AZTECH SYSTEMZ LTD.

Company Overview with Service

www.aztechsystemz.com
Email: info@aztechsystemz.com | Mobile: +8801935007700

Table of Contents

Company Overview 3
Mission 4
Vision 4
Background 4
About Us 7
Why Choose Us 8
Corporate Philosophy 9
Corporate Values 9
Environmental Policy 9
Human Resource 10
General Policy 10
Available Key Professional of AZTech Systemz Ltd. 10
Project Management Capacity 11
Monitoring and Evaluation Capacity 11
Products & Services 12
Services 12
Penetration Testing 13
Mobile App & Device Security 13
Network Pentesting 13
Vulnerability Assessment 13
Web Server Pentesting 14
Source Code Audit 14
Web Application Pentesting 14
Mobile Application Pentesting 14
Methodology and Technical Approach 15
Background of Services 15

Planning phase 21
Pretesting process 27
Penetration testing tools 34
Features and benefits 35
Our reporting formats 36
Management Development Program 38
Organogram 39
General Information of Legal Status of AZTech Systemz Ltd. 40
Contact Information 41

AZTECH SYSTEMZ LTD.

Company Overview

AZTech Systemz Ltd. is a managed Cyber Security firm providing cyber security consulting services for small, medium and large-sized companies. We understand that every business needs to be secured with a cybersecurity program.

We are experienced security specialists devoted to offering cutting-edge business digital protection administrations and arrangements. We assist associations in-safeguarding their representatives, clients, offices and tasks from inner and outer dangers and permit organizations to work more intelligently through improved security the board and data the executives arrangements.

Our experts are prepared and qualified Cyber security experts who have transformed their energy of Cyber security into a profession.

AZTech Systemz Ltd. expertise: -

01. Security Information and Event Management (SIEM)
02. Security Orchestration, Automation and Response (SOAR)
03. Cyber Threat Intelligence
04. Managed Detection & Response (MDR)
05. Cybersecurity Compliance
06. Application PenTesting
07. Web PenTesting
08. Network PenTesting
09. Network Device Configuration Review
10. VPN Configuration Assessment
11. Cloud Security Review
12. PCI DSS CDE Pentest
13. Mobile App PenTesting
14. Data Recovery
15. Training

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Mission

To keep offer and continuously support our customers with reliable technologies, services and solutions to ensure they stay at the maintain there competitive edge .

To provide customized security administration of the highest quality, to safeguard the life and property of our clients, delivered with warmth, friendliness, pride and organizational soul.

Vision

To become a leading Cyber Security solutions provider. Combining our internationally recognized abilities with local skills we continuously keep the wheels of AZTech Systemz Ltd turning and assisting our clients with gaining a firm grip on the most recent innovations and arrangements.

Background

In AZTech Systemz our primary strength is our highly capable representatives, who are competent in this field. We have three Certified Ethical Hackers in our team. Every one of our individuals is passionately committed. AZTech Systemz Ltd. works closely with the Government sector in Bangladesh as well as with internationally renowned organizations worldwide. We offer simple and flexible support programs to maximize the value of your AZTech Systemz services. We have assets like Prof. Dr. Touhid Bhuiyan and Dr. Hasan Azad who established AZTech Systemz Ltd. both of whom are exceptionally capable for growing our organization.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Dr. Hasan Azad

Ph.D Columbia University,New York

Founder of AZTech Systemz Ltd.

A truly dynamic thinker and business leader, Dr. Azad is seriously engaged with cyber security related work, where he is open to challenges, conversations, and the exchange of ideas from top players in the industry.

Attending Columbia University, Dr. Azad earned his Ph.D. in Religion and Philosophy in 2017. He is a published novelist—"*Red and Green Oil on Water being*" his first novel. He runs a well regarded academic podcast called CIME (Center for Interreligious and Multidisciplinary Ethics) where he interviews internationally renowned thinkers. He is working on a book length treatment examining the Ethics of Artificial Intelligence through a religious and philosophical lens. He writes on topics relating to spirituality while also working as a holistic life and wellness coach. He has research publications in renowned journals and conference proceedings.

Prior to establishing AZTech Systemz Ltd., Dr. Azad previously ran (and continues to do so) the property development company Tower Hamlet Properties Ltd.

(which has completed several residential and commercial buildings in prime locations in Dhaka), and the multimedia platform company N-Media. In Bangladesh, cybersecurity continues to be an area of some concern. As such, Dr. Azad is committed to providing a protected stage for end clients. His goal is to massively grow AZTech company in the next five year

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Dr. Touhid Bhuiyan

PhD from Queensland University of Technology, Australia

Co-Founder & COO of AZTech Systemz Ltd.

Dr. Bhuiyan received his PhD from Queensland University of Technology, Australia in the area of Information Security focusing on Trust Management for Intelligent Recommendations. He is a Certified Ethical Hacker. He obtained his Cyber Security: Cyber Risk and Resilience certificate from the University of Oxford. He is the recipient of the Australian Postgraduate Award (APA) and Deputy Vice-Chancellor's Award from QUT, Australia. He has received several scholarships, including the DGF-KTC ICT Scholarship, Ministry of Information and Communication, Korean Govt. CICC Scholarship in IT, Ministry of Economy, Trade and Industry, Japanese Govt. Commercialization Training Scheme Scholarship, Australian Govt. FIT Top-up Scholarship and FIT Faculty Scholarship from QUT, Australia. Furth he received the "Award for Excellent Achievement" as the best participant in the e-Learning Contents Development Course from CICC, Tokyo, Japan.

Dr. Bhuiyan was the Director of the Cyber Security Centre, Daffodil International University (DIU), Bangladesh. He is also the Head and Professor of the Computer Science & Engineering department at the same university. His research interests are in cyber security, intelligent recommendations, social network, trust management, bigdata analytics, e-Health, e-Learning etc. Before founding AZTech Systemz Ltd. he worked for several institutions including Monash University, The University of Western Australia, Queensland University of Technology, University of Western Sydney and Central College Sydney. Dr. Bhuiyan has over 18 years experience in teaching, research and working in the IT industry in Australia, Singapore, Malaysia and Bangladesh. He has more than 114 research publications in renowned national and international journals, books and conference proceedings.

