BEETLES
THE HACKER'S APPROACH

Beetles Cyber Security Limited

Aziz Bhaban
93 Motijheel C/A (3rd Fl.)
Dhaka-1000, Bangladesh

+8802-9513744
query@beetles.io
www.beetles.io

Company Profile

Primary Company Details	
Company Name:	**Beetles Cyber Security Ltd**
Trade License Number:	02069666
TIN:	772205665647
Company Type:	Private Limited

Secondary Company Details	
Year Founded:	2017
Incorporated in:	Dhaka, Bangladesh
Type of Business:	InfoSec Services

Number of Employees	
Developers / Programmers	03
UI/UX Developers	02
Infrastructure Management	02
Security Operations Researchers / Analysts (in-house)	08
Business Development Team	05
Finance and Accounts	02
Total Employees	**24**

Company Address and Communication	
Address:	Aziz Bhaban, 93 Motijheel C/A (3rd Floor), Dhaka - 1000, Bangladesh.
Phone:	8802- 9558998; 880- 9611688226
E-mail:	info@beetles.io
Web:	www.beetles.io

Business Description

Beetles – The Hacker's Approach has been created teaming up with some of the best young minds in the field of Cyber Security, hosting services such as, among others:

- ✓ Cyber Security Consultancy
- ✓ Vulnerability Assessment
- ✓ Penetration Testing
- ✓ Source Code Audit
- ✓ Mobility Security
- ✓ Forensics – IoA, IoC
- ✓ Malware Analysis
- ✓ Managed Security Services

Beetles is a crowdsourced penetration testing platform designed to build a trusted, hacker-centric approach to protecting an organization's digital attack surface.

Mission & Vision

Mission - At Beetles, our mission is to enhance the business operations of it's clients by implementing premium Cyber Security practices with state-of-the-art technologies and services.

Vision - Beetles aims to be a global leader in state-of-the-art cyber security solutions, helping individuals and innovative companies to functions in a more secure and stable environment.

Resources and Strengths

Led by a dynamic team with a wide array of experience, both internationally and domestically, The Beetles Red Team provides on-site and off-site, 24.7.365 service, committed to securing the client's web facing and network assets.

Even though Beetles is new concept in terms of Bangladesh, this practice is widely accepted and incorporated in the daily lives of businesses all over the modern world. We have found that some of the researchers working for top security firms such as **Synack, Cobalt, HackerOne, Bugcrowd** etc., are Bangladeshi young men and women. We have successfully managed to incorporate these talents into our Beetles program, as we all share a common vision, to develop the IT Security sector in Bangladesh and to raise awareness on the possible dangers of the dark web. Our selected researchers and analysts are all incorporated in some of the Fortune 500 companies', such as **Google, Microsoft, Facebook, EBay, Twitter, Slack, PayPal** hall of fame as well as previously working freelance for some of the top ranked security firms abroad. Even then, we have a tough initiation process where the applicant has to go through a written and practical exam where we assess them thoroughly and do due diligence checks before incorporating them into the Beetles team. All our researchers are under strict Non-Disclosure Agreement Contracts, in accordance with the laws of The Government of the People's Republic of Bangladesh.

Our team is kept up-to-date with extensive training on the latest technology advances, security adversaries and required skills.

Industry Information

The Internet is infinite, but still growing every day. It has given rise to new opportunities in every field imaginable, be it business, entertainment, education or otherwise. Our entire lives have been neatly packaged and upload in a digital version of ourselves. All our personal data, our friends and families, our likes and dislikes, even our financial history and current data are stored in invisible packets in the vast openness of the world-wide web. For our own ease of access, we have digitalized our entire businesses, where we prefer to store even the most sensitive information in these packets, all our trade secrets, our financial data, our vulnerabilities and our opportunities.

The internet has been a boon and an inseparable partner in our modern lives, but it has its own disadvantages as well. Criminals are now faceless and seemingly traceless. The bigger weapon now is not a gun, but a keyboard. From malicious codes to Trojans to phishing and organized crimes (data theft, DoS, DDoS) are the new threats we face every day. The new criminal hides in the Deep Web, without a face or a name, waiting, only but a keystroke away.

Forbes estimated the size of the cyber security market to be at USD 77 billion at the end of 2015 with a projected growth to USD 170 billion by 2020. The market is potentially huge and growing every day. At the end of 2015, it was estimated by both PwC and Forbes that cybercrime is costing the business USD 400 to USD 500 million annually, and that estimate excludes the large number of unreported crimes. Banking and Financial Services industry is the fastest growing non-government cyber security market, as they are the first targets of persons with hostile intentions.

