SERVICE DESCRIPTION

Purple Teaming: Attack and Defense Drills

Service Scope

At SpiderLabs, we build our purple teams from our very best consultants. We have a pool of over 140 penetration testers, red teamers, security researchers, malware reverse engineers and incident responders globally. Our team comprises members sourced from more than 16 countries globally, with each team member having an average of 12 years' experience. Each year we conduct more than fifty Red Team engagements, over 4000 manual penetration tests, and over 1000 incident response engagements. We utilize this wealth of experience to create a unique engagement that maximizes the return on investment to our clients.

Our purple teaming service simulates threats to your organization based on real-world intelligence. We utilize our team of dedicated researchers, red teamers and blue teamers to create tactics, techniques and procedures (TTPs) that closely replicate real-world threat actors. We then coach your blue team leaders on how to resist, detect, respond and recover from attacks in your own environment. This culminates with a mini-red team assessment where your team can pit their new skills against our ethical hackers.

The idea of purple teaming is that it is used to help organizations mature and get ready to defend in their own environment while simulating real attacks such as Advanced Persistent Threats (APTs) and ransomware-based threats. At SpiderLabs we feel this is the very best preparation for red teaming and also enhances your defensive capability and increasing maturity. The way our purple teaming works is that we embed a red and blue team coach within your defensive team and run a series of drills and teaching break-outs that replicate real life attack simulations. Following this, we assess the learning outcomes and progress of the team by running a mini-red teaming assessment at the end. Essentially, we train your team in the offensive and defensive arts.

The structure of the engagement is based around two key concepts and methodologies: the Cyber Kill Chain and the Mitre Att&ck Matrix. We utilize these frameworks to structure the sessions and to ensure coverage of common advanced attacks during both our purple and red teams. More detail is given in our methodology section, directly below.

Project Phases & Timelines

This section defines the potential tasks for the project. The appropriate estimate, based on Trustwave's knowledge of the date of signatures in the scoping document and/or order form, will likely outline man-hour initiative based on the phases below.

Phase 0: Engagement Model and Prerequisites

The following engagement model defines our approach at a high-level; however, we can always tailor this to meet your organization's expectations and specific requirements.

It is expected that your organization understands the assets, processes and critical systems that you want to be included in the assessment. Typically, we advise that tests are performed on live environments and that critical systems are included in scope.

It's expected that your organization will assign a managerial resource to this engagement that serves as a single point of contact. It is recommended your organization establish a control group and select senior representatives that are stakeholders responsible for all critical assets and systems. This will be important when discussing simulated attack activities as part of the simulation.

It is expected that your organization prepares some basics in advance of the engagement, in order to get the most out of the assessment. If some of these elements are not in place, we can assist in getting you ready. They key prerequisites are:

- A robust vulnerability management program (scanning capability and risk register)
- Patch management, and / or a fully patched environment
- Incident Response Playbook

The reason we recommend these elements be in place, is because you need to have good security hygiene and the basics covered before you can begin thinking about resisting more advanced attacks.

Phase One: Initiation Phase and Outline Scope

Phase one starts with a project initiation meeting with the aim of creating a high-level outline scope and checking that everyone has the same understanding of the process. Key stakeholders from your organization should be present who will be involved with approving the scope and goals of the assessment.

The key elements for discussion will be:

- Identification of key functions.
- Identification of critical services or systems.
- Discussion of risk mitigation and management processes.
- Definitions of test goals.

A high-level outline scope document will be created as a result of these initial discussions. The document will be distributed to all key stakeholders in your organization for review. Key areas for this discussion will be:

- Stakeholder roles and responsibilities – establishing a control group.
- Scope – defining what systems are in and out of scope or areas that are considered too sensitive to be within scope; for example, legacy equipment that is unlikely to be resilient to modern red teaming techniques and tactics.
- Security protocols – establishing escalation paths and agree suitable communication channels.
- Contracts – finalizing contracts (legal, insurance), inclusion of contracts with any third parties, financial terms, etc.
- Letter of authority – signed by all key stakeholders giving authorization for the assessment to go ahead against the agreed scope.

