the red team vs blue team; the roles of both teams are now explored a little more closely.

The red team would utilize the necessary TTPs and offensive techniques in order to establish a foothold within the organizations network and achieve the outlined objectives of the engagement. They would generally perform the assessment from a black-box perspective, with as wide-ranging a scope as possible, covering all assets that are defined as belonging to the organization. Information such as IP addresses, URLs and key assets would not normally be shared prior to the start of a red team engagement. A red team would also look to establish persistence within an organization over a period of time, such that should the blue team identify their efforts to establish unauthorised access, they would be easily able to regain the necessary access.

In contrast to the red team, the, typically internally resourced, blue team has a primary focus to proactively and reactively defend an organization against attacks, in this case, those originating from the red team. They would typically have zero knowledge of the assessment, lending itself to accurately emulating a real-world situation. Operating this way ensures the optimum level of realism by offering no means for the blue team to prepare for the attack, be on the lookout for suspicious activity or raise awareness amongst staff members, all of which may impact the effectiveness of a red team engagement. For smaller organizations, the blue team effort may well be outsourced through the use of a Security Operations Centre, who will monitor a network for suspicious activity.

By testing the blue team, the red team engagement is designed to allow an organization to have insight into the suitability of their incident response policies, procedures and technical ability. A full timeline of events is also provided to the blue team following the engagement to allow for the identification of attacks that occurred and to bolster detection capabilities if they were missed.

Assessment levels

Within a red teaming engagement, there are a number of different levels of testing, each of which are intended to represent the types and level of attack an organization may face, dependent on their risk profile.

Threat intelligence is the first phase of a red team engagement and is used as a way to inform the assessment, and to highlight the type of threats that the target organization may face and from which adversaries. The output from this phase dictates the type of adversary and their skill level that will be imitated during the testing.

Examples of types of adversaries could range from an opportunistic attacker using off-the-shelf products, exploiting known vulnerabilities within common frameworks or performing a generic phishing campaign, to a slightly more sophisticated attacker who may be using more advanced techniques, such as spear phishing, using private or commercial-only exploits or commercial level implants and Remote Access Tools (RATs).

There are even further levels of adversaries that exist beyond this level, including nation states, who would perform very sophisticated attacks, including using custom implants and RATs, unpublished zero-day vulnerabilities or advanced physical attacks. The assessment level required to be replicated should be based on the risk profile of the organization.

During the assessment, there are also varying levels of "noise" that can be replicated which correlate to the level of adversary being emulated. The lowest level of adversary highlighted here would typically be quite noisy on a network by performing activities which should be easily detected. The more advanced adversaries would perhaps be a little less noisy minimizing scan activity and avoiding techniques such as brute-forcing to further minimize the likelihood of detection. The nation state adversaries would typically be very stealthy, often performing these attacks over a long period of time whilst evading security products such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and anti-virus solutions. The levels of "noise" can be tuned up or down during the engagement to simulate the level at which attacks are formed.

Organizational buy-in

In comparison to penetration testing or objective-oriented testing, a red teaming assessment does require a much higher level of organizational buy-in from the outset to be accepted and successful. Typically, the involvement and drive for such an assessment comes from the senior management within an organization to provide assurances that the organization is as resilient to attack as expected or to independently highlight the impact an organization's current security posture and its security budget, could have on the business.

Additionally, there would typically need to be buy-in from other areas of the organization too, including HR due to the people element of the testing and also the legal team, to ensure that the testing is above board and does not break any laws or contracts that the organization is bound to.

Other than the above, the remainder of the organization is typically unaware of the engagement to ensure the realistic nature of the testing is upheld.

Conclusion

The penetration test, which has been a focal point of the industry for many years, is a tried-and-tested method for understanding the security posture of assets. That being said, there are limitations to this approach, and it can indeed be enhanced.

This whitepaper has explored two additional testing types which can add a real-world element to organizations' penetration testing efforts; objective-oriented penetration testing and red teaming. Both types of assessment offer an advancement over standard penetration testing as they reflect realistic attack scenarios and therefore allow organisations to better understand their cybersecurity weaknesses. Also, by shifting the focus of the test to pre-defined and agreed objectives, the testing can then encompass the many different domains of cyber and information security across the organization.
Planning and delivering an objective based penetration test or red teaming engagement, an organization can gain a greater understanding and appreciation of the likelihood of a successful compromise, the types of adversary they may face, and how well they are equipped to respond to and deal with such an incident.

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

bsi.

India

Call: +91 11 4762 9000

Email: info.in@bsigroup.com

Visit: bsigroup.com/en-in