His cyber security related publication was Evaluating the Readiness of Cyber Resilient Bangladesh. Journal of Internet Technology and Secured Transactions (JITST), Vol. 4, No.3, pp. 405-415, ISSN 2046-3723. He likewise presented at a cyber security related International conference for his publication on SQLi Vulnerability in Education Sector Websites of Bangladesh. The Second International Conference on Information Security and Cyber Forensics,15-17Nov, 2015, Cape Town, South Africa and A Case Study of SQL Injection Vulnerabilities Assessment of .bd Domain Web Applications. The Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic, 29-31 Oct, 2015, Jakarta, Indonesia.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

About Us

Name of the Company	**AZTech Systemz Ltd.**
Nature of Business:	Application PenTesting , Cybersecurity compliance, API PenTesting, Radio, Network PenTesting, Network Device Configuration Review, VPN Configuration Assessment, Cloud Infrastructure Security Review, PCI DSS CDE PenTest, InfoSec Consultancy, Application Design, Testing, IT Audit, 24/7 Services & Support and Maintenance.
Bangladesh Corporate & Registered Office and Development Center Bangladesh:	104 Sukrabad,Dhanmondi, Dhaka -1205
Chairman:	Ashrafi Azad
Managing Director	Dr. Hasan Azad
Director	Dr. Touhid Bhuiyan
Contact Person:	Kazi Imdadul Islam Business Development Coordinator kaziimdadulislam@aztechsystemz.com
Other Sister Concerns:	N-Media

AZTECH SYSTEMZ LTD.

Why Choose Us

AZTech Systemz Ltd: Key Strengths & ifferentiators

At **AZTech Systemz Ltd,** we endeavor to accomplish greatness in all that we do. In this specific situation, the administrations we give to different area will be the same. Tasks are led overseen on location/offsite by our senior experts conveying quality experience and overseen by experienced Project Managers of in Cyber Security.

1. **Multi-Disciplinary Team:** Our team comprises experts with multi-disciplinary capabilities (Cyber security compliance, Penetration Tester, Ethical Hacker, etc.)

2. **Domain Expertise across various functions with Business & Technology domains:-** AZTech team houses business and technology domain professionals experienced in conducting Information Security Compliance, Risk Management Reviews, IS Reviews, VA/PT Reviews, Process Reviews, Risk Based Reviews, Infrastructure Management.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Corporate Philosophy

1. Ensure Clients Prosperity.
2. Focus on outcome.
3. Strive toward greatness.

Corporate Values

AZTech Systemz Ltd. committed to:

1. True cooperation with clients and accomplices.
2. Complete comprehension of client's business.
3. Persistence in following through with the task anything that it takes.
4. Ensure the work principles.

Environmental Policy

AZTech Systemz Ltd. is committed to improving the environmental performance of its business operations. We seek to:

1. Meet or surpass all relevant ecological regulations and guidelines.
2. Minimize the impact on the climate by decreasing use of every unrefined substance, energy, and providers.
3. Identify and measure the natural effects of our activities and items.
4. Increase the effectiveness of the current asset by reusing or reusing our waste or passing it to another business.
5. Encourage providers, merchants, and colleagues to be earth capable.
6. Provide a protected climate for the local area overall and a sound work environment for our representatives.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Human Resource

General Policy

AZTech Systemz Ltd. enlists knowledgeable, adaptable, motivated, and proactive individuals who prosper under conditions of change and challenge. They are, imaginative, fearless and acknowledge liability by stepping up to the plate continuously growing according to an invigorating global work space.

We look for initiative attributes, phenomenal relational abilities, solid scholastic execution, and significant expert experience. Past involvement with a worldwide or multicultural climate is seen in extremely favorable terms.

The organization offers excellent serious pay bundles and a superb path to professional development. Our diverse labor force and multicultural climate assists our representatives in adjusting and integrating their work and individual lives. Our workers appreciate nonstop learning and expert development in a unique professional climate.

Available Key Professional of AZTech Systemz Ltd.

SL No.	Description	Number of Professional
1	Chief Operating Officer	1
2	Chief Technology Officer	1
3	Chief Information Officer	1
4	Technology Manager	1
5	Project Management Professional & Marketing	2
6	Website Development	9
7	App Development	8
8	Cyber Security Analyst	4
9	PenTester	9
10	Training Coordinator	4
11	Business Development Manager	1
12	Business Development Executive	1
13	HR and Administrator	2
14	Accounts and Finance	1
14	Others & Technicians	5
Total		**50**

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Project Management Capacity

The term project the executives is frequently used to depict the hierarchical or administrative way to deal with carrying out projects. AZTech Systemz Ltd. has an undertaken supervisory crew to achieve exercises through the use of cycle gatherings, such as: starting, arranging, execution, testing, and backing and upkeep.

The faculty keep up with the joint effort with the clients' contact staff and gather all expected data since commencement to conveyance of a specific venture. The Certified Project Management Professionals deal with the advancement utilizing dependable Project Management Tools Agile/Scrum.

Starting from the inception of a task this group sets up the achievements of the venture expectations and draws in the assets as per the volume of the undertaking. This group circles back to the venture progress and is capable of providing a moment answer for the client. After the completion of a venture, the group likewise keeps contact with the clients' contact staff to guarantee after conveyance/upkeep administration.

Monitoring and Evaluation Capacity

For an IT empowered specialist co-op it is more fundamental to manage the advancement of a specific Software Development progress or Database Development and furthermore Network, Infrastructure, and Hardware Monitoring. AZTech systemz Ltd. has a number of experts who are specialists in Cyber Security Audit. In particular, this group has participated in Monitoring and Supervising the Progress of Software Development and Database Development of a specific venture.

Products & Services

Our various products and services include technical consultation, application development, business process automation and business and application support. We are developing a wide range of products catering to customized business solutions. Our Products are designed in an innovative front-line manner to meet rapidly evolving and growing requirements. Our comprehensive and flexible products and solutions are designed to:

- Minimize paperwork.
- Reduce administrative costs.
- Adopt international standards.
- Sustain business workflow.
- Enhance productivity.
- Assure quality customer service.

