WHITE KNIGHT LABS

RED TEAM

White Knight Labs Red Teaming Services enable organizations with mature security postures to perform advanced testing of their people, processes, and procedures. In a standard penetration test, the testers are "allowed in" and are not stopped after detection. In an Red Team Engagement your team will have standard protections in place and may stop the attack in process, causing the team to reassess and pivot, to achieve an agreed upon goal. Our team will leverage multi-faceted attacks using more advanced real-world scenarios.

Attacks performed, tactics used, and results collected during these simulations are compiled into actionable reports that identify risk to your organization's most valuable assets. Our reports provide you with highly valuable information regarding security posture and security awareness levels of employees, physical protections, blue teams, and technology deterrents. This information is a critical component of measuring the overall security posture and can help pinpoint security gaps and drive risk-focused security spending.

Red Team Engagment

Our Red Team Engagements involve establishing a goal that is technical and/or physical. White Knight Labs works intimately with the client to establish the rules of engagement to attain the goal. Then WKL security consultants develop a plan for achieving that goal. This could involve them being physically onsite at the target location. They could either overtly interact with staff to persuade them into performing certain actions or covertly attempt to blend in and gain access into certain areas or information. Both overt and covert tactical approaches can easily be blended into a single engagement for a more comprehensive evaluation.

A Red Team Engagement offering could also include: gaining network control, compromising cameras and security systems, or data exfiltration. Goals during a Red Team Engagement can be focused on exploiting technical security or physical security.

A Red Team Engagement could test your security awareness training, corporate policies, physical security, and detection/response procedures.

Advanced Adversary Simulation

An Advanced Adversary Simulation involves setting a goal that is related to technology (i.e. being able to extract HR information) and establishing the rules of engagement to obtain it. These types of engagements do not involve physical breaches, however, they may involve email phishing, phone vishing, dropping or mailing USB drives or breaching the network. The Advanced Adversary Simulation may also include testing: email filters, security awareness training, network protections, and/or blue team responses.
Regardless of the type of Advanced Adversary Simulationthat is chosen, White Knight Labs will work in conjunction with you to create the rules of engagement to solidify details such as:

- Authorized actions the red team may perform in pursuit of their objectives
- Roles and responsibilities for each team member involved in the attack
- A high-level description of the types of attacks that could be executed
- Explicitly prohibited tactics
- Authorized targets and target networks
- Restricted items on the network
- Engagement objectives
- Types of hardware and software that might be used

Additionally, at the end of the engagement, White Knight Labs will conduct a highly valuable technical out-brief. This technical exchange of information provides the opportunity for a step-by-step review of each tactic, procedure, and result.

This additional discussion provides an opportunity for immediate feedback for the blue team while the events of the engagement remain current to all involved. With such a detailed walkthrough and the benefit of a question-and-answer venue, your team will hear firsthand how the red team was able to accomplish the goal.

Offensive Endpoint Evasion

True red team assessments require a secondary objective of avoiding detection. Part of the glory of a successful red team assessment is not getting detected by anything or anyone on the network. As modern Endpoint Detection and Response (EDR) products have matured over the years, red teams have followed suit.

When it comes to measuring the effectiveness of EDR products, White Knight Labs specializes in testing Endpoint Detection and Response (EDR) products to determine if host-level security is effective. WKL will test your current EDR solution and match its effectiveness against Microsoft's industry recognized EDR product Advanced Threat Protection

Evasion Concepts

Endpoint Detection and Response (EDR) products monitor programs during execution to detect/respond to suspicious behaviors. This complements traditional anti-virus functionality which uses signatures and heuristics to block unwanted programs prior to execution.

While evasion can be a broad term, attacker responses to EDR typically fall into these buckets:

1. Avoidance:
Furthering mission goals on systems that don't have the product installed or enabled (e.g. operating from an un-provisioned endpoint, or proxying traffic through a provisioned endpoint).

2. Blending In:
Hiding in the noise of what's commonly recorded by EDR sensors (e.g. using common parent-child process relationships).

3. Abusing Blind Spots:
Taking advantage of areas that the sensor doesn't capture or report on (e.g. using certain APIs not being logged, making direct syscalls).

4. Tampering Sensors:
Altering sensor behavior to the attacker's advantage (e.g. removing hooks, patching the sensor so malicious behavior is not reported and/or collected).

The White Knight Labs Offensive Endpoint Evasion service offering involves testing:

- Malicious payload execution against your current endpoint protection
- Logging capabilities and threat detection
- Application control and device policy enforcement
- Basic privilege escalation and lateral movement