Deliverables and Outputs

- Risk mitigation

Phase Two: Delivery Methodology

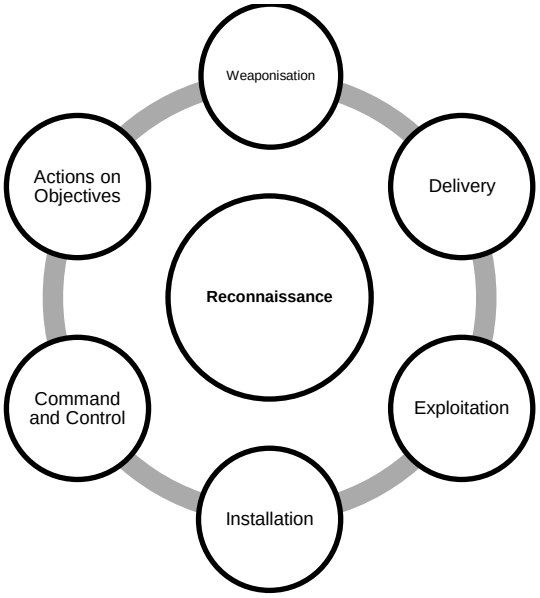
Our approach is structured around the cyber kill chain, which outlines the different phases of an advanced and persistent attack. We move through each of the kill chain phases (as shown below) in sequence, mixing both teaching sessions and live fire drills. During the engagement, our red team coach will execute mock-attacks in your live environment while your team attempts to detect and defend against the activity, under the watchful eye of our blue team coach. We check that your security appliances can detect our activity and that your team understands what we're doing and how to defend.

Planning	Malware and Tooling				Pivoting	Detection
Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C2	Action on Objectives
Preparation	Purple Teaming					Mini-Red Team
2 days	7 days					1 day

Table 1: **Engagement Structure**

Reconnaissance

Our reconnaissance phase focuses on Open Source Intelligence Gathering (OSINT) and happens within SpiderLabs in advance of the engagement. We utilize the information in the same way an attacker would, to build a view of the information exposure of your organization. We also utilize the information to build specific exploitation cases and feed into the rest of the kill chain modules. We provide full information of the data discovered and utilized within a report at the end of the assessment.



Kill Chain Fed by Reconnaissance

Data Sources and Techniques

Our SpiderLabs Research (SLR) team collects telemetry daily from multiple sources both internally and through third party relationships. Internal sources include direct research, multiple service specific honeynets (web, email, remote services) as well as telemetry directly acquired from our customer base. SLR also maintains third party relationships and threat exchanges with organizations like Microsoft (MAPP partners), Google / VirusTotal, the Anti-Phishing Working Group (APWG), Facebook, Malicious URL Threat Exchange (MUTE), and Team Cymru.

Dark and Deep Web Reconnaissance

As part of the reconnaissance phase of the assessment, we include specific findings from the dark web. In order to do this, we utilize intelligence from the dark and deep webs gathered by our research team. The information that we gather can indicate whether an organization or even their staff have already been breached and if data has been exposed. This adds great value for the client and useful intelligence when building out the purple teaming assessment scenarios, as this gives real-world evidence to base this on.

Our research team has many specialists who go ‘under-cover’ on the dark web to unearth information related to stolen data that has been bought and sold on dark markets. These ‘agents’ have deep insights into how these transactions happen and they feed this into our threat intelligence. We also utilize a proprietary platform that indexes vast amounts of the dark web including Tor Onions and hidden encrypted networks. Utilizing this platform, we are able to search for credit card details, email addresses, passwords, usernames, PII and much more that have been leaked onto the dark web.

Weaponization

This phase typically involves preparation and staging; the reconnaissance phase will have identified possible vectors of attack against your organization based on the output of Open Source Intelligence (OSINT) gathering and dark web analysis. An example would be identified metadata from available documents that disclose Microsoft office versions, Operating System versions and originating authors.

Once the target technologies have been identified the consultant can use this information to create a viable attack payload. An example of this would be to create an MS Office document with an embedded payload that will execute system commands on either opening or closing the file. The authenticity of this document can be further enhanced by including company branding and calls to action that persuade a user to accept any warnings presented to them.

The consultant will discuss the information gleaned from the OSINT phase and explain why this led to the specific weaponization of the payload being chosen.

Delivery

Once a viable payload has been created, then the goal is to attempt to successfully deliver this payload through any edge controls and security boundaries. As an example of an external based source attack, the reconnaissance phase will have feed into the creation of a focused target list, and the objective will be to gain access to internal systems in the context of those users through a targeted email spear phishing campaign.

The first stage of this delivery process could include benign email correspondence through a legitimate action. An example of a benign action would be to request information pertaining to a current job vacancy. This may also provide further confirmation of implemented technologies; for example, the addition of content headers in a return email disclosing a mail gateway scanning platform. Other common delivery mechanisms include USB drops, watering hole attacks (in-direct compromise) or direct exploitation of web sites.

Once the consultant understands the security controls, they will then attempt payload delivery to the selected target list. This phase highlights the effectiveness of the edge controls together with your organizations ability to detect these types of external based attacks and control these at the edge. It also validates awareness of internal staff in being vigilant against email-based threats.

The red team coach will utilize various delivery mechanisms to ensure that your organization is resilient to different TTPs (tactics, techniques and procedures). We will utilize the most likely vector based on the OSINT / reconnaissance phase and then look to walk through other vectors.