TrustWave's 2015 Global Security Report found that 98% of tested web applications, from online payment gateways to e-commerce sites, were vulnerable to attacks and PwC claims, in their Global State of Information Security Survey, that 75% of directors in major firms and banks are not actively involved in reviewing security and privacy risks.

The threat is very real and the danger of coming under attack is imminent. Beetles has been created with the sole purpose of warding off these criminals, safeguarding the clients' data, both personal and professional from such attacks, ensuring that no Revenue Impact or Business Impact befall the client. Carefully selected and rigorously vetted researchers from our global resource pool make up the Beetles Red Team and they have been structured and molded in such a fashion, always vigilant, always protecting. They are strong, versatile and sharp, like the tip of a dagger!

Services Overview

Automated security scanners do not get the job done thoroughly. As applications become more complex day by day, we find that human intervention becomes increasingly mandatory. Vulnerabilities require pure business logic and human ingenuity to detect. After all, there is no substitute for the human mind.

A vulnerability assessment and penetration test is a comprehensive test of physical weaknesses in computers and networks as well as word practices and procedures. It identifies potential weaknesses, risks, threats and exposure and defines strategies for dealing with them.

Our services:

- ✓ Cyber Security Consultancy
- ✓ Vulnerability Assessment
- ✓ Penetration Testing
- ✓ Source Code Audit
- ✓ Mobility Security
- ✓ Forensics – IoA, IoC
- ✓ Malware Analysis
- ✓ Managed Security Services

Cyber Security Consulting:

We have a dedicated team of security consultants to support your organization. As regular practitioners, the consultants are able to assess your business needs and determine the most effective way of securing your information and reducing the risks affecting your organization. We provide consultancy in the following areas:

People: Cyber Security is not only about firewalls and passwords. It includes people, security training, policies and processes are vital to ensuring that the technology solutions are enabled to work to their full potential.

Processes: The team, with their experience and accreditation, can help you reduce disruption to your business.

Technology: Technology is what we do best. The team will refer your business to your proprietary Beetles Platform, where we can initiate a deep-dive into your systems and applications, in what we call **"The Hacker's Approach".**

We have experts across a wide range of domains, from risk assessment and mitigation, disaster recovery and cryptography, to IT security and infrastructure solutions.

Source Code Audit:

A software code audit is a comprehensive analysis of source code in a programming project with the intent of discovering bugs, security breaches or violations of programming conventions. During a Source Code Security Audit, experts manually inspect the source code of your new or existing application on a line-by-line basis, for security weaknesses, review authentication, authorization, session and communication mechanisms. They will identify issues that could result in unauthorized access or leaking of sensitive information. The audit can be done immediately post-deployment but we recommend that you incorporate us in your SDLC for a better and secured development process.

Vulnerability Assessment:

This is an off-site, non-exploitative test of individual Internet Protocol addresses or nodes owned or controlled by your organization. To perform this test, you must designate the IP addresses you want tested. This is usually done with automatic scanners.

External Penetration Test:

This test will actually exploit the vulnerabilities to determine what information is actually exposed to the outside world. It mimics what an outside hacker would do to exploit weaknesses in the application's security without the usual dangers. It also identifies weaknesses in the external IT systems that could be used to disrupt the confidentiality, availability or integrity of the network, thereby allowing your organization to fix them. Our methods for this test includes:

a. Public and private information leakage
b. DNS Analysis and Brute-forcing
c. Services Probing
d. Exploit Research
e. Manual Vulnerability Testing and Verification
f. Intrusion Detection and Prevention System Testing
g. Password Service Strength Testing

h. Remediation Re-testing (optional and add-on)

Internal Penetration Test:

This is an exploitive test to determine what vulnerabilities are present behind the firewall. It identifies weaknesses in the internal IT systems. Our methods for this test includes:

a. Internal Network Scanning
b. Port Scanning
c. Services Probing
d. Exploit Research
e. Manual Vulnerability Assessment and Verification
f. Limited Applications Layer Testing
g. Firewall and ACL Testing
h. Privilege Escalation Testing
i. Password strength testing
j. Network Equipment Security Control Testing

Holistic Audit:

