



BEEETLES

THE HACKER'S APPROACH



INFORMATION SECURITY MANAGEMENT SYSTEMS



ISO/IEC 27001-2013

SAFETY Password
Protection likes
Security Code dislikes
financial history friends
PERSONAL DATA
Data INFORMATION
Information Data Privacy
PRIVACY Security
SAFETY Protection
Password
FRIENDS AND FAMILIES
financial history
SECURITY Data Code
Protection information
likes and dislikes
PROTECTION SAFETY families
Information protection
Information

Preface


The internet is infinite, but still growing every day. It has given rise to new opportunities in every field imaginable, be it business, education, entertainment or otherwise. Our entire lives have been neatly packaged and uploaded in a digital version of ourselves. All our personal data, our friends and family, our likes and dislikes, even our personal 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 digitized our entire businesses, where we prefer to store even the most sensitive information in these packets, all our trade secrets, our finances, our weaknesses, and our strengths.

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 no longer a GUN, but a KEYBOARD.** From malicious codes to Trojans to phishing and organized crimes (data theft, DoS, DDoS, etc.) 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.

As threats are increasing, the danger of coming under attack is imminent. BEETLES has been created with the sole purpose of warding off these criminals, safeguarding clients' data, be it personal or 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 way that they are always vigilant, always protecting. **They are strong, versatile and sharp, like the tip of a dagger!**

BEETLES Cyber Security was founded by hackers and security enthusiasts, driven by the need to create a pen-testing platform and to help enhance the IT security industry in Bangladesh. Through our CrwodSpark platform, we have set the industry baseline for hacker-powered security. With our growing resource pool within the global hacker community, we strive to identify the most relevant and prevailing security vulnerabilities of our clients, before the criminal can exploit them.






**We provide you with a
hacker's point-of-view
in securing your
systems.**

Our PenTesting Engagements are
customizable to fit your budget.

**You focus on your business;
we'll take care of your security!**



Why is cyber security important?

It wasn't that long ago that Cyber Security was just something that the IT department worried about. Corporate leaders and organizational owners delegated the task to their IT departments and as long as they had the right firewalls, anti-virus software, and other tools in place, they could simply leave security matters to their IT experts and focus on the other integral elements of running their businesses. Wrongly, it seems, in retrospect.



/// Cyber Security is not something // that anybody can afford to ignore

Over the past few years, there has been a drastic change in the IT forefront. More and more companies are adopting technology and web services to enforce business needs and enhance growth. We now live in a connected world, where every single element in our IT environment interacts with each other and the cloud. This grants us the ease of access to our data, makes our lives better and keeps our customers happy. But this comes with the price of added security risks to our everyday lives.

Threats can occur at any point in the internet.

There is always a potential weakness that malicious hackers can exploit. As our usage of and dependency on the internet grows, so do the potential for attacks and breaches. Then there are the compliance issues. International and local regulators, enforce compliance frameworks such as **PCI DSS, ICT Guideline, GDPR, HIPAA**, etc.

The cost of a breach

It is an established fact that cyberattacks and data breaches are extremely costly for businesses to endure, both in terms of business capital and reputation. Juniper Research estimates that the 2019 cybercrime cost will be upwards of **USD 2 Trillion, with the collective financial cost expected to more than double to USD 5 Trillion in 2020**, according to Cyber Defense Magazine. But Deloitte suggests that these numbers are small in comparison to the real costs imposed by the harder-to-quantify factors such as **reputational harm, loss of market share, loss of customer trust**, etc. These 'hidden' costs run to 90 percent of the total business impact and aren't typically felt until two years or more after the event, according to "Beneath the Surface of a Cyberattack, a Deloitte Advisory".

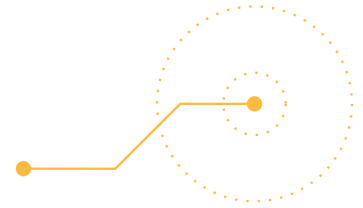
Alongside the obvious financial damages, such an attack could also result in disrupting or harming our personal lives, careers as well as business relationships.

Since almost every business and organization nowadays has a website and has multiple systems or applications exposed, this provides criminals with potential entry points into internal networks. **Criminals are highly skilled, motivated, funded and even coordinated.** A successful breach on a high-value target has a potentially large yield. Alongside this, the availability of various hacking tools on the internet encourages less skilled hackers and script-kiddies to launch damaging attacks against businesses such as ransomware, etc.

