BLUE GOAT CYBER

Black Box Penetration Testing Services

- Unauthenticated Network and System
- External and Internal Black Box Penetration Testing Services

Steps to Schedule Your Penetration Test:

- Schedule a 30-minute Discovery Session
- We determine IF and HOW we can help
- We provide a Tailored Proposal
- Together, we review the Proposal

A Black Box Penetration Test, also known as a unauthenticated test, is commonly used as an external penetration test against an organization's Internet-facing systems, such as the following:

- Web Servers
- VPN Concentrators
- Firewalls
- Routers
- Proxy Servers
- DNS Servers
- Mail (SMTP Servers)
- Custom Application Servers
- Cloud Services

We have performed many external Black Box Penetration Tests against the above systems.

As ethical hackers, we emulate an attacker by utilizing similar techniques to perform reconnaissance, identify vulnerabilities, and break into your systems. Unlike an attacker, however, we stop our penetration test before exposing sensitive data or doing harm to your environment.

With a Black Box Penetration Test we have unauthenticated access and have little prior knowledge, except the IP Address, domain name, or URL, about the systems in scope.

We've also performed Black Box Penetration Tests against embedded systems and LRUs (Line Replaceable Units) that integrate into larger systems, such as commercial aircraft, weapon systems, or SCADA/ICS systems. A few examples of what we've tested:

- Medical devices
- Commercial aircraft
- Vehicles
- Offshore Drilling Platforms

METHODOLOGY

We follow a seven phase methodology designed to maximize our efficiency, minimize risk, and provide complete and accurate results. The overarching seven phases of the methodology are:

- Planning and Preparation
- Reconnaissance / Discovery
- Vulnerability Enumeration / Analysis
- Initial Exploitation
- Expanding Foothold / Deeper Penetration
- Cleanup
- Report Generation

BENEFITS / RETURN ON INVESTMENT (ROI)

We think it is better to have an ethical hacker find the holes into your enterprise than an adversary. Our Black Box Penetration Testing provides details on exploitable vulnerabilities in a prioritized, tangible manner. Our report allows you to better understand what your environment looks like from an attacker perspective. This helps you prioritize efforts to mitigate risk to reduce breach likelihood or damage.

Not only do our Black Box Penetration Testing Services show you what your attack surface looks like to an adversary attacker, but they can be used as a safe way to test your organization's Incident Response (IR) and digital forensics capabilities. Our Penetration Testing services can be used to tune and test your security controls, such as your IDS, Firewall, Endpoint Security, Router ACLs, etc.

Our Penetration Testing services also help you meet compliance audit requirements such as HIPAA, PCI DSS, SOC 2, and FISMA.

DELIVERABLE

The **Penetration Test Report** includes IP addresses tested, vulnerabilities discovered, steps taken during the assessment, exploitable areas discovered, and prioritized recommendations. For any systems we are able to exploit, an "Attack Narrative" section is used to discuss step-by-step the process we used to gain access, escalate privileges, etc. The report sample below is used as a quick reference to focus remediation and mitigation efforts on. The findings are ranked by risk rating and include recommendations (rec), reference links for mitigation steps, and tester notes.