Services

01. Security Information and Event Management (SIEM)
02. Security Orchestration, Automation and Response (SOAR)
03. Cyber Threat Intelligence
04. Managed Detection & Response (MDR)
05. Cybersecurity Compliance
06. Application PenTesting
07. Web PenTesting
08. Network PenTesting
09. Network Device Configuration Review
10. VPN Configuration Assessment
11. Cloud Security Review
12. PCI DSS CDE Pentest
13. Mobile App PenTesting
14. Data Recovery
15. Training provider

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Penetration Testing

Penetration testing finds out whether unauthorized access or other malicious activity is possible in the existing vulnerabilities of any system. It identifies and prioritizes security risks. A good penetration testing process is a great tool to defend all the flaws in any system.

- Quickly discover the attack surface of a target Organization.
- Bypass local network restrictions and scan from external IP addresses.
- Create credible proofs-of-concept to prove the real risk of vulnerabilities.

Mobile App & Device Security

We specialize in performing security assessments of mobile applications in iOS and Android environments. These operating systems on tablets and smartphones cover the vast majority of the mobile. Today we are using these devices in our business fields and this use has dramatically increased. We are using them in buying products, banking, mobile banking and mobile payment solutions. In fact, the app economy has created an entire industry with it. Extended use of these devices has created huge scope for the hackers to get access into them and cause a serious threat.

Network Pentesting

By network penetration test, we identify exploitable vulnerabilities in networks, systems, hosts and network devices (ie: routers, switches). These vulnerabilities allow hackers to exploit the network. Network penetration testing provides opportunities for hackers to compromise systems and networks. In this way, they can have access to sensitive data. Intrusion prevention systems (IPS): IPS record network traffic and analyze activity to prevent advanced malware threats and zero-day vulnerabilities.

- Find out security flaws present in the network
- Estimate the level of risk for your organization
- Fix unidentified network security flaws

Vulnerability Assessment

Vulnerability in software means a bug in the code that can be exploited to cause harm or a weakness in internal controls that can cause a security breach. Vulnerability assessment is the process used to identify, classify and prioritize vulnerabilities in a system. We identify and understand the threats of vulnerability and react appropriately.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Web Server Pentesting

We check whether your organization is resistant to a variety of simulated social engineering attacks, conducted over the Internet. Web server pentesting performing under 3 major category which is identity, analysis, and reporting vulnerabilities such as authentication weaknesses, configuration errors, and protocol relation vulnerabilities.

- Enumerate web server Directories to extract important information about web functionalities, login forms, etc.

Source Code Audit

Source code audit is formed on the basis of an integrated analysis of violations of programming conventions, discovering AZTech Systemz, security breaches. It makes a software error free before its release. To find out the security weaknesses, experts manually inspect the source code during the source code audit. Our experts put emphasis on every critical component carefully and complete the audit. They work on both high-risk vulnerabilities and low-risk vulnerabilities.

Web Application Pentesting

Our expert website penetration testers will analyze all aspects of your web app to help you stamp out security weaknesses. This helps to identify and prioritize organizational risks and works towards a secure software development lifecycle.

- Uncover vulnerabilities and poor security controls
- Exploit web application security flaws
- Expose insecure functionality in your app
- Catch security design issues before it’s too late

Mobile Application Pentesting

Mobile devices have become an extremely attractive platform for the development of business applications in various industries. Ease of use and mobility are just some of the advantages that such mobile applications bring when compared to standard online services. On the other hand, new attack vectors and threats against mobile devices are often overseen. Due to this new threat landscape, AZTech Systemz offers specialized mobile application penetration test services.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Methodology and Technical Approach

Background of Services

Penetration testing

Penetration testing is the activity conducted by a penetration tester (Penetration Tester) or auditor. A group of many testers is called tiger team. Technically, a penetration test is a securityoriented systematic probing of system from" inside" or" outside" to seek out vulnerabilities that an attacker could exploit. A system could be any combination of application, host or networks. In other word, it is the act of assessing all the IT infrastructure components including operating systems, communication medium, applications, network devices, physical security, and human psychology using similar or identical methods to that of an attacker but perform by the authorized and qualified IT professionals.

Penetration test can be defined as the" simulation of a real-world attack against a target network or application, encompassing a wide range of activities and variations". The variations include simulating an insider threat as opposed to an external attacker, varying the amount of target information provided in advance of the testing.

A simple example of penetration testing is to use 'Google Search Engine'. In a book," Google Hacking for Penetration Testers" by Johnny Long demonstrated many tricks to get information from the engine using Google's massive database. This book provides a good resource for security experts and penetration testers to discover preliminary information about the target by using directives such as" site: target-domain.com", find employee contact and email address, trace vulnerable software installations, map the network and more. Similarly, when a bug is found in another popular web application, Google can often provide a list of vulnerable servers worldwide within seconds, giving information to a well-trained attacker.

Penetration testing is a critical step in the development of any secure system as it not only stresses the operation, but the implementation and design of a system. It is an authorized and scheduled act that separates a penetration tester from an attacker and has been widely adopted by the organization and institutions. For example, a simple penetration testing may involve scanning of an IP address to identify hosts that are offering services with known vulnerabilities or even exploitable vulnerabilities that exist in an unpatched operating system. The results of these tests are then documented and submitted as report and the vulnerabilities identified can then be resolved. It does an extensive and systematic test by analyzing the systems for security breaches and providing valuable information to map security issues clearly with either manual or automated tools. Throughout penetration testing period, the aware- ness of management

and staffs of an organization is important as such tests sometime can have some serious consequences such as system crashing and network congestion resulting the outage of

the system or network equipment and also may alert the IDS. In the worst-case scenario, it can result in exactly the thing it is intended to prevent.

Objectives of Penetration Test

Penetration test provides a bird-eye perspective on current security posture of an organization's IT infrastructure. The intent of a penetration test is to determine the feasibility of an attack and its impact of a successful exploit if discovered. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. It helps to narrow down security risk and confirm whether the current security measures implemented are effective, or not. Some of the other principal reasons for adopting penetration testing are listed below:

Providing a Good Starting point

A penetration testing provides a good first step to understanding present security posture of an organization by identifying flaws and breaches of security, and point outs where to apply security technologies and services so that the organization can deploy an action plan to mitigate the threats of attack or misuse.

