ASCOTBARCLAY™

www.ascotbarclay.com
info@ascotbarclay.com

VULNERABILITY ASSESSMENT

JUST HOW EASY A CYBER TARGET FOR THE MOTIVATED AND PROFESSIONAL ADVERSARY IS YOUR ORGANISATION?

Ascot Barclays Evolution Threat Monitor provides an Adversarial Assessment using OPENSOURCE INTELIGENCE (OSINT) sensors on the dark web to seek out and capture potentially exploitable information about your organisation.

For organisation's seeking a real-world view of what information malicious actors can find about them on the open and dark web. Our data collection spans seven years in most languages covering the most important sources to discover when your company's information is leaked online, bad guys are talking about attacking you, or exploit code is being developed that can compromise your infrastructure.

We cover over 750,000 data sources from the deep and dark web, underground forums, to social media.

Unlike "boiler rooms" of human analysts working manually, our service automatically collects and analyses intelligence from technical, open, and dark web sources. We deliver radically more context than threat feeds alone, updates in real time so intelligence stays relevant, and packages information ready for human analysis or instant integration with your existing security stack.

Our adversary assessment report provides insight and mitigation recommendations into the following:

- Leaked credentials
- Negative sentiment company chatter
- Repository code and files exposed
- Exposed company web servers and databases
- Insecure infrastru cture
- Deep & Dark web markets where company sensitive information is traded
- Mentions of company IP's, Domains, or Files

IF YOU ARE CONCERNED OR CURIOUS ABOUT THE INFORMATION AVAILABLE IN THE DEEP WEB, UNDERGROUND SITES AND IN HACKER FORUMS THEN DO GET IN TOUCH AS PREVENTING SECURITY BREACHES IS WHAT WE DO.

SMALL BUSINESS AWARDS 2016 CV MAGAZINE

winner
Cyber Security Awards

TESTING, AUDIT AND MANAGED SERVICES IN OUR SERVICE PORTFOLIO INCLUDE:

AUDITING

- Secure Source Code Auditing
- OAuth/API Testing
- Social Engineering Assessment
- Digital Signature Audit
- Secure Architecture Review

CMS SECURITY

- Wordpress Security
- Magento Security

PENETRATION TESTING

- Web Application Testing
- Cloud Application Testing
- Mobile Application Testing
- Network Penetration Testing
- VoIP Penetration Testing

COMPLIANCE

- PCI DSS Security Auditing
- ISO 27001 Security Auditing
- GDPR

MANAGED SECURITY

- Vulnerability Assessment (VAPT)
- Firewall Auditing
- Data Security
- Application Security
- Website Malware Removal

DEVICE SECURITY

- IoT Security
- BYOD Security

A FOCUS ON CLOUD APPLICATION PENETRATION TESTING

Cloud is the preferred solution for data storage, infrastructure and services on demand today. Most enterprises migrate to the Cloud following different models as alternatives; Public, Private or Hybrid and also service models of choice SaaS, IaaS or PaaS.

The vulnerabilities faced by the data stored on the Cloud or applications hosted there are self-explanatory, justifying the increasing importance of the Penetration Testing of Cloud based applications, services and infrastructure. With an increasing number of enterprises migrating to the Cloud, the chances of breaches, threats and vulnerabilities increase day by day. Enterprises face unique challenges in protecting their resources over the various models of the Cloud.

Cloud Applications Penetration testing comes with a unique challenge. The test strategy changes if the testing is to be done for the Cloud Service Provider versus the Tenant. Since a Cloud is essentially a multi-tenant model; when the Cloud testing needs to be done for a particular tenant, it should avoid putting others at unease and also be conducted within the legal limits.

A meticulous Cloud Pen test would be a combination of using internal as well as external Pen Tests. An internal pen test accesses the servers and hosts in the Cloud, initiating a vulnerability test with the authenticated credentials. Once inside the perimeter, the Pen Tests stimulate what a hacker could. Security in the Cloud requires a well thought of strategy with continuous vigil and surveillance.

SERVICES FOR CLOUD APPLICATION PENETRATION TESTING

Combination of penetration tests for testing in the Cloud

- Saas Pen test
- IaaS and Paas Pen test
- Internal Pen test
- External Pen test

Multi Cloud Security Solutions & Specialised solutions for Cloud based deployments

- Data Protection
- User Access Management
- Cloud Visibility and Discrepancy Detections

Niche Hybrid Cloud security testing encompassing

- On-Premise Solutions
- Cloud based Solutions

WE DON'T DO PARANOID WE DO FACTS. Because there is real comfort in knowing just how targeted you have been, targetable you are now and the simple steps you can take to HACKER HARDENED™ status from today. Please reach out to our team on +44 (0) 203 697 1364 for a confidential discussion in the first instance. We look forward to hearing from you.

ASCOTBARCLAY™

71-75 Shelton Street,
Covent Garden
London, UK, WC2H 9JQ

+44 (0)20 3897 2249
info@ascotbarclay.com
www.ascotbarclay.com