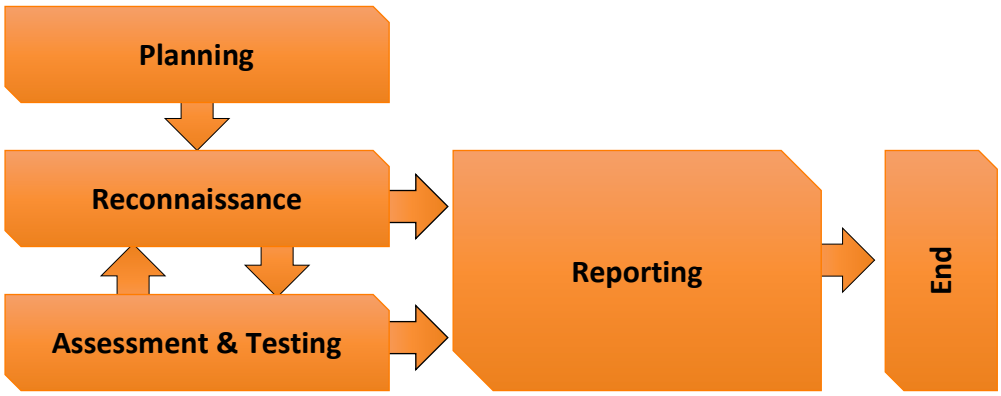
Our holistic audit goes beyond the immediate cyber domain to deliver a complete 360-degree security assessment of your business, including human and environmental factors. It will provide you a comprehensive report detailing vulnerabilities across your organization as a complete entity and make wide ranging recommendations to address these. We will help you understand the current status of your information security across the entirety of your business, thus allowing you to make informed business decisions.

Our Methodology

As each application is unique, the testing methodology needs to be customized and tailor-fit and will therefore vary from one to the next. But the objective of the test would remain the same, and that is to resist the intrusion from an outsider or from within the network.

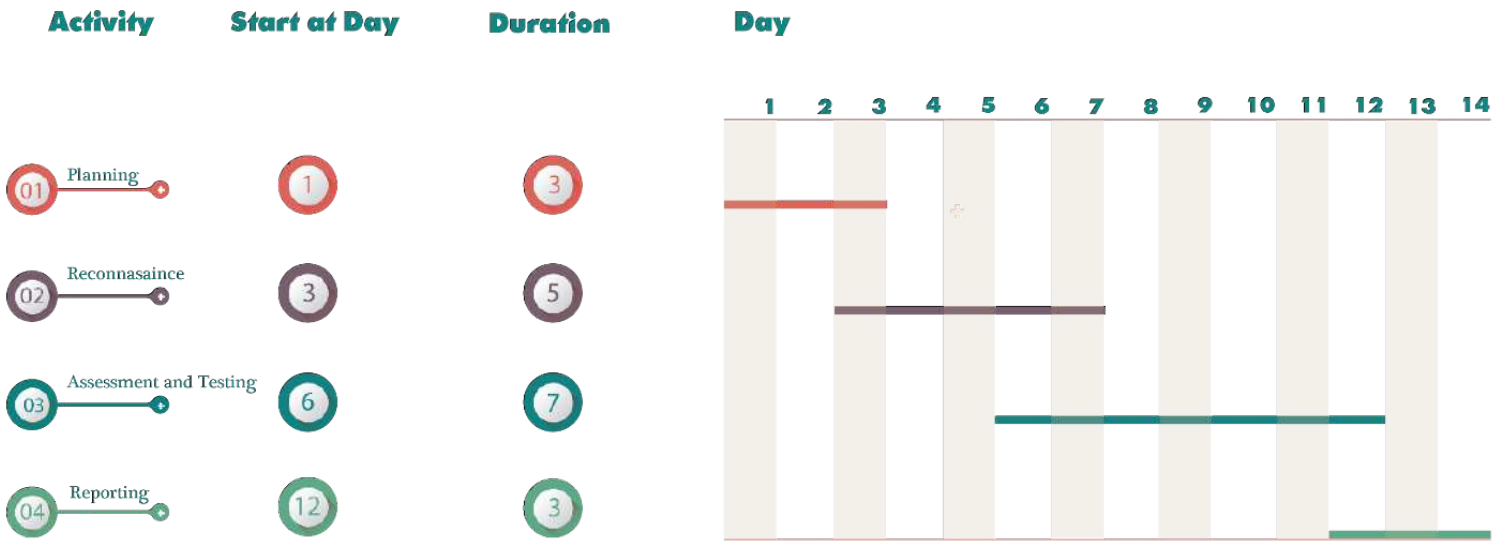
We will assign at least one member of the Beetles Red Team along with an accredited Bug Bounty Hunter and a CISSP / CISA certified moderator in an attempt to gain access into the system. The initial test would be executed via "The Hacker's Approach" in an attempt to breach the target, i.e., Blackbox. The secondary test would be run as an authorized user account, with greater application visibility, in order to breach from within, i.e., Whitebox.