Identify and prioritize security risk

Identifying the security risk is the actual objective of penetration testing. The use of penetration testing not only help to understand the security risk, it also helps to prioritize risk issues together with an assessment of their impact and often with a proposal for mitigations. The risk identified during the testing can be prioritized on the basis of severity. Also, these efforts can lead to efficient budget allocation for information security issues.

Improving security of computer system

Penetration testing is performed with the objective of improving the security of computer systems such as firewalls, routers and servers. Different security mechanisms like IDS, firewall, and cryptography are used to protect data. How- ever, the frequency and severity of network intrusion, data theft and attacks caused by malicious code, hackers, disgruntled employees continue to increase along with the risks and costs associated with network security breaches and data theft. Penetration testing helps to

address such concerns. For example, to find unnecessary open ports or vulnerable versions of web applications and operating systems.

Improving security of an overall organizational infrastructure

Apart from testing the technical infrastructure, a penetration test can also test management and employee infrastructure, to monitor escalation procedures, for instance, with the scope and/or aggressiveness of the tests being increased step by step. Social engineering techniques, such as requesting passwords over the telephone, can be

employed to assess the level of general security awareness and the effectiveness of security policies and user agreements.

Performing Due Diligence and Independent Audits

An unbiased security analysis and penetration test can focus internal security resources where they are needed most. In addition, an independent security audit provides evidence of due diligence in a legal context for protecting online assets, minimizing potential loss of shareholder value. This independent audit is rapidly becoming a requirement for obtaining cyber-security insurance.

Reducing financial losses

Once security risk and infrastructure are in place, penetration test provides critical validation feedback between business initiatives and a security framework that allows to mitigate the financial loss and successful implementation of minimal risk.

Phases of Penetration Testing

The overall process of penetration testing can be broken into a number of steps or phases. When these steps or phases are put together, they form a comprehensive penetration testing methodology. Different methodologies have used different nomenclature for various steps or phases, but they share the same objective. Although, the specific terminology may differ, the process provides a complete overview of the penetration testing methodologies. There are three phases namely Pre-Attack phase, Attack phase and Post-Attack phase, as shown in Figure The activities in each phase depends on how the rules of engagement have specified that the penetration testing should be conducted. Each phase has been briefly described below from the perspective of blackbox approach targeting information systems.

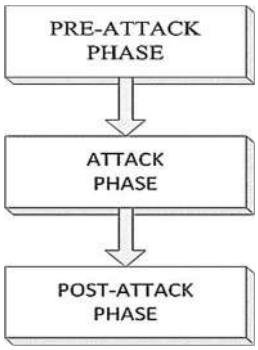


Figure A : The Three phases in a Penetration Test

Pre-Attack Phase

The pre-attack phase, as shown in Figure, involves reconnaissance or data gathering to discover as much information as possible of the target, nearly all facets of information gathering leverage the power of the Internet. To be successful at

reconnaissance, strategy needs to include both passive and active reconnaissance techniques. Passive Reconnaissance makes use of the information resources available on the web. Unlike active reconnaissance, there is no direct interaction with the target as such, the tar- get has no way of knowing, recording, or logging Penetration Tester's activities. It involves activities like obtaining registration information, product and services offered, document sifting and social engineering Etc. Active Reconnaissance attempts to profile and map the Internet profile of the target. It involves activities like OS fingerprinting, port scanning, network mapping, perimeter mapping and web profiling.

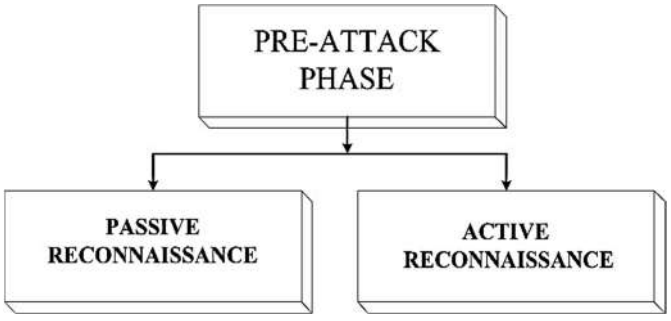


Figure B: The Pre-Attack Phase in a Penetration Test

Attack Phase

As the name suggests, this attack phase, as shown in Figure, involves the actual compromise of the target. The attacks are performed based on the flaws and vulnerabilities discovered during the pre-attack phase. During this phase, tools can range from exploitive to responsive to find as many vulnerabilities as possible because neither the organization nor the Penetration Tester will know which vulnerability an attacker will choose to exploit first.

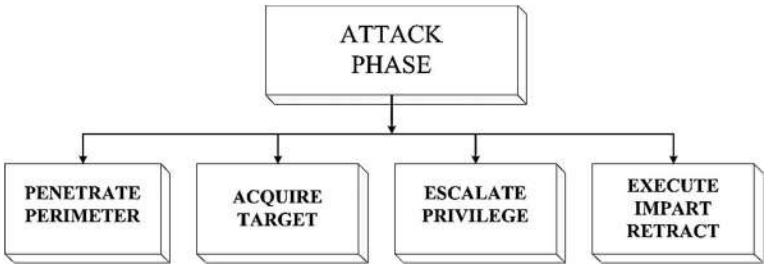


Figure C: The Attack Phase in a Penetration Test

Various tools and techniques such as vulnerability scanner, active probing scans and social engineering, are deployed to acquire the target machine. When the target is acquired, an attempt is made to escalate privileges by exploiting the target and installing one or more applications to sustain their access, further exploit the compromised system, and/or attempt to extend their control to other systems within the network. The use of techniques like brute force to obtain an authenticated status and use of Trojans, Protocol Analyzers, or any other means to get information are involved during privileges escalation. The main goal here is to explore the extent to which defenses fail. Finally, the way is made into the system or network, to eliminate all evidence of their presence in a process some call" covering their tracks." Normal activities included in this phase are as follows:

1. Checking to see how the target is responding to error responses and how it is managing errors when probed with ICMP probes.
2. Spoofing responses by creating specially crafted packets to test the access control lists.

