GOTHAM SECURITY

AN ABACUS GROUP COMPANY

Attack Simulation Services

Red Teaming & Black Box Network Penetration Testing

Identify and exploit perimeter vulnerabilities within your cloud, network and server infrastructure. We chain specifically-tailored exploits and attacks together to gain privileged access to network systems and confidential data. Our comprehensive penetration testing methodology is in accordance with NIST SP800-115 (Technical Guide to Information Security Testing and Assessment) and PTES (Penetration Testing Execution Standard).

Objectives:

- Replicate the vantage point of a malicious actor with no access or prior information about your organization and its external / internal information systems.
- Identify high risk vulnerabilities in your organization's external and internal information systems.
- Expose the weakest areas of your organization's security posture by exploiting the highest risk vulnerabilities and attack vectors present in your external and internal information systems.
- Provide a full due diligence report including:
  - Vulnerability details
  - Risk mitigation & remediation recommendations
  - Reconnaissance process
  - Exploitation methods
  - Information system statistics
  - Lists of any compromised systems/credentials
  - Network diagrams
  - And more...
- For standard network penetration testing projects, Gotham Security provides a free retest and report after a 30-day remediation period.

Standard Engagement Process:

Typical Timeline of Initial Test: 2 Weeks
Scheduling Kickoff: 1 - 2 Weeks after ROE is signed
Remediation Retest Policy: Free within 30 days of initial report delivery

- Once the client has financed the project, Gotham Security will provide the client with a Rules of Engagement (ROE) document that outlines the scope of the tested client information systems, project assumptions, and Gotham's commitment to our client's information systems' Confidentiality, Integrity and Availability (CIA).
- For any network penetration testing against a client's internal information systems, Gotham Security will either ship or hand deliver Gotham's network scanning appliance.
- Gotham's network penetration testing typically takes place in a 24 x 7 format over the course of 2 weeks. Special attention is provided to ensure client information system CIA remains unaffected throughout the project.
- After the first network penetration test is completed, Gotham will present the report findings with the client and discuss the remediation recommendations provided in the report.
- After the 30-day remediation period, Gotham will perform rescanning of the same information systems to validate if previous risks were indeed remediated.
- Gotham will then present and provide the client with a post-risk mitigation network penetration testing report.

Social Engineering and Physical Penetration Testing

The scale of our operation goes beyond amateur spear phishing testing. We emulate a sophisticated malicious actor manipulating your organization's employees into exposing company weaknesses, including unknowingly allowing unauthorized access to sensitive corporate information via multiple avenues (both remotely and / or in-person).

Objectives:

- Model sophisticated malicious actors' creative attacks focused on exploiting the human error. We expose company vulnerabilities in one of the most realistic simulations of a real malicious agent's attack vectors.
- We use up-to-date techniques, including remote and in-person attacks.
- We evaluate the following:
  - Organization employee security awareness
  - Maturity and implementation level of technical security controls throughout the organization
  - Organization security awareness policies and employee adherence to those policies

We provide your organization a full due diligence report including information such as:

- Utilized social engineering techniques
- Social engineering campaign data
- Observed administrative / technical risks
- Risk mitigation recommendations
- Supporting evidence of all campaign findings

Standard Engagement Process:

Phone Call and Email Pretexting
Pretexting is the act of creating and using an invented scenario (the pretext) to engage a target in a way that increases the chance that the target will divulge information or take an action that is most often not in the target's best interest.

Email Spoofing
Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.

Website Phishing
A phishing website is a web page made to fraudulently imitate a legitimate website. Typically, a phishing website only consists of a login page, where victims of a phishing email are directed in order to harvest their credentials, after which they are forwarded to the legitimate website to avoid arousing suspicion.

Domain Typo-Squatting
Domain typo-squatting refers to the practice of buying and using a website domain that is very similar to a legitimate website, but with subtle typographical differences such as replacing O's with 0's or utilizing slightly misspelled words. This technique is often used in conjunction with phishing.

Employee Impersonation
Employee impersonation is the process of fraudulently presenting oneself as a company employee or trusted vendor by utilizing fake props such as uniforms or badges, and by providing insider information such as employee names and details pertinent to the company.

In-Person Wireless Cracking
In-person wireless cracking is the practice of defeating the security of a wireless local area network by hovering outside a company office or building and exploiting poor Wi-Fi configurations and/or weak authentication pre-shared keys (PSKs).

USB Storage Malware
USB storage malware involves the creation and installation of a malware payload onto a USB storage device, so that upon inserting the device into a computer, the malware is either automatically executed or executed by an unsuspecting employee on the target computer.

USB Keyboard Emulation and Malicious Code Injection
USB keyboard emulation and malicious code injection is like a USB storage malware attack, with the primary difference being that upon inserting this USB device into a target machine the USB device imitates a keyboard rather than appearing as a storage device. It then delivers a series of keyboard commands that executes malicious code to the target computer. The ability to emulate a keyboard allows the USB device to bypass common IT security controls that prevent typical USB storage devices from being accessible on company computers.

Corporate Data Exfiltration
Corporate data exfiltration is the act of unauthorized transportation of sensitive company data from a corporate network environment into the possession of a malicious actor (external to the company) for later analysis and use.

Network Backdoor Device Installation
Network backdoor installation involves the installation of a physical "leave behind" device that is connected to a corporate network. The network backdoor device allows for remote access to the corporate network and the interception/manipulation of wired corporate network traffic.

(212) 696-0500
hello@gotham-security.com