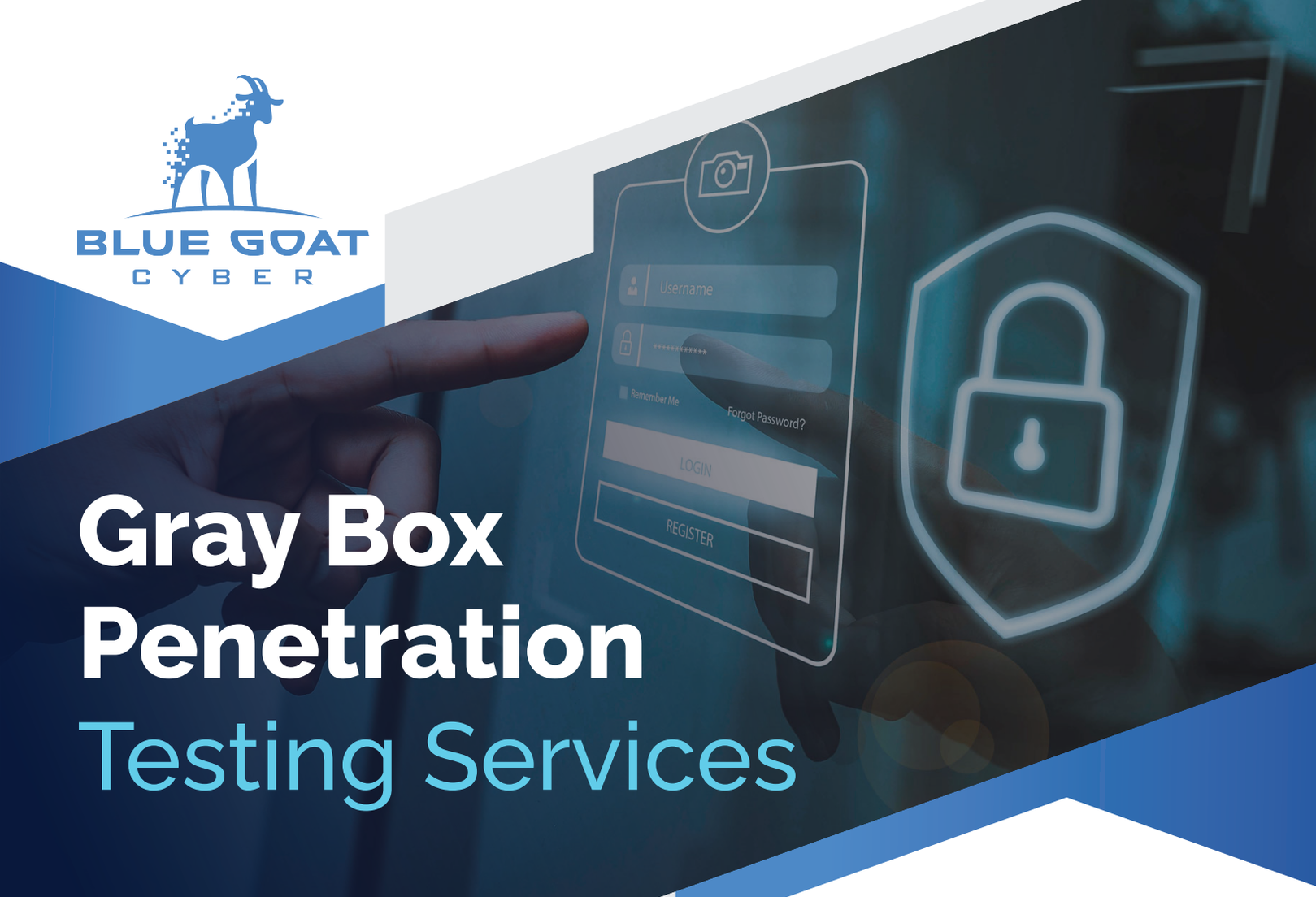
BLUE GOAT CYBER



Gray Box Penetration Testing Services

As ethical (white hat) 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 test before exposing sensitive data or doing harm to your environment. With a Gray Box Penetration Test, we have "user" level knowledge about and access to a system. A Gray Box Penetration Test is typically used when you want to test an insider threat or test an application that supports multiple users. The insider threat is tested to see what damage a user (non-administrator) could do to your environment. Application testing is used to test authenticated user access to ensure a user on an application cannot access another user's data or escalate privileges.

Steps to Schedule Your Gray Box 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 Gray Box Penetration Test is commonly used in the following two scenarios:

- Insider Threat
- Application Testing, such as a Web Application

We are often provided user-level access to an Enterprise Windows Domain for the Insider Threat scenario. We use this authenticated, user-level access to validate and test user rights, permissions, and access. A user should only be provided what is required for them to perform their job. Many organizations do not fully understand or have documented all the access a "user" may have. For example, we have found organizations where a standard user-level account could access the network shares of everyone in the company, including the CEO. This was due to improper permissions on network shares. This is not an uncommon scenario.

For the Application Testing scenario, we typically test an application, such as a web application or custom-built application, as an authenticated user. We log on to the application as that user and then perform testing to see if we can perform any of the following:

- **Horizontal Privilege Escalation –** where an authenticated user can access another user's data. An example of horizontal privilege escalation is a bank application, where an authenticated user's account number shows up in a URL. I've just performed a horizontal privilege escalation if I can change the account number in the URL to another account number and access another user's banking information.
- **Vertical Privilege Escalation –** where an authenticated user can escalate privileges to an administrator-level account. An example is a web application with a value representing the username in a hidden field that is returned after successful authentication. What would happen if we changed the value from 'username' to 'root' or 'administrator' and passed this back to the web application server?

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 or insider. Our 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 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, SOC 2, PCI DSS, and FISMA.

Blue Goat Cyber
PO Box 20310
PMB 45092
Cheyenne, Wyoming 82003-7007

(307) 317-8884
info@bluegoatcyber.com