3. Testing to measure the threshold of denial-of-service attacks by sending different connection variations of both TCP and UDP.
4. Testing to see which protocol filters are in place by trying to connect with the most frequently used protocols (such as SSH, FTP, and Telnet).
5. Testing to see whether the IDS allow malicious content and scanning the target in many ways to see whether the IDS captures abnormal traffic.
6. Test to see if systems in the DMZ, such as web server, respond to the web server scans by performing various methods such as POST, DELETE, and COPY

Post-Attack Phase

The post-attack phase, as shown in Figure D, involves restoring the systems back to their original pre-test state, which includes removing uploaded root kits files or back-door programs, reversing of any access control list (ACL) changes to files or folders or other system or user objects, restoration of the network devices, and network infrastructure, cleaning up the Registry entries added during the exploitation, and removing shares and connections established during the gaining access phase.

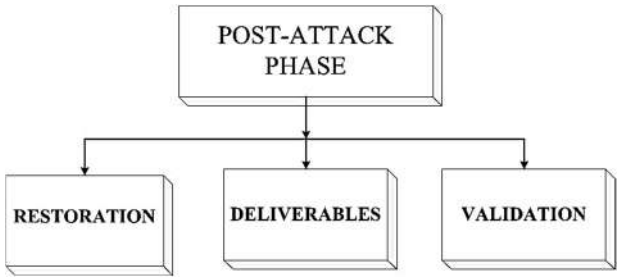


Figure D: The Post-Attack Phase in a Penetration Test

Penetration Testing Deliverables include a detailed report of all incidents that occurred and all activities carried out throughout the testing phase with recommended corrective measures as agreed upon in the rules of engagement. Validation of Penetration is a documented report with the actual validation of asses value that would be lost in regards to breach of security defenses. This report also defines to what degree the penetration testing was successful, and unsuccessful. Validation establishes the worth of penetration testing for its defensive measures in the entire environment.

Planning phase

A great deal of planning and preparation needs to be done, in order to make penetration testing a success. During this phase, the objectives, the scope, legal restriction and scheduling for the assignment are defined and formulated. In a company, the objective of a penetration testing is to demonstrate what exploitable vulnerabilities exist within a company's network. The scoping can be done by identifying existing security policies, industry standards and best practices etc. Some of the inputs and the expertise of a penetration testing team must also be part of the scope when deciding the level of the penetration test. Additionally, some legal restriction, which lists the acceptable and non-acceptable procedures, a penetration testing team must follow to ensure no accidental targeting the wrong application or interface which could have serious legal ramifications. Also, the scheduling about what will be attacked, when, from where and how must be discussed during the kickoff meeting sessions. This is vital, as it ensures normal business and everyday operations of the company will not be disrupted.

Administrative tasks like assembling a team, gathering documentation, acquiring test accounts, reserving equipment, etc. also fall under the planning and preparation phase. This phase consists of all the activities that are needed to be performed prior to commencement of the actual penetration test. When a company decides to conduct a penetration test, it is imperative to get formal permission for conducting penetration testing prior to starting. This permission, often called the rules of engagement (ROE), should include:

- Specific IP addresses/ranges to be tested
- Any restricted host (i.e., hosts, systems, subnets, not to be tested)
- A list of acceptable testing techniques e.g. social engineering, DoS (Denial of Service), etc. and tools (password crackers, network sniffers, etc.)
- Times to conduct the testing (e.g. during business hours, after business hours, etc)
- Identification of a finite period of testing
- IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual malicious attacks
- Points of contacts for the penetration testing team, the targeted system and the networks
- Measures to prevent law enforcement being called with false alarms (created by the testing)
- Handling of information collected by the penetration testing team

Discovery Phase

After defining the objectives, scope, legal restriction and scheduling, the actual testing starts; it can be regarded as an information gathering phase. This phase can be further divided into as follows:

i. Reconnaissance and Target discovery
ii. Scanning and Enumeration

i. Reconnaissance and Target discovery

In this phase, penetration tester tries to compile as much publicly available information as possible via both technical and non-technical means. The goal is to identify the types of systems within the network, including operating system, information areas open to attack or known security shortcomings etc.

Reconnaissance can be segregated into two different types - passive and active. During passive reconnaissance, various types of searches are conducted, including information related to the target network and systems without connecting to them directly, including employee information, physical location and business activity. Active reconnaissance will also find information similar to what already found using passive reconnaissance. The benefit of these two types of reconnaissance is twofold: identify historical information using passive gathering and confirm findings with active methods.

Penetration tester performs this phase with open-source information, tools and techniques to acquire a specific view of the target. However, going through the literature, one can see the extensive use of certain tools and techniques. In most of reconnaissance, tools and techniques listed within ISSAF

methodology and SANS are more likely to be used. The most common and non-evasive tools and techniques used for reconnaissance are:

- Social Engineering Social engineering techniques like impersonation, bribery, deception, conformity and reverse social engineering can be

- deployed to gain specific information about an individual or about target. All of these techniques are accomplished via physical entry into the target organization or through communication with individuals at the target organization. Social engineering works because people are, for the most

part, trusting and helpful. The success or failure of social engineering depends on the tester's ability to manipulate human psychology.

- Dumpster Diving Dumpster diving can provide testers with sensitive information, as well as hardware and software. Normally, documents like drafts of letters, mailmerge documents, company directory sheets, catalog lists, policy manuals are considered less sensitive are dumped into publicly available receptacles. These documents can act as an information source, to find out names, ad- dresses, phone numbers and employee ID and aid in all sorts of reconnaissance techniques.