With such attacks becoming extensively common nowadays, businesses need to accept that it's only a matter of 'when' that they are breached. They need to be proactive in their security, implement controls, test them accordingly and take proactive security measures that allow them to deter, detect and respond to such malicious attacks.

Increasingly sophisticated hackers with widely available hacking tools.





How do you get started? What do you need?

Spend wisely!



KNOW THYSELF,

learn about the threats which are most likely to befall your business specifically. Cyber Security is a broad term, and it's just not possible to spend limitlessly. After carefully analyzing the key areas of your business, people, process and technology, our team of security experts will advise you about which approach is the safest and which approach is the most cost-effective. Consequently, you will not have to worry about spending too much or too little on your security with the help of our cyber security consultancy experts.

People



Firewalls, security solutions, and network security devices are all well and good, but the main threat of a security breach lies within the human factor of your organization itself. People **misplace their passwords, connect to unsecured networks, share credentials and delegate control**, all the while being negligent about their important data. We help them by empowering them with the proper knowledge, helping construct strong policies and governance and increase general awareness so that chances of a breach are reduced.

Process

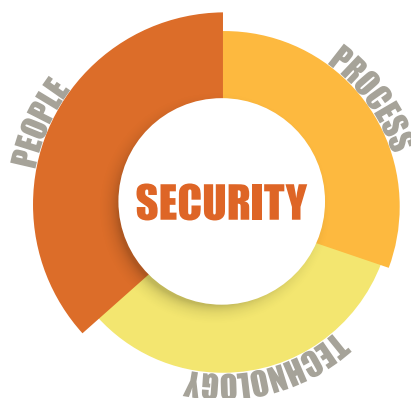


The next step is consulting about the processes of your business that are electronically integrated to limit your exposure and reduce your risk position.

Technology



You may need to implement a few security solutions to aid your security team in protecting your assets. How best do you understand what solution is needed? How do you ensure that the solution you buy is the right one or the one you need? Our consultants will dive deep into your current network architecture and layout a plan for the future, while we advise you on the best solutions that you can deploy, within your budget.



Assess your current risk position and likelihood of an attack.

Vulnerability Assessment is defining, identifying and classifying any security gaps or breaches in devices and infrastructures, as well as forecasting the effectiveness of proposed countermeasures and evaluating their actual effectiveness after they deployed.

This is an automated, non-exploitive (does not breach your systems) test. Performed on individual IP addresses or nodes owned by your organization, this test provides you with the necessary knowledge and risk posture to understand the threats to your IT environment and to take appropriate measures.



What is pentesting?

A penetration test, or a pentest in short, is **an attack simulation against your IT environment**, applications or networks, to check for vulnerabilities that could be exploited by any malicious attacker. It works to secure IT security's three main pillars, **Confidentiality, Integrity, Availability** (CIA Triad). Insights provided by the penetration test will enable you to patch existing vulnerabilities, define your security policies and align security measures against business goals.

A hacker-powered penetration testing engagement is a **knowledge-based, manual approach** to the traditional tool based pentests and it relies on **human expertise, experience, and skills**, on top of the professional software and automated tools. Even though automated tools are great at discovering vulnerabilities up to a certain level, **they are unable to detect design and business logic flaws**, which is why a manual pentest by a skilled hacker provides complete and in-depth coverage that is only possible by **leveraging the power of the**

human mind. **Threats to businesses are increasing.** Day by day, criminals are becoming more and more determined and sophisticated. This is why most companies or institutions you work with may demand that you have a proactive approach to securing your applications from the start. The goal of the pentesting exercise is to **identify existing and new vulnerabilities, meeting with compliance regulatory requirements, test your Incident Response capabilities** and generally improve employee awareness.

Security is expensive, or so they said

With a crowdsourced, hacker-powered pentesting-as-a-service, you can maintain your security with the same on-demand elasticity as any SaaS, and that too within your budget.

Benefits of an independent, external pentesting?

- Avoid **potential conflict of interest** and/or biases that internal security teams have from testing the same application continuously.
- External pentesters can **view the target with fresh eyes and employ customized and curated methodologies** that results in better quality and coverage.