The figure below illustrates our approach to attacking a network:



Testing Timeline

Our layer 1, layer 2 and layer 3 external penetration tests are conducted within a timeboxed, fourteen (14) day, sprint. We find that this is the optimal time needed to successfully and completely run a testing cycle. Our timebox is divided into four (4) phases as shown in the following illustration:

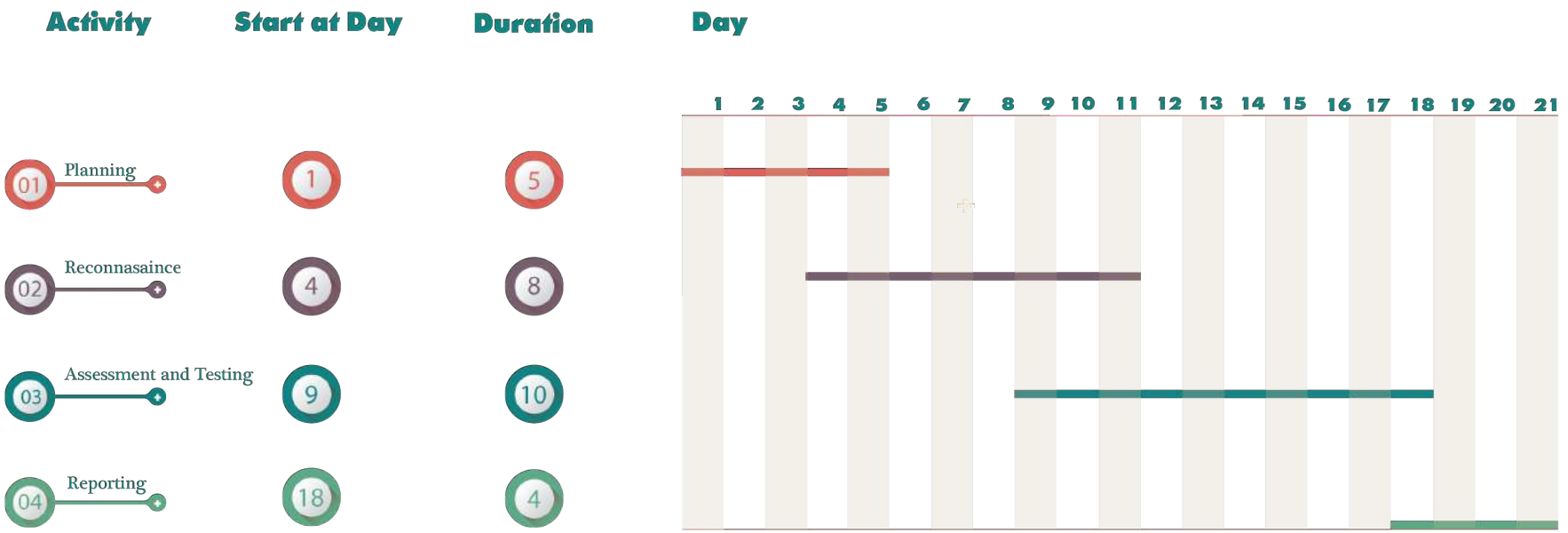


+8802-9513744
query@beetles.io
www.beetles.io

Aziz Bhaban
93 Motijheel C/A (3rd Fl.)
Dhaka-1000, Bangladesh

Beetles Cyber Security Limited

Our network system penetration tests and server configuration reviews are conducted within a timeboxed, twenty-one (21) day, sprint. We find that this is the optimal time needed to successfully and completely run a testing cycle. Our timebox is divided into four (4) phases as shown in the following illustration:



+8802-9513744
query@beetles.io
www.beetles.io

Aziz Bhaban
93 Motijheel C/A (3rd Fl.)
Dhaka-1000, Bangladesh

Beetles Cyber Security Limited

The Onion Skin Approach

We recommend an in-depth and comprehensive testing of an entire network structure, especially if that network hasn't been security testing in a while. A comprehensive takes a four-layer approach, where our specialized Red Team would start that the outside and would gradually make their way into the core or the network, peeling off one layer of security at a time, as the following illustration demonstrate:

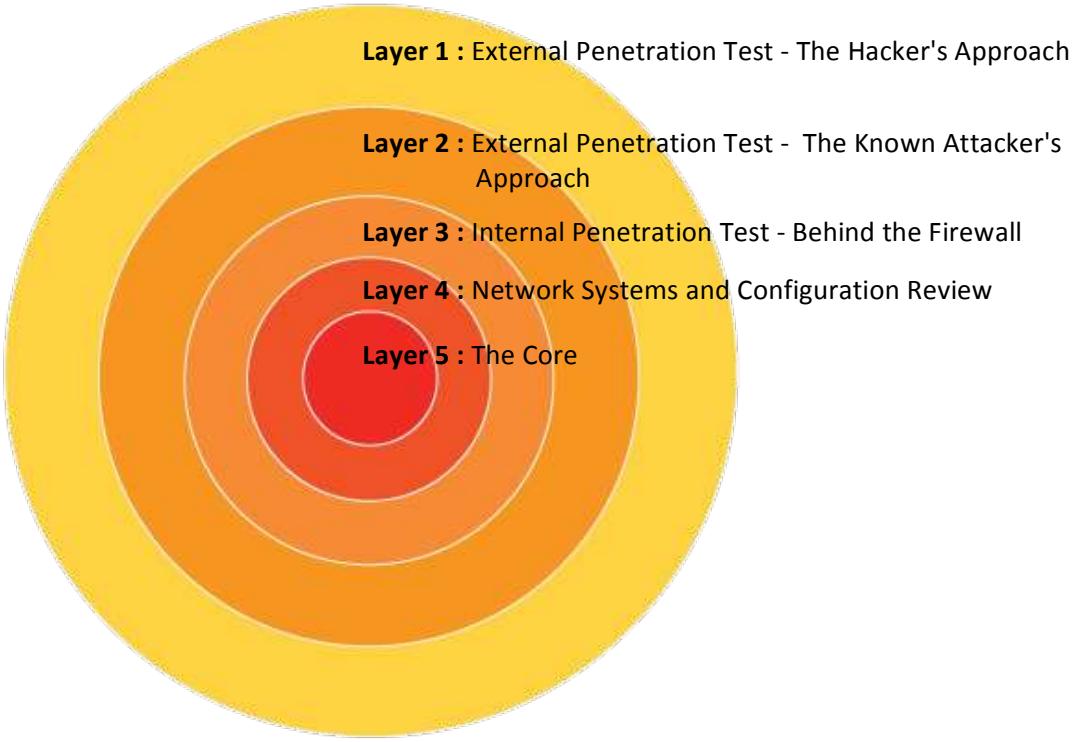


Fig: The Onion Skin Approach

The Beetles Red Team

SHAHEE MIRZA	**Information Security Professional with concentration on Penetration Testing of Web and Network Applications.**
Experience	08 (Eight) years of experience of working as a security analyst and system security engineer on multiple leading organizations.
Skills	• Penetration testing • Vulnerability assessment • Network designing • Network engineering • Network security engineering
Certifications and Credentials	• Certified Ethical Hacker (CEH). • eLearnSecurity Penetration Testing hands on training. • Operational Security (OPSEC) for Control Systems from ICS-CERT, NCCIC & U.S DHS. • Cyber security for Industrial Control Systems from ICS-CERT, NCCIC & U.S DHS. • Cisco CCNA Security Course from Charles Sturt University (CSU | IT Masters). • Maintaining Cyber Security Course from DeVry University • Microsoft® Certified Systems Administrator (MCSA). • Microsoft® Certified Professional (MCP). • Cisco Certified Network Associate (CCNA Course Completed). Acknowledged by 100+ fortune five hundred companies for security infringement reporting which includes but not limited to: • Facebook • Google • Microsoft • Twitter • Yahoo • Github • Sony • Mozilla • Blackberry

MD NAHIDUL KIBRIA	**Information Security Professional with concentration on Penetration Testing of Network & cyber forensics.**
Experience	• 03 years of experience of working as a red team member in Synack, which is a private network of highly curated and vetted security researchers, founded by ex NSA officials. • 10 years of experience as a software architect and security professional.
Skills	• Secure Code Review • WIN32 exploit development • Network Security Hardening • Configuration Audit • Malware Analysis • Cyber Forensics • System level security auditing
Certifications and Credentials	Co-leader of OWASP Bangladesh Chapter Contributed to OWASP (www.owasp.org). The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. As a part of OWASP some public talks are: • Sending a for ahuh. Win32 exploit development. • Malware: Zeus zombies are being used in online banking theft. • Everybody loves HTML5, hackers too