- Internet Footprinting Internet footprinting is a technical method of reconnaissance. It is clean, legal and safe method of surveillance. There are four methods of Internet footprinting: Web presence, Network enumeration, Domain Name System (DNS)- based reconnaissance, and network-based reconnaissance. During Web presence, penetration tester can collect wealth of information about a target company including employee information by surfing company's web pages and other online documents related about the organization. The penetration tester's research tools may include browser, Usenet, Dogpile.com, Alexa.org, search engines, newsgroup, security-related web sites and newsletters. Net- work enumeration is the process of identifying domain names and other re- sources on the target network. Penetration tester make use of a tool called WHOIS in order to gather this data. WHOIS database contains information regarding assignment of Internet addresses, domain names, and individual con- tracts. WHOIS information is based on a hierarchy, and the best place to the starting point for all manual WHOIS queries is the top of the tree - ICANN5 Once the WHOIS tool finds a matching entry in the Registrar database, it disses- plays information about the searched item. The result may include:

  - The address of the registrant
  - Domain name
  - Administrative and technical contact information, with names, phone numbers, and e-mail address
  - A list of Domain servers, with names and IP addresses

- Date and time of record creation
- Date and time when the record was last modified

- Domain Name System (DNS)- based reconnaissance uses information available from DNS servers about the IP address of the target network domain names and alternate domains that might be on or connected to the target network. This method uses DNS lookup, DNS Zone Transfer tools like nslookup, dig, host and Network-based Reconnaissance is the process of identifying active computers and services on a target network via tools like as ping, traceroute and netstat.

ii. Scanning and Enumeration

After reconnaissance, penetration tester moves into a scanning and enumeration phase. Scanning phase comprises of identifying live systems within the target network, find5A technical coordination body for the Internet that assigns Internet Domain names, IP ad- dress numbers, Protocol parameters and port numbers open and filtered ports, services running on these ports, identifying the operating system details(fingerprinting) and network path discovery, etc. to identify potential security holes and vulnerabilities on the target host or network using active probes and passive network sniffing tools and techniques. After the successful identification of live system and running services, they should be fingerprinted and enumerated.

In general, information seeks via fingerprinting includes the exact name and versions of the services running on the target system, and the underlying Operating system help in identifying and eliminating various false positive, and information seek via enumeration includes user account names (to inform subsequent password guessing attacks), misconfigured shared resources (for example, unsecured file shares) and older software versions with known security vulnerabilities (such as web servers with remote buffer overflows). Throughout this and other successive phases, penetration tester must be cautious not to overwhelm the target system or network with excessive traffic. Some of the most popular and common tools used during this phase are nmap, netcat, hping2 and superscan etc.

Assessment Phase

The next is an assessment phase, after identifying underlying technology and services versions in the target system or network. This phase is closely linked with discovery phase. For successful completion of this phase, discovery phase plays a vital

role and the information derived from discovery phase are the source of input for the assessment phase and vice versa. During previous phases, data on operating system, IP addresses, services/applications are collected mainly from Internet and performed scanning and enumeration based on these data, and now this information will be re- fined to examine and communicate directly with the target systems or network with the intent of identifying and analyzing the potential vulnerabilities and threats. The vulnerabilities that constitute threats in a network include software AZTech Systemz, system misconfiguration, unsecured accounts and unnecessary services. During this phase, a systematic examination of the system or network is performed to determine the necessity of security measures, identify security flaws and provide data for further phases. Assessment phase involves:

i. Vulnerabilities Identification
ii. Vulnerabilities Analysis

i. **Vulnerabilities Identification**

This sub-phase possesses the characteristics of the discovery phase. Penetration tester starts from probing the live target systems or networks closer than what was done in the discovery phase, using active probes and passive network sniffing. Both active probes and passive network sniffers are used to understand what services are running on a target system, to understand the internal network and fingerprint the operating system running on the target systems. Once the systems are detected, operating systems are identified, and services available are verified then the analysis should be performed to find the potential threats and vulnerabilities. There are vulnerability databases like SecurityFocus (www.securityfocus.com) and PacketStrom (www.packetstormsecurity.com) available on the Internet, which pro- vides information about the vulnerability and threats.

ii. **Vulnerabilities Analysis**

Penetration tester needs to understand the state of security within a system or a network and find out which vulnerability are real and which ones are false positive. If identifying vulnerability help to improve the security of system by understanding the current risk environment in information security, analysis of vulnerability shows how bad things can get if vulnerabilities are exploited. Penetration tester may use automated scanning tools along with their own skills to test the target system or network for vulnerabilities. These automated tools have their own database

which provides information about the past and latest vulnerabilities and their details.

Exploration Phase

This is an enthralling and challenging phase in any penetration testing. This step selects attack methods, and identify suitable targets for penetration attempts, after identifying and analyzing the vulnerabilities. Once the suitable targets are identified, the penetration attempt will be performed on these targets. If an attack is successful, the vulnerability is verified and confirmed, and further attempts are made to gain higher privilege. Exploration phase, also sometimes referred as attack phase can be further categorized into:

i. Exploitation
ii. Privilege Escalation

i. **Exploitation**

By now, the penetration tester has acquired lots of information about the target system and network. This information is now used to break into the target system. However, at this point penetration tester should consider external factors that affect what tools to use and when. This phase acts as verification of potential vulnerabilities and thus, entails the highest risk within a penetration test so it should be performed with a lot of caution. All the possible effects need to be carefully considered; all the exploits need to be thoroughly tested in a controlled environment before performing critical test procedures, such as the utilization of buffer overflow exploits. Time restriction always exists, forcing the penetration to make use of the framework as these frameworks help to reduce a lot of time instead of writing custom exploits. Metasploit is one of such open source exploitation frameworks that is extensively used during penetration test.

ii. Privilege Escalation

After an initial compromise of a target system or network, the penetration tester should look for ways, to increase their access to the system. Suppose, if a penetration tester has gained a local system access, tester should make an effort to carry out further analysis on the target system to gain root privilege. Likewise, if the penetration tester has network access, the tester should sniff for traffic on the network, to see what sensitive information can be obtained. Successful exploitation of vulnerability does not guarantee a root access, so a tester should make constant attempts to escalate the privilege and, in the process, tester might install rootkits or backdoors that assist in gaining a higher privilege level. This process is called privilege escalation. Along with vulnerability exploits, social

engineering tactics should also be deployed for the purpose of privilege escalation because social engineering has proven to be an effective way of obtaining sensitive information about a company and its employees.

At the end of this phase, the penetration tester will most likely understand the security strength and weaknesses of the target system or network. The penetration test will soon conclude, and the tester will begin to work on the final report. It is necessary to remember the actual goal and objective in a penetration test is not only to compromise a system or network, but it is also to inform and bring awareness to the stakeholders and computer professional specially network/system administrator, who are associated with the organization, as to what vulnerabilities exist on their system.

