Cyber 51

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 competitor or 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 industry and government security certifications
- Experience across all sectors and business sizes
- 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 DDoS 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
- 1 Re-test after the initially encountered vulnerabilities have been mitigated (at a heavily discounted rate)

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Cyber 51

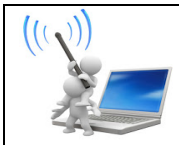
Our Penetration Testing Services

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

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.

"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."
John Chambers, Ex-CEO, Cisco Systems

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

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Cyber 51

Additional Core IT Security Services

Digital Forensics and Incident Response (DFIR) – Threat Hunting

Has a penetration test turned up a vulnerability on your network? Is something "off" with one of your systems? Have you been compromised? Our team provides digital forensics, threat hunting, and incident response services to help you defend your information and assets. Our team can help find attackers inside your network, identify how it was breached, and develop a remediation plan to eradicate their foothold. Our team has worked with the Department of Defense including the U.S. Navy and U.S. Air Force to provide Hunt Operations to identify some of the most advanced persistent threats in use today.

Advanced Cyber Security Training

Our team develops custom curriculum content for all areas of cyber security. We can provide training for all dimensions of your cyber security needs, including advanced adversary tactics, vulnerability management, detection and response, compliance management, defense architectures, and general security training for your end users to help keep your systems protected.

Security Program Development

Need general security consulting? How about help refining a security strategy? We have seasoned cyber security experts with experience in all dimensions of cyber security program development. We specialize in threat management, training, vulnerability management, risk management, incident response, comprehensive detection strategies, and corporate governance.

Cyber Risk Assessments

Our team has pioneered a cyber risk assessment approach to help you identify where to focus your valuable dollars. We can help your organization focus on where to get the "biggest bang for the buck" based upon a disciplined cyber risk assessment that prioritizes the security need with your defined risk tolerance thresholds.

Software Code Analysis

Through the use of both static and dynamic code analysis, our team is able to identify bugs or defects in software. By identifying and remediating these software bugs your code becomes more resilient to attack from intruders.

Vulnerability Research

Previously unknown software flaws pose a serious threat to any organization, whether it is a large enterprise system or a small business network, a single exploited vulnerability in one of your computers or networks can be devastating. Although a penetration test can include a small amount of time dedicated to looking for unknown vulnerabilities, sometimes a much deeper analysis of critical software and systems is required. Our team can identify vulnerabilities and create a proof of concept that illustrates how an attacker can exploit these vulnerabilities in order to adversely affect computer programs, data, additional computers or networks.

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Supply Chain Security

Companies often overlook the security of their supply chain, and place trust in the goods and services that are delivered by external organizations. Advanced attackers are willing to use any means necessary to gain access to intellectual property, including targeting third-party vendors (whom may have lax security controls). Once breached, attackers can leverage these vendors' access as an ingress point into your trusted network. We assess the security stand point of your supply chain to include: networks, programming environment, software/hardware delivery methods, external services (cloud, hosting, cluster computing, etc.), how they are storing your credentials, etc. to ensure that your inherited risk is low.

Threat Intelligence

Our team can help organizations understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats, and exploits. The emphasis here is on the external threats that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself from the types of attacks that could do them the most damage.

Insider Threat

Insider Threat may be the biggest cyber issue facing organizations today. Employees may deliberately steal from an organization, or they may unwittingly become the victims of phishing attacks, crypto viruses, or other common threats. From teaching employees how to practice good cyber hygiene to auditing of computers and mobile devices, monitoring of high risk employees, and developing a cyber program plan we can support in protecting from the insider threat.

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Our Team at Cyber 51

All our Security Consultants have at least 5+ years professional work experience. Many of our Security Consultants have worked with the US government, US military & financial organizations. They hold the highest vendor and government certifications. Additionally, may of our Consultants hold various active US Security clearance levels. Our consultants are certified and operate to Penetration Test compliance standards.

Internationally recognized Certifications

- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- Licensed Penetration Tester (LPT – EC-Council)
- Certified Ethical Hacker (CEH – EC-Council)
- Certified Security Analyst (ECSA – EC-Council)
- Computer Hacking Forensic Investigator (CHFI – EC-Council)
- Certified Information Systems Security Professional (CISSP – ISC)
- GIAC Certified Forensics Analyst (GIAC GCFA)
- GIAC Exploitation Researcher & Advanced Penetration Tester (GIAC GXPN)
- GIAC Reverse Engineering Malware (GIAC GREM)

U.S. Government Certifications

- INFOSEC – NSA Information Systems Security Professional
- 4011 Recognition – U.S. National Security Agency (NSA)
- 4013 Recognition – U.S. National Security Agency (NSA)
- DoD Information Assurance Awareness

UK Industry and Government Certifications

- UK CREST Registered Penetration Tester

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Cyber 51

Why Cyber Intelligence?