Benefits of Hacker-Powered Testing

- On-Demand: Pentesters are **always available and ready** to go at any time.
- Scalability: Engage as many hackers with just as many **varied skillsets and diverse experiences to your program.**

Different type of Pentesting Engagements

BEETLES' curated penetration testing services are segmented into 4 different engagement types:

Point-in-Time: A point-in-time security testing is a timeboxed, specific scope defined penetration test of your application and assets. A point-in-time penetration test is done within specific dates, on a specific build, which can be used as a version control to ensure which version of the application has been pentested and secured. There are many strategies for conducting a point-in-pentest, it can be performed as a full disclosure test, in which case, the client's IT and Security teams are notified of the engagement and staging servers are set up and credentials provided. It can also be performed as a "blind" pentest, in which case the strategy is to simulate the actions of a real-world hacker and the testing team is provided with little or no information about the client. The team uses publicly available information to gather intel and conduct the pentest.

Pentesting-as-a-Service (PTaaS): Our specially crafted PTaaS model allows you to schedule and initiate your penetration testing engagements through our proprietary platform, CrowdSpark. Our collaborative and data-enriched process makes the third-party penetration testing process easier while increasing visibility. It is powered by our global pool of accredited pentesters and it delivers real-time results that allows you to identify, track and remediate your vulnerabilities swiftly, rather than waiting for the one-time report you would generally get with traditional pentesting.

Code Assisted Pentest: A code assisted pentest takes out the guesswork that pentesters go through when testing. With access to the source code, our pentesters can gain a thorough understanding of your application and thereby enhance the accuracy of the discoveries made during testing. It allows the pentesters to gain a better understanding of the workflows. This is a more efficient and in-depth manner of testing. But do remember, while a code assisted pentest does provide transparency to the target application, it is not a code review.

Red Teaming Exercise: This is where we utilize our "The Hacker's Approach" and emulate an actual hacker's attempt to penetrate you in order to identify the possible point of exploitable vulnerability, to breach your systems and simulate to compromise sensitive data and systems. This multi-layered attack simulation is designed to measure how well your people, processes, networks, and applications can withstand, detect and remediate an attack in a real-world attack scenario.

PCI DSS Compliance Penetration Testing: BEETLES Cyber Security's approach and methodology to penetration testing are fully compliant with all of the PCI DSS requirements for CDE (Cardholder Data Environment) security compliance. Even though there is a lack of understanding of the PCI DSS standards itself, BEETLES' subject matter experts will help and guide you in identifying, validating and remediating identified issues so that you can achieve your PCI DSS compliance easily and effortlessly.



Application Penetration Testing

The application layer is the closest layer to the end-user and therefore it provides hackers with the largest attack surface. Poorly designed or implemented application layer security can lead to performance issues, stability issues, loss of asset, data theft and eventually, loss of customer confidence. This engagement aims to uncover application vulnerabilities and to help ensure the adequacy of the protective measures. We have an established methodology that allows our specialists to iteratively build a knowledge base of systems. We believe this holistic approach is essential as often several seemingly unimportant settings on a few machines can combine to result in serious security exposure.

Network Penetration Testing

The aim of network penetration testing is to emulate an internal and external attack on your critical internal and external IPs and identify any weaknesses which may provide unauthorized access to systems or data. Using minimal initial information, we will build a comprehensive map of your internal and external network and proceed to test, from a hacker's point of view, the security of the hosts within these networks.

Network Device Configuration Review

Network devices are crucial for the operation for any organization and, if compromised, will have a huge impact on the operations of the business, which is immediately quantified in both business and revenue loss. We will conduct a thorough review of the configuration files and all of the devices and ensure that weaknesses are identified and the risk of a security incident, reduced.

API Penetration Testing

API penetration testing is focused on exposing security vulnerabilities on the APIs your business exposes to its users and vendors. BEETLES have an established methodology where we would construct user API calls, using the same documentation you provide your users and use them to identify security issues. API security is crucial to organizational security as they have a similar impact to web applications but requires a different approach and skillset to test thoroughly.

PCI DSS CDE Penetration Test

As defined in the PCI DSS requirements, a penetration test must include entire CDE (Cardholder Data Environment) perimeter and any critical systems that may impact the security of the CDE as well as the environment in scope for PCI-DSS. This included both the external (public-facing attack surface) and the internal perimeter of CDE (LAN-LAN attack surfaces). PCI DSS describes "Critical Systems" as "Security systems, public-facing devices and systems, databases and other systems that store, process or transmit cardholder data." As well as "firewalls, IDS, authentication servers, etc. any assets utilized by privileged users to support and manage CDE. PCI DSS also describes the CDE as "the people, processes, and technology that store, process or transmit cardholder data or sensitive authentication data."



