Red Teaming

When did you last test the security of your systems?

Call today to book the experts »

What is Red Teaming?

A red team engagement is an objective-based assessment that requires a holistic view of the organisation from the perspective of an adversary. This assessment process is designed to meet the needs of complex organisations handling a variety of sensitive assets through technical, physical, or process-based means.

The purpose of carrying out a red team assessment is to demonstrate how real world attackers can combine exploits and tactics to achieve their goal. It is an effective way to show that even the most sophisticated technology in the world means very little if an attacker can walk out of the data centre with an un-encrypted hard drive. Instead of relying on a single network appliance to secure sensitive data, it's better to take a

Penetration Testing

Social Engineering

defence in depth approach and continuously improve your people, process, and technology.

Red Teams are brought in by mature organisations to assess their blue team to ensure that, should a real world attack occur, the defensive capabilities are sufficiently tested and prepared.

How does it differ from pentesting?

It differs in may ways, whereby usually the scope is much larger; including physical and social engineering aspects. They also are usually much more covert than pentests; as an attacker is trying to be stealthy (understanding how operational security works and how to be stealthy is useful and key to emulating threats) and hide their tracks on the target network, the red team should opt to emulate this.

It also follows an attack <-> defend methodology whereby the red team is there to outline attack paths and better educate the blue team should a real attack occur. Red teams test full stacks of processes, people and technology and are much more than just vulnerability assessments/penetration tests.

Daniel Miessler put it perfectly;

> *Red Teams are most often confused with penetration testers, but while they have tremendous overlap in skills and function, they*

are not the same.

Fundamental areas of understanding

It is important to note that the sections below are not all encompassing and are only the tip of the iceberg when it comes to delivering red teaming.

1: Common phrases & acronyms

- **C2 Frameworks** – Command-and-control servers, also called C&C or C2, are used by attackers and/or threat actors to maintain contact and communications with compromised systems within a target network.
- **Implants –** Hardware or software tooling used to gain an initial foothold into an organisation, usually used to communicate outbound to a C2 infrastructure setup. Attackers use implants to gain access to target networks, often they are the first point of contact with a network. They usually come in the form of a physical drop box(a small [usually] Linux based computer with a 4G or network connection outbound to a C2 server) plugged into the target network OR as some form of software remote access tool(RAT), usually custom code written to bypass endpoint detection and response(EDR) solutions.

- **EDR Solutions** – Endpoint detection and response solutions are a bit like anti-virus solutions on steroids, whereby they are no longer based off of signature detection and smarter in their detection. A lot of solutions out there now do network monitoring and are centrally managed meaning that the blue team(defence) has oversight as to what is going on the network and respective computers.
- **Indicators of Compromise(IOCs) –** Indicator of compromise in computer security is an artefact observed on an operating system or network which indicates that a computer network has been breached or there has been an intrusion. IOC is commonly used when describing attack vectors and indicators that an attacker has been on a network.
- **Advanced Persistent Threats(APT)/Threat Actors –** When discussing APT groups, usually they are described as an unauthorised attack carried out by a certain type of attacker. Usually APT groups are either organised crime (OCG), nation state attackers or other motivated attackers. The attack can be described as when an unauthorised user gains access to a system or network and remains there for an extended period of time without being detected.
- **Tactics, Techniques, and Procedures (TTP)** – This describes an approach of analysing an APT's operation, looking at how it has been executed. Usually TTPs are mapped against the ATT&CK framework. Certain TTPs can be used as means of profiling a certain threat actor. The word Tactics is meant to outline the way an adversary chooses to carry out their attacks from the beginning till the end.

2: Windows Enterprise networks

Red Teamers need to understand windows networks and how domains are set up. Having a fundamental understanding of active directory is an excellent start; why not setup your own domain and understand how networks are built? Neil Lines(@myexploit2600) has a great post on creating an active directory environment and a domain setup, this can be found on his blog here.

Some of the experience around networks cannot be gained in a heartbeat unfortunately as it needs to be built up from seeing different set ups. So, following on from building your own you'll want to look at how others are set up. This can be achieved in several ways. First and foremost would be to do internal infrastructure penetration testing to see clients' networks and how they are glued together.

If you don't have the opportunity to see bigger networks as part of a day job, there are lab environments around that do somewhat emulate an enterprise network with scripted users. However I will say that some of these set ups are not aimed at new folks starting out as they can be quite challenging.

