BONGO SECURITY

IS YOUR BUSINESS AT RISK?

Let us find out…before a malicious hacker does

Why should you get regular Penetration Tests?

- What would happen if a hacker would steal your digital assets?
- What legal consequences and lawsuits would a security breach have for you?
- What financial implications would you face if your IT systems are taken down?
- What reputational damage would a successful hack pose to your business?
- Did you know that 90% of all deployed IT systems have vulnerabilities?

A Penetration Test is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats. The same tools, know-how and methodologies are being used, as malicious hackers would employ.

The Value of our Services

- Discovery & Mitigation of vulnerabilities
- Reducing risk to your business
- Protecting your IT security investment
- Protecting clients, partners and third parties
- One-time off or recurring options

Why Us?

- We are experts in Penetration Testing
- Consultants holding the highest certifications (OSCE, OSCP, OSWP, CEH, LPT, CREST etc.)
- Experience across all sectors and business sizes (Private & Government)
- Pride in excellence of our work
- Your Security is our Priority!

Deliverables

Every Penetration Testing / Vulnerability Testing Service contains the following deliverables:

- Comprehensive report (Executive summary and in-depth technical report)
- Testing only at agreed testing times (for example at nights, weekends etc.)
- Mitigation Advice on encountered vulnerabilities
- Never running malicious exploits or DoS Tests unless agreed beforehand
- 1 Debrief call with the client over WebEx to go through the report
- Instant notification of critical vulnerabilities found during testing phase
- Secure report delivery by encrypted email

Bongo LLC Email: info@bongosecurity.com - Web: www.bongosecurity.com

Our Services

1. Network Penetration Testing / Vulnerability Assessment

Network Penetration Testing / Ethical Hacking is a security testing service that focuses on locating flaws in your networks, infrastructure and overall architecture (i.e. Server services, Operating Systems and other Networking components). In this service, vulnerabilities will be exploited in order to gain access to vulnerable systems. In a Network Vulnerability Assessment, which is a cost effective alternative to a Network Penetration Test, we only report on the flaws without actively exploiting them.

2. Web App Penetration Testing / Vulnerability Assessment

More than 70% of all technical attacks aim at the Application layer. This service examines your web applications from a coding and implementation flaw perspective, but also looks at other issues like SQL injection and cross-site-scripting (XSS), involving active exploitation of vulnerabilities in order to gain access. In a Web Application Vulnerability Assessment, which is a cost effective alternative to a Web Application Penetration Test, we only report on the flaws without actively exploiting them.

3. Wireless Penetration Testing

Wireless Penetration Testing covers all threat vectors of Wireless Networks. Our audits contain attempts to crack Wireless Encryption and Authentication mechanisms, include the set up of rogue access points along with test phishing portals, a variety of man-in-the-middle (MITM) attacks, Denial of Service Testing and Bluetooth Security tests.

4. Mobile Application Penetration Testing

Mobile Application Penetration Testing covers all threat vectors concerning Mobile Apps. The audits contain Application Runtime Analysis, Traffic & Encryption flaws, Insecure Storage, Code Signing, Memory Protections, Fuzzing and Exploitation.

5. Social Engineering Testing

Often the latest perimeter defenses may be in place, yet the security is breached. Why? Because an employee may plug a USB stick in, brought their own infected device into the corporate network, clicked on a malicious PDF or simple visited a malware website. Could your staff be tricked that way? Our Social Engineering services will find out.

6. Cyber Intelligence

Have you heard about the dark web? This is where a lot of illegal hacking activities take place. Has any of your confidential business data leaked out already? Are hackers planning to attack your business? Have you unintentionally shared too much information with Google? We provide you high-class reports around threats concerning your business. Reports can be delivered as a one time off or on a regular recurring basis.

"There are two types of companies: those that have been hacked and those who don't know they have been hacked."

John Chambers, Former CEO, Cisco Systems

Don't wait until you become a Cyber crime victim…
…Contact us today for a free consultation and quotation

Bongo LLC Email: info@bongosecurity.com - Web: www.bongosecurity.com