Methodology

All applications are bespoke, therefore, testing will inevitably vary and be tailored to the nature of the application.

All of our testing engagements are done in a 14 to 21-day engagement cycle, where, depending on the number of pentesters you chose to engage, the minimum testing time is 35 man-hours, in a 14-day engagement cycle.

There are five stages to our testing methodology:



BEETLES will kick off the engagement with a **“Planning and Reconnaissance”** meeting. We will sit and consult with your team to assess your environment and technology stack used. We will also consult with you in formulating the Rules of Engagement and the Scope of the engagement. We will create a baseline by assessing whatever else is publicly discoverable and identifying possible attack vectors, for the engagement.

In the **“Discovery and Analysis”** stage, we will use a hybrid approach of manual testing techniques and automated scanning tools to look for possible vulnerabilities in your environment. Based on our findings, we will develop an action plan, considering the attack vectors, and start the engagement.

During **“Exploitation and Verification”** we employ our own **“The Hacker’s Approach”** and proceed to test your environment manually. Most automated scanners have a high percentage of **“false positives”** as well as **“false negatives”** and this is where we vet through them. We leverage the vulnerabilities, exploit them and chain them together until the target is fully compromised.

“Reporting and Consultation” is where we present our findings to you and your team and discuss the issues found so that you can start with implementing the recommended remediation steps, based on a priority of **“Criticality”** basis. This is an interactive process. Individual reports are posted on our CrowdSpark platform, as they are submitted by our pentesters. At the end of the testing timeline, our engagement lead reviews all of the findings and writes up a final summary report which is then submitted to you.

In the last stage of the engagement, **“Implementation and Validation”**, once your team has implemented the remediations to the findings, we will conduct a remediation-implementation-validation test cycle to make sure that they have been implemented correctly. This is crucial to improve the security and quality of the code. When you mark a report as **“re-test”** on our platform, the researcher validates the patch and marks the report as **“Resolved”**.

Throughout the five stages, we want to make sure that this engagement gives your team the confidence and peace of mind that they are implementing secure codes effectively and in accordance with the security industries’ best practices. It is also important to treat a pentest as an on-going process.