Exploitation

The objective of this phase will be to determine whether, firstly, an attacker is able to execute the malware (including both the initial dropper and payload of the implant) with a view of achieving a foothold into your internal network; and secondly, to elevate privileges on the local system in order to achieve persistence and to facilitate further reconnaissance to assist pivoting. This may highlight weaknesses in your endpoint security, AV, system hardening, patching, egress filtering, group policy controls and/or lack reporting. The consultant will execute a custom implant which will initially be a dropper which will then fetch the actual implant payload. The consultant will work with the incident response teams to determine whether this activity has been detected and also observe internal responses to this.

After this simulation runs, execution and exploitation in relation to the implant will be discussed, touching upon the various mechanisms and techniques utilized in order to be stealthy, ranging from PowerShell (v2 – v5) to Windows Management Instrumentation (msbuild).

When selecting (or developing) exploits, Trustwave SpiderLabs ensures that every care is taken to launch the exploit safely and handle the communications appropriately. To ensure that this is done, we follow the following selection criteria:

Specific intelligence on appropriateness (e.g. Windows 7 exploits for Windows 7 hosts);

- We select only exploits that can be controlled (and we have tested ourselves offline in advance);
- We select exploits that we can track and audit;
- We select exploits that we can clean up after and resilient by design;
- We select exploits that are reliable and infrequently cause system crashes or undesirable states, such as DoS.

Installation

The objective of this phase will be to assess your organization's ability to detect (and perhaps deter) an attacker being able to install an implant (or RAT) to gain a persistent foothold into your internal network. This simulation may highlight gaps in your endpoint security, system hardening, group policy controls and/or lack reporting. The consultant will attempt to gain persistence of the implant through common techniques. The consultant will work closely with the incident response team to determine whether any alerts have been triggered due to this action, together with observing appropriate response (either manual or automated).

Following this simulation, common persistence methods and techniques will be discussed at length, ranging from registry run keys to other start-up items.

We include the following design attributes in each implant we create to assure safe operation of our engagements.

- Removal
  - Each implant has the capability of being fully controlled manually (after establishing connectivity to the C2 server). In addition, there is a mechanism that uninstalls and deletes the implant after a specified period, should the implant not make contact with the C2 server.
- Encrypted communication channels
  - All our implants use strong encryption for data in motion and data at rest. This means that we encrypt all communications to and from the C2 server.
- Encrypted local data store
  - All data collected within a client network is stored using strong encryption.
- Attribution and identification
  - All our implants are attributable to us. We vary the specific indicators of compromise on a per engagement basis, this information is outlined in the Risk Management plan and will be explained in detail to the client in advance of testing. Typically, we drop a text file (containing our contract information) within a hidden folder on the operating system.
- Logging
  - We log all activities performed during the testing phase. This can be made available at the end of the engagement as raw data if required.

- Persistence controls
  - Each implant has different attributes based on the engagement it is created for. Persistence after reboot is important in a lot of cases and is often built into our design.
- Stealth
  - Our implants are designed not to be easily detectable. They are also designed to bypass most major AV products.
- Delivery mechanism control
  - Our implants are designed to be deployed using a multitude of vectors. These can include delivery via: drive by web attacks, USB introduction, email attachment and direct install.
- Beacon domains registered
  - Any and all domains we register point back to us. When creating new Internet-based sites / hosts for our scenarios, we register the domains in our name, so that it can be quickly established that any suspicious activity is being performed by Trustwave.

Command and Control

The objective of this phase will be to identify whether your organization is able to detect (and stop) a common C2 channel and to measure the effectiveness of the response in relation to it. The consultant will setup a C2 and issue non-malicious commands in order to generate network traffic to assist with the detection. Emphasis will then be placed on exfiltration of data, to determine whether an attacker is able to exfiltrate data out of the network through gaps in egress filtering. The consultant may use the same C2 channel for this or an additional technique.

Following the simulation, C2 channels will be discussed at length, delving into the various types, from the most common (using common ports with no encryption) to the more advanced, to those using multi-stage channels with custom cryptographic protocols. Exfiltration techniques will also be discussed, covering the common and typically easily detectable to the less common and more covert, such as scheduled transfers and exfiltration over other mediums.

Actions on Objectives

This phase involves the execution of a mini-red team assessment. The objective of this phase will be for the consultant to utilize all the phases in combination to achieve the goals set out in the statement of work. The consultant will work through pre-defined scenarios, highlighting whether it is possible for an attacker to compromise high value assets and/or areas of concern specific to your organization or industry.

Phase Three: Reporting

Following the conclusion of the engagement, the output will be made available to your organization. Following the production of the report, SpiderLabs will run a one-day ‘round table’ session with your stakeholders to discuss the engagement. The purpose of this meeting is to discuss the findings, methods and remediation requirements.

Deliverables and Outputs

Any applicable deliverables shall be outlined in the scoping document.