MD TAREK SIDDIKI	**Information Security Professional with concentration on Penetration Testing of Web Applications.**
Experience	05 years of experience as a security researcher and code auditor. 02 years of experience as a red team member in Synack. Which is a private network of highly curated and vetted security researchers, founded by ex NSA officials. 01 years with Cobalt, which is another private network of highly curated and vetted security researchers.
Skills	Web application Penetration testing API testing in security perspective Secure Code Auditing Vulnerability Assessment
Certifications and Credentials	Acknowledged by 100+ fortune five hundred companies for security infringement reporting which includes but not limited to: • Facebook • Google • Microsoft • Twitter • Yahoo • Apple • Barracuda Ranked 11th on Synack Red Team's worldwide ranking. Ranked 11th on Hackerone's Researchers Worldwide leaderboard (2015 Q1) Ranked 61st on Hackerone's all time researchers ranking. Advisory Board Member at Hacken.io

Frequently Asked Questions

Automated scan or manual pentesting?

An automated scan is done using one of the many automated security scanning utilities available to identify vulnerabilities on a wide range of systems in the shortest possible time. It will only test for the most common and well-known vulnerabilities and if the vulnerability does not exist in the database, the scanner will miss it, giving the user a false sense of security. An automated scan is fast, cheap but not accurate.

Manual pentesting is done by leveraging the intelligence, ingenuity and experience of a seasoned, professional security researcher. The security researcher uses their knowledge and experience to manually identify and remove the false positives and to find the false negatives.

An automated scanner cannot think, cannot predict, cannot evolve along with the adversary in an active threat situation and therefore cannot be truly secure; it needs to be combined with the adaptability, creativity and power of the human mind for an optimal security scenario.

A true penetration testing is in taking “The Hacker’s Approach!”

What is the difference between the types of services?

In many scenarios, the terms “vulnerability assessment” and “penetration testing” may be used interchangeably. But we refer to the vulnerability assessment as being non-exploitable; meaning we will report on detected vulnerabilities but will not attempt to actively exploit these findings. But in an external penetration test we will conduct a more thorough, in-depth test that will seek to actively exploit detected vulnerabilities in order to compromise, or set up a scenario where we demonstrate to compromise, your systems and assets just like an outside hacker or attacker would. In an internal penetration test, we will focus on testing devices found behind the firewall or located so that they are not directly internet facing.

What tools do we use?

Our vulnerability assessments and penetration tests are mostly conducted manually because we believe that there is no substitute for the human mind. But even then, we do need the help of some tools to conduct the test more efficiently and thoroughly. Some of the tools that we use are Metaspoilt, Retina, Burp Suite, NMap etc. But the tool selected for your engagement may vary based on our perception of the appropriate tool necessary to properly assess your requirement and application.

What is required to perform a remote test and how will you attach to my network?

We will consult with your administrative and technical personnel to determine the most effective manner in which to perform the internal vulnerability assessment. Generally, your test can be performed through allowing Beetles a temporary Virtual Private Network (VPN) connection to our internal network. We will make sure that you enable necessary logging and implement practices to ensure our administrative and VPN privileges are disabled after the completion of our testing.

Who will perform the tests?

Your tests will be conducted by our Beetles Red Team, consisting of highly vetted and carefully selected researchers from our global resource pool. All our researchers are regularly evaluated based on their work and client reviews. They are subject to extensive background checks and have confidentiality and non-disclosure agreements with our firm.

What is the time frame for performing a vulnerability test?

We can perform your penetration testing in two to three weeks, in general, after we receive the official work order. If you require an expedited test, we can customize a schedule for you.

How will I receive the finding from the vulnerability assessment?

We issue a formal report for all our review services. This report will include an overview of the findings from our test as well as any recommendations regarding remediation. You will be invited to join our proprietary Beetles – The Hacker's Approach Platform, where you will be kept updated on the current status of your test as well as have access to all your results. Our researcher's every action and movement will be logged and you will be able to monitor our work in real-time. You will receive formal reports of our review services here and the report will include the details of the findings from the test as well as any recommendations regarding remediation. You will also be able to download a PDF copy of your report, if you wish to do so.

Beetles Cyber Security Ltd.

Aziz Bhaban
93, Mothijheel C/A (3rd Floor)
Dhaka-1000, Bangladesh

+88 02-9513744
query@beetles.io
www.beetles.io

A Concern Of Big Web Technologies Ltd.