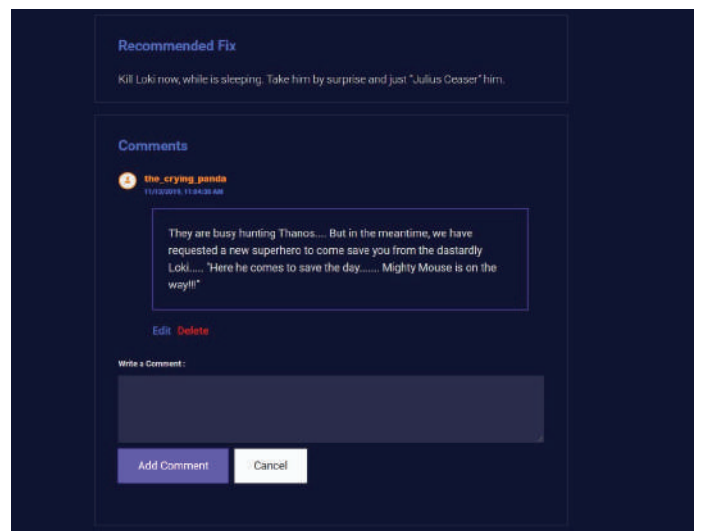
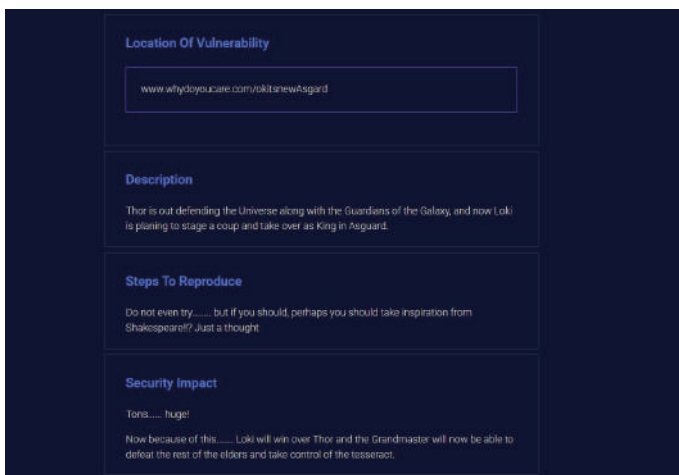
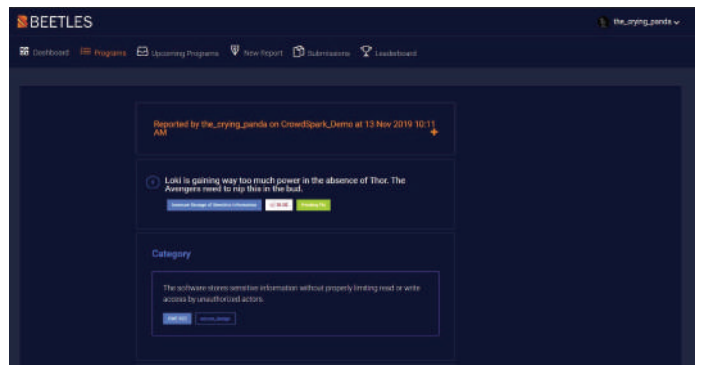
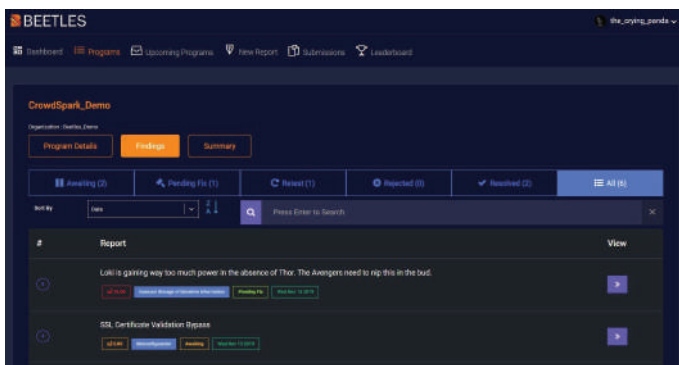
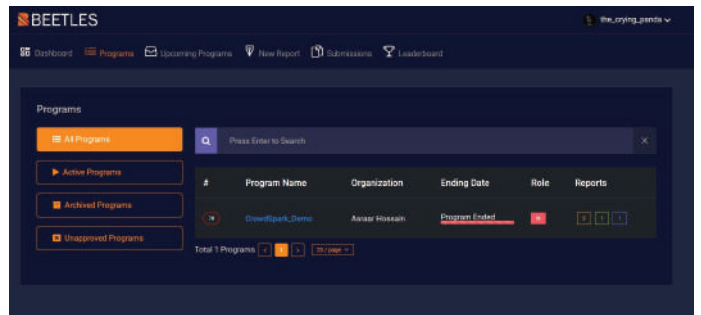
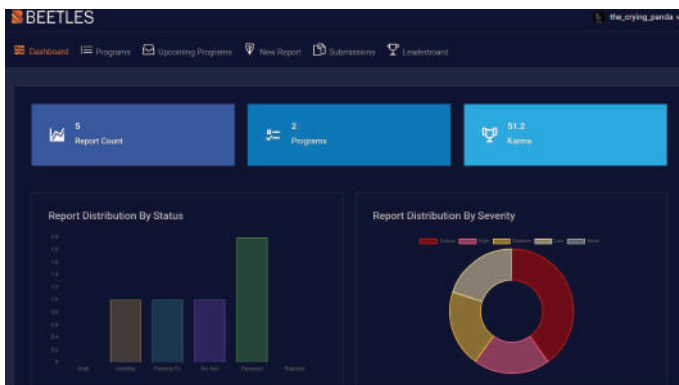
The last phase of the testing cycle should lead into the preparation for the next pentest, whether it’s done in a week, month or year.

The crowdsourced hacker-powered penetration testing platform

The BEETLES Platform, called **CrowdSpark**, is a proprietary engagement management application that provides our clients with a one-stop dashboard for all vital information. It has a number of features that allow our clients the freedom to operate and control their penetration testing engagements with us seamlessly and smoothly. Starting from launching a new on-demand penetration testing engagement to vulnerability tracking and query management to the resolution of an

issue, CrowdSpark is smart, secure and user-friendly, even on-the-go.