Reporting Phase

Reporting phase can occur in parallel to the other phases or at the end of the exploitation phase. Reports should contain an evaluation of the vulnerabilities located in the form of potential risks and recommendations for mitigating the vulnerabilities and risk. This reporting phase must guarantee the transparency of the tests and the vulnerabilities it disclosed. In general, this final report is an opportunity to understand the overall security posture of the systems or network.

Pretesting process

✓ *Black Box Testing*

Scanning of all critical documents has to be taken up initially. For all the critical applications and data vendor is required to perform Black Box testing and thereby perform the penetration test to simulate an external hacking or cyber warfare attack both at Application layer as well as Network layer. The vendor shall also carry out the segmentation check.

✓ *White Box Testing*

With knowledge of the internal structure/design/implementation of the application/object allowed to be tested vendor shall perform the White Box testing both at Application layer as well as Network layer. The vendor shall also carry out the segmentation check.

✓ *Gray Box Testing*

Successful vendor shall also perform Gray Box Testing both at Application layer as well as Network layer.The vendor shall also carry out the segmentation check. Interim Reports & Post Execution Activities It is recommended that the report should contain any and all the findings that impact the security posture of the

assessed entity even in cases where exploitation did not occur. In the testing phase, all relevant tests need to be conducted as per the project schedule and satisfactory report should be obtained from the concerned authorities of NABARD before preparing it for execution. Potential risks posed by known vulnerabilities, ranked in accordance with NVD/CVSS base scores associated with each vulnerability. Note that external vulnerability scans must be performed by an ASV and the risks ranked in accordance with the CVSS. Internal vulnerability scans may be performed by qualified personnel (does not require an ASV).

Website/Web – Application Assessment

Website/Web- Application assessment should be done as per latest OWASP guidelines including but not limited to the following: -

- SQL Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security misconfiguration
- Insecure Cryptographic Storage
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Any other attacks, which are vulnerable to the web sites and web Applications

The vendor has also to perform the following activities to assess the internet facing applications: -

a) Re-Engineering

b) Decompose or deconstruct the binary codes, if accessible.

c) Determine the protocol specification of the server/client application.

d) Guess program logic from the error/debug messages in the application outputs and pro- gram behaviors/performance.

- **Authentication**

a) Find possible brute force password guessing access points in the applications.

b) Find a valid login credentials with password grinding, if possible.

c) Bypass authentication system with spoofed tokens.

d) Bypass authentication system using Injection attacks.

e) Bypass authentication system with replay authentication information.

f) Determine the application logic to maintain the authentication sessions - number of (consecutive) failure logins allowed, login timeout, etc.

g) Determine the limitations of access control in the applications - access permissions, login session duration, idle duration.

h) Determine the transmission of authentication credentials in clear text/ encrypted/ hash form.

- **Session Management**

a) Determine the session management information - number of concurrent sessions, IP- based authentication, role-based authentication, identity-based authentication, cookie usage, session ID in URL encoding string, session ID in hidden HTML field variables, etc.

b) Guess the session ID sequence and format

c) Determine the session ID is maintained with IP address information; check if the same session information can be retried and reused in another machine.

d) Determine the session management limitations - bandwidth usages, file download/up- load limitations, transaction limitations, etc.

e) Gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping.

f) Gather sensitive information with Man-In-the-Middle attacks.

g) Inject excess/bogus information with Session-Hijacking techniques.

h) Replay gathered information to fool the applications.

- **Input Manipulation**

a) Verify that input validation is happening at client or server or both ends.

b) Find the limitations of the defined variables and protocol payload - data length, data type, construct format, etc.

c) Use exceptionally long character-strings to find buffer overflows vulnerability in

d) The applications. Concatenate commands in the input strings of the applications.

e) Inject SQL language in the input strings of database-tiered web applications.

f) Examine "Cross-Site Scripting" in the web applications of the system.

g) Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.

h) Use specific URL-encoded strings and/or Unicode-encoded strings to bypass input validation mechanisms of the applications.

i) Execute remote commands through "Server Side Include".

j) Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.

k) Manipulate the (hidden) field variable in the HTML forms to fool or modify the logic in the server-side web applications.

l) Manipulate the "Referrer", "Host", etc. HTTP Protocol variables to fool or modify the logic in the server-side web applications.

m) Use illogical/illegal input to test the application error-handling routines and to find useful debug/error messages from the applications.

- **Output Manipulation**

a) Retrieve valuable information stored in the cookies

b) Retrieve valuable information from the client application cache.

c) Retrieve valuable information stored in the serialized objects.

d) Retrieve valuable information stored in the temporary files and objects.

e) Retrieve bulk information/ multiple rows from database.

f) Information Leakage

g) Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.

h) Find valuable information stored in the HTML source code on browser like Unencrypted

View State

i) Examine the information contained in the application banners, usage instructions,

j) Welcome messages, farewell messages, application help messages, debug/error messages, etc.

Open Web Application Security Project Top Ten

To address the issue of more and more applications becoming Internet based, and the need to test the security aspects of Web applications, resources such as the open-source methodology Open Web Application Security Project (OWASP) can be used [29]. OWASP is an open-source project that provides a testing framework for http-based applications. It is more limited in scope than the other standards but covers its area in detail.