- Has your business been hacked & sensitive information has been disclosed?
- Have you unintentionally disclosed confidential information online?
- Are Hackers talking about your business and potential attacks your company?
- Are any exploits available, which could breach your security?
- Are any industry specific threats concerning your business?

Who should get Cyber Intelligence reports?

- Businesses that use online IT systems and hold confidential data
- Businesses that don't want lawsuits from clients, when data has been stolen
- Businesses that have fallen victim and don't want to wait for the next attack
- Businesses that must comply to Industry Compliance regulations
- Businesses that understand that being pro-active is cheaper than re-active

Our Cyber Intelligence reports are not comparable with classical technical Cyber threat feeds or standard security advisories. Our Cyber Intelligence Analysts gather intelligence, which is of concern to the client's business interests and provide comprehensive reports.

The Value of our Cyber Intelligence Services

- Receive first class intelligence around your business interests
- One-time off or recurring options
- Be aware of risks before they turn into serious problems
- Clear web, Deep Web and Dark Web intelligence analysis
- Law enforcement grade reports and evidence, which will be admissible in court

Why Us?

- Combining IT Skills with Investigative Skills from ex-law enforcement staff
- Team of multilingual intelligence Analysts
- Experience across all sectors and business sizes
- Experience in covert operations
- We only use legal methods and open source investigation techniques

Deliverables

- Comprehensive and detailed reports
- Secure encrypted report delivery and destruction of all records upon delivery
- Debrief call to discuss results

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Service 6: Cyber Intelligence for Businesses

We offer an intelligence service to the private sector by proactively monitoring and reporting activity in cyber space, which concerns client's interests. We turn all intelligence into an informational product delivered to the client.

We gather intelligence by use of the following means:

- Technical Cyber feeds incl. Botnets, attack sources, malware, trends etc.
- Observation and Monitoring of underground hacking groups / chat rooms
- Monitoring Information on the Dark/Deep Web relevant to the client
- Activity monitoring on Social Media concerning client's interests
- Intentional and unintentional client information disclosure online
- Information gathering on groups / individual posing a potential risk

Deliverables
We offer the following packages to suit the client's needs:

- 1 report per year or one time off
- 2 reports per year (biannually reporting) whilst gathering Intel monthly
- 4 reports per year (quarterly reporting) whilst gathering Intel monthly

Should we encounter imminent threats, we will inform the customer immediately. All intelligence reports contain recommendations on how to mitigate threats encountered and provide detailed information on threat sources for potential legal action and law enforcement involvement against the individual(s) / group(s) posing a risk.

Example Threats we report on can include:

- Confidential and Secret information hacked and leaked by criminals on the dark web such as Usernames, Passwords, Logins, SQL database dumps, confidential documents and more.
- Hacking groups discussing attacks or potential attacks against our clients.
- Misconduct and information disclosure by disgruntled employees or ex-employees.
- Reputational damage done to our client's interests
- Anything else concerning security around client's interests

We are a Private Intelligence Service which delivers Intel to clients in the same manner a state intelligence agency provides information to the government concerning national interests.

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849

Service 7: Individual Cyber Intelligence

We use our extensive Cyber knowledge, extensive network and sophisticated tools in order to investigate, correlate and report on information needed by clients. Our investigation services are offered on a global basis in most languages. We have recognized the increased reliance on computer and other electronic devices and understand the value of capturing a digital footprint when conducting any form of investigation.

Our OSINT Services can contain any of the following modules:

- Tracking, Locating Individuals and missing person cases
- IP address / Email Tracing / Domain Ownership investigations
- Intellectual Property and Brand Protection investigations
- Locating Witnesses and Defendants
- Background Checks of any kind incl. Social Media Investigations
- Criminal Record Investigations / Credit investigations
- Online scams (Dating, Romance, Marriage Fraud etc.)
- ID Theft investigations
- Identity Verification and Surveillance
- Online reputation management / Defamation / Harassment Investigations
- Internet and Forensic Investigations
- Pretext Inquiries and covert undercover investigations

Sample cases we have recently worked on:

- Identifying radicalized individuals working at company X
- Identifying person and location of a criminal selling stolen goods online
- Numerous Background checks on potential investors and business partners
- Identifying whereabouts of husband refusing to pay childcare support
- Identifying a stalker making death threats online to a specific individual
- OSINT evidence of an employee doing harm to the company he worked for
- Locating a UK national who emigrated to Canada in the 80s

Our excellent team of IT specialists, ex law enforcement and private investigators allows us to combine our skill set to provide excellent investigative results in order to meet our client's needs.

Cyber 51 LLC
1546 NW 56th Street #384, Seattle, WA 98107, USA
Email: info@c51.io - Web: www.c51.io - Phone: +1 (206)-965-9849