Should you have any questions or queries on any vulnerability report, or should you require some clarity or more information, you can post a message on the report and get a response directly from the pentester who discovered and reported the issue. This provides you with an extra layer of clarity for your pentests



Reporting Format

Throughout the whole engagement process, written logs and artifacts are usually kept and periodic reports are generated for the system administrators and the management. At the conclusion of the test, a Report of Findings is developed to describe identified vulnerabilities, a step by step method to reproduce the vulnerabilities found, present a risk rating and provide remediation recommendations for the discovered vulnerabilities.

The Report of Findings includes:

- Executive Summary
- Details of the Findings
- Criticality rating of the findings
- Step to reproduce
- Impact, Business and Financial
- Recommended Fix
- Patch validation retesting

Risk Scoring

Risk is calculated according to the Common Vulnerability Scoring System (CVSS) 2.0 which consists of 3 groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10 and a Vector which is a compressed textual representation that reflects the values used to derive the score. CVSS provides a common language for scoring IT vulnerabilities.

Standards and Guidelines

We adhere to the following standards in our penetration testing methodologies:

- Open Web Application Security Project (OWASP)
- Application Security Verification Standard (ASVS)
- MITRE ATT&CK Guideline
- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Source Intelligence Techniques
- Penetration Testing Execution Standard (PTES)
- PCI DSS Penetration Testing For Compliance



Red Teaming Exercise

Red Teaming is a **full-scope, multi-layered attack simulation** designed to measure how well a company or an institution's people, processes, networks, and applications can withstand an attack from a real-life threat actor.

Any organization's defensive team is known as the Blue Team and they have a very tough job. They are responsible for defending their organization against every single attack, while on the other hand, **the attacker has to only succeed once**. To aid the Blue Team in their relentless efforts, there are some great tools and processes to help them, but the question is, how do you know if that is enough? You don't really, not **until you test it out!** This is where the Red Team comes in.

The Red Team, in our case, the BEETLES Red Team (BRT) is your adversary. They will run a full-scale simulated attack, using covert techniques to avoid detection by the Blue Team and your defensive solution. Before launching the exercise, the BRT will sit with you and define the **objectives and the Rules of Engagement** of the

exercise. We will help you identify your critical assets and what flags need to be captured in order for the exercise to be successful. Our Red Teaming Exercise is conducted over a 3 to 5 week period, using a minimum of 3 Red Team members, depending on your scope.

The BRT will create **real-world attack scenarios** that will be played out against your defenses. This can be done either blindly, keeping your team in the dark to assess their true detection capabilities, or by letting them know when it's going to take place to collaboratively test your defenses.

The results from the Red Teaming Exercise provide an **overview into the gaps of your entire IT environment and security posture**, including both the technology you deployed and the people you have involved. It is of significant importance to test the configuration of your technology, the adequacy of the people and related processes that are a critical element of your incident response processes. Our thoroughly planned exercise puts your entire process under scrutiny, both for an **attempted breach and a successful one**.

Red Teaming Methodology

Week 1

Initial reconnaissance

This is phase one of the engagement. The first week, BEETLES Red Team (BRT), will consolidate efforts on collecting as much information as publicly and externally available, both on and off from client premises.

Week 2

Exploitation

The second week, BRT will focus on harnessing information gathered in the first phase and exploit your network to gain unauthorized access to the internal network.

Week 3

Action

Once the BRT has successfully exploited their way into the internal network, they will now focus on moving laterally across the network, compromise the domain controller and simulate to exfiltrate and/or simulate to compromise critical data and systems.

Week 4

Reporting

The fourth week of the engagement, BRT will take time to write up detailed reports, along with evidence of the findings and upload them onto our proprietary CrowdSpark Platform.

What is PCI DSS?

The Payment Card Industry Data Security Standard is a set of standards set by the Payment Card Industry Security Standards Council (PCI SSC) that merchants and payment card processors are required to follow in order to remain compliant. It is also a mandatory requirement set forth in the Bangladesh Bank ICT Guideline.

PCI standards present technical and operational requirements for protecting cardholder data. These standards are only applicable to any organization that stores, processes, or transmits cardholder data.

The PCI standards are personalized for these communities: merchants and processors, software developers and manufacturers and financial institutions. They address the 'ecosystem' of retail payment devices, applications, card processing infrastructure and the organizations that execute related operations. Every standard has its manager, and PCI is no different. An open global forum called the PCI SSC develops, manages, educates and raises awareness of the three PCI standards.