To get a better feel for how active directory and windows security operates, it is worth checking out Directory Ranger on twitter. When it comes to learning offensive techniques too it is just as important to understand how those environments are built and defended. As a red teamer you need to have an understanding of building, defending and breaking to be more effective.

If you are interested in cutting your teeth on pre-built environments it is worth checking out hack the box pro labs. At the time of writing there is

Offshore and Rastalabs both paid for on a monthly basis ~£90/Month. There is also the windows red team lab by pentester academy; I've not done this personally but have heard mixed reviews!

3: Operational security

Operational Security, often referred to as OpSec, originated in the military. The military leveraged opsec to identify, classify and protect information that can be exploited by opponents and used to collect critical info about a certain mission, organisation or an individual.

Opsec is both a strategic and analytical process used in all areas and elements of security. One of the main objectives of OpSec is to observe the data you want to protect from the angle of an opponent, just as it's done by red teams.

The primary objective of cyber security is to protect yourself and your business against organised crime groups(OCGs), hackers, or anyone who attempts to obtain data that can be used to reveal sensitive information. OpSec is there to put you one step closer to that goal.

In a modern day of social media it is even easier to collect information about a company or individual using minimal effort. It can be done in only a few hours of good targeting and intel gathering.

Gathering intelligence about organisations is also easy for the experienced attacker. Targeting, gathering and analysing publicly available data is mostly done with open source intelligence tooling.

With minimal effort, it is possible to identify IP addresses, domain names, servers, technology in use and much more about an organisation. With all this data in the wrong hands, there is high potential for serious damage. This is the very reason why constant work with data, monitoring its transfer, and looking at it through the eyes of an attacker, will place you one step ahead of the threats, and one step closer to a better security system altogether.

4: MITRE ATT&CK

Mitre's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a knowledge base with information about offensive actors behaviour, it outlines the different parts of an attack cycle and tactics, techniques and procedures leveraged by different adversaries.

Attackers will use thousands of different entry methods via malware, trojans, back doors and the rest. However, once they have access to a network, most exhibit a lot of common behaviours. They learn about their surroundings and the environment they're in, gather credentials for legitimate users and accounts, and move to other systems in the network to steal information or set up some longer-term operation or effect.

ATT&CK is a widely known about and understood matrix for mapping attacks and emulating threats, therefore it is important for those learning the dark arts to understand the different techniques used and how to replicate and emulate them.

5: Reconnaissance

Alongside understanding TTPs it is just as important when starting out, to understand the process of recon. Having the ability to identify points of interest and add them into potential attack paths is a key skill to learn. Red team engagements typically are led by threat intelligence. However, to make waves into learning, it is worth looking into open source intelligence techniques before diving head first into cyber threat intelligence(CTI). While CTI is an important step pre-engagement, not all clients want full TI, some are more interested in black box approaches.

This is where learning the skills of recon can come into their own, being able to identify resources, domains, IP ranges, documents, individuals, technologies and everything in-between. There are so many write-ups about OSINT and bug bounty recon and both are directly applicable for asset identification for red teams. It is worth checking out intel techniques for OSINT tooling and information.

Further reading

- Red Team Toolkit – An in-depth github containing hundreds of links to tooling and reading.
- SpectreOps Blog – SpectreOps are a US based company who run training on red and blue teaming; their blog and consultants' blogs have a massive wealth of information about evolving techniques and tactics.

- Red Team Tips – Vincent Yiu has compiled many different tips for red teaming and a few gotchas which are incredibly useful to note!
- Rastamouse Blog – Rastamouse is a red teamer who frequently puts out content related to red teaming and new techniques. He is also the creator of rastalabs; a CTF/Windows environment geared towards learning red teaming.
- Red Team Sec – Red Team Sec is a subreddit with a constant feed of new posts specifically around red teaming.

Get in touch

020 3095 0500

info@pentestpartners.com

Contact Us »

Verney Junction Business Park
Verney Junction
Buckingham
MK18 2LB
United Kingdom Map »

Connect

Twitter
LinkedIn
YouTube

CHECK IT Health Check Service | CREST | PCI Security Standards Council QUALIFIED SECURITY ASSESSOR | CYBER ESSENTIALS