The council was founded in 2006 by the major card brands:

American Express, VISA World, MasterCard, Discover Financial Services, JCB International, etc. Each brand recognized the importance of securing cardholder data and agreed to incorporate the PCI Data Security Standard within its own compliance programs. The PCI SSC also recognizes Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV) who are duly certified by the council as certifying authority and audit resources for PCI DSS Compliance.

How to Comply with PCI DSS?

Merchants and other entities that store, process and/or transmit cardholder data must comply with the standards set forth with PCI DSS. While the Council is responsible for managing the data security standards, each payment card brand maintains its own separate compliance enforcement programs. Each payment card brand has defined specific requirements for compliance validation and reporting, such as provisions for performing self-assessments and when to engage a QSA.

Depending on an entity's classification or risk level (determined by the individual payment card brands) processes for validating compliance and reporting to acquiring financial institutions usually follow this track:

- PCI DSS scoping - determine what system components are governed by PCI DSS
- Assessing - examine the compliance of system components in scope.
- Compensating Controls - The assessor validates alternative control technologies/processes.
- Reporting - assessor and/or entity submits required documentation.
- Clarifications - assessor and/or entity clarifies/updates report statement (if applicable) upon request of the acquiring bank or payment card brand.

The Assessment Process

The beginning stages of validation and assessment can be **challenging for any organization**. To ensure that your organization is moving in the right direction, BEETLES provides consultation before beginning the assessment process to help analyze the scope of your compliance efforts and also assuring to put your firm in a better position in achieving compliance and saving you costs and efforts.

During the assessment process, our team will work with your team in performing a **specialized IT audit to assess the security of your systems**. Even though testing for vulnerabilities may be time-consuming, working with our

Why BEETLES?

BEETLES Cyber Security is a **PCI SSC enlisted and approved certifying authority** for the Bangladesh region with our own certified Qualified Security Assessor (QSA), under PCI SSC.

Along with fulfilling all the PCI DSS validation qualifications, our team will also help meet the following PCI DSS

Firewall
Management

Data Access
Control

Vendor Default
Controls

Personal Access
Controls

Data
Protection

Physical Access
Controls

Data Transmission
Encryption

Data & Network
Access Controls

Antivirus
Controls

Security
Testing

System &
Application Security

Information
Security Policy

Deliverables

BEETLES will assist your organization with every aspect of meeting PCI DSS compliance requirements and help you:

- Maximize the return on your security investment.
- Understand the PCI DSS and how it applies to your organization.
- Work towards achieving, validating and maintaining your compliance.

We pride ourselves on being able to help simplify the process of meeting your compliance status with the PCI DSS. Our process is scalable for any environment size and knowledge level. Whether you are a big financial institution or a small business owner going through your first PCI audit, we will make the process as simple as possible.

We can guide you through the validation process to get you back to your core competency running your business. Only now, your organization's critical data will be better protected!!

The BEETLES Red Team

Highly Skilled and Globally Accredited

BEETLES Cyber Security has brought together a team of individuals with a broad range of **knowledge, skill set and industry experiences**, both domestic and international. Our Red Team members are some of the most talented and experienced people in the field of cybersecurity penetration testing and bug bounty hunting. They are listed on the fortune 500 tech giant's Hall of Fame, such as Google, Microsoft, Facebook, Paypal, etc. and are ranked above 100 in HackerOne, one of the leading crowdsourced Bug Bounty hunting platforms in the world. They have extensive work experience with the US DoD, Military and Pentagon on Synack™ and Cobalt™.

Alongside them, we share a common vision, to develop the IT security industry in Bangladesh and to raise security awareness and meet standards Globally. All of our Red Team members are under strict **Non-Disclosure Agreement Contracts**, in accordance with the laws of The Government of the People's Republic of Bangladesh. The team is kept up-to-date with extensive training on the latest technology advances, security adversaries tactics, required skills as well as the latest in Tactics, Techniques and Procedures (TTPs).



SAFETY Password
Protection likes
Security Code dislikes
financial history friends
PERSONAL DATA
Data INFORMATION
Information Data Privacy
PRIVACY Security
SAFETY Protection
Password
FRIENDS AND FAMILIES
financial history
SECURITY Data Code
Protection information
likes and dislikes
PROTECTION SAFETY families
Information protection
Information



BEEETLES
THE HACKER'S APPROACH

Aziz Bhaban
93, Motijheel C/A (3rd Floor)
Dhaka-1000, Bangladesh
Phone: +880-2-9513744
Email: query@beetles.io
Web: www.beetles.io