OWASP Testing Guide is an excellent description of the numerous kinds of testing that is needed to be properly done and executed, providing great depth and a broad selection of tools to use in the web applications security testing process. This OWASP testing guide attempts to bring its top ten projects forward with its comprehensive description of determining the organization's risk, and increase the awareness of application security among various organizations. The OWASP testing guide rates risk based on the impact it could have to the business and organization, and the probability of it to occur. The guide does not focus on the complete application security programs but provides a necessary foundation to integrate security through secure coding principles and practices. It categorizes the application security risks by evaluating the top attack vectors and security weaknesses in relation with their technical and business impact. OWASP testing guide primarily concentrates on web application testing, which includes:

- Information gathering
- Configuration management

- Authentication testing
- Authorization testing
- Business logic testing
- Data validation testing
- Denial of service attacks testing
- Session management testing
- Web services testing
- Risk severity
- AJAX testing

The OWASP Top 10 Web Application Security Risks for 2010 are

a) A1: Injection

b) A2: Cross-Site Scripting (XSS)

c) A3: Broken Authentication and Session Management

d) A4: Insecure Direct Object References

e) A5: Cross-Site Request Forgery (CSRF)

f) A6: Security Misconfiguration

g) A7: Insecure Cryptographic Storage

h) A8: Failure to Restrict URL Access

i) A9: Insufficient Transport Layer Protection

j) A10: Invalidated Redirects and Forwards

Mobile Application

The mobile application penetration testing methodology is typically based on the application security methodology. The focus shifts from traditional application security, where the primary threat is from multiple sources over the

Internet. The key difference is in the client-side security, filesystem, hardware, and network security. Traditionally for mobile applications, an end user is in control of the device.

The penetration test as a whole will follow a general penetration test process: information gathering, scanning and probing, vulnerability assessment, exploitation, and reporting. The mobile app itself will be checked for:

- Input validation vulnerabilities
- Sensitive data in the app binary or code
- Sensitive data in memory and local storage
- Local communication issues such as Bluetooth or NFC
- Residual sensitive data on removal
- Platform specific logging vulnerabilities
- Issues around jailbroken devices

The platforms included in the penetration test could be iOS IPA files on the iPhone or iPad, Java APKs on Android devices, XAP files for Windows Phone, other mobile platforms, or several of these platforms.

The penetration test on the web services that the mobile app communicates with is more like a standard web application penetration test, with consideration of the OWASP top ten, business logic flaws, information disclosure, and web server infrastructure vulnerabilities.

The final deliverable is a comprehensive report with an executive summary and a list of technical vulnerabilities, prioritized by risk. The vulnerabilities will have recommendations for remediation.

Severity Scoring

Since all the vulnerabilities identified may not have equal severity so in order to prioritize remediation of the penetration test findings, risk ranking is to be assigned for each detected security issue. The Report should clearly document how the severity/risk ranking is derived. Vendor may refer the applicable industry standard or any suitable severity ranking mentioned below: -

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposure (CVE)
- Common Weakness Enumeration (CWE)
- National Vulnerability Database (NVD)

- Open Source Vulnerability Database (OSVDB)
- Bugtraq ID (BID)

In case of custom scoring is adopted during the risk-ranking process, the report should clearly justify with acceptable reasoning for the modification of industry-standard scores and also in case of arriving at a score for a vulnerability that does not have an industry-standard score defined.

Penetration testing tools

Most penetration testers make use of a combination of general-purpose exploit applications such as

Core Impact, Canvas and Metasploit Framework, in addition to their own custom, scripts and applications.

For beginners who want to practice penetration testing, these applications might not be a good choice due to cost involve purchasing them. It should be kept into consideration that the effectiveness of any application commercial or open source is not determined by the price tag, but the skill of the penetration tester. It is a good practice to try all possible applications and tools and decide which one work best for project environment.

We offer a basic functionality of robust commercial Metasploit Express Edition and Metasploit Pro. According to Metasploit's website" Metasploit Community Edition simplifies network discovery and vulnerability verification for specific exploits, increasing the effectiveness of vulnerability scanners". Vulnerability scanners like Nessus and Open- VAS can be easily integrated with Metasploit Framework making it a good choice for penetration testing purpose. The proposed tools following bellow:

a. Metasploit Framework
b. OpenVAS
c. Nessus
d. Acunetix
e. Wp-scan
f. Nmap
g. Sqlmap
h. Netcat
i. Burpsuite
j. Cain and Abel
k. MobSF
l. Drozer
m. Hping

Features and benefits

There are numerous benefits of employing penetration testing.

Detect and arrange security threats

A penetration test (pen test) estimates the ability of an organization to defend its applications, networks, users and endpoints from internal and external attempts to dodge its security controls to achieve privileged or unapproved access to protected assets. Pen test results confirm the threat posed by particular security vulnerabilities or faulty processes, allowing IT management and security experts to arrange remediation efforts. Organizations can more efficiently anticipate emergent security threats and avoid unauthorized access to crucial information and critical systems through executing regular and complete penetration testing.

Meet monitoring necessities and evade penalties

IT departments address the overall auditing/compliance facets of procedures such as HIPAA, SARBANES – OXLEY, and GLBA, and report testing necessities recognized in the federal NIST/FISMA and PCI-DSS commands. The complete reports produced by the penetration tests can assist organizations in evading substantial penalties for non-compliance and let them illustrate ongoing due diligence into assessors by maintaining required security controls to auditors.

Circumvent the rate of network downtime

Recuperating from a security flaw is expensive. Recuperation may include IT remediation efforts, retention programs, and customer protection, legal activities, reduced revenues, dropped employee output and discouraged trade associates. Penetration testing supports an organization to evade these financial setbacks by proactively detecting and addressing threats before security breaches or attacks take place.

Protect customer loyalty and company image

Even a single occurrence of compromised customer data can destroy a company's brand and negatively impact its bottom line. Penetration testing helps an organization avoid data incidents that may put the company's reputation and reliability at stake.

Service disturbances and Security breaches are expensive

Security faults and any associated disruptions in the performance of applications or services may cause debilitating financial harm, damage an organization's reputation, grind down customer loyalties, generate negative press, and incur unanticipated fines and penalties. Frequent employment of penetration testing avoids these expenses by the organization.

Penetration testing helps your organization avoid IT infrastructure invasions. It is better for your business to proactively maintain its security than to face extreme losses, both to its brand equity and to its financial stability.

Our reporting formats

Executive Summary
Brief high-level summary of the penetration test scope and major findings with overall severity graph

Statement of Scope
A detailed definition of the scope of the network and systems tested as part of the engagement, Clarification of Environment vs. non- Environment systems or segments that are considered during the test, Identification of critical systems in or out of the Environment and explanation of why they are included in the test as targets

Review of past threats & vulnerabilities
This will include all the threats & vulnerabilities identified and based on those the vendor would carry out the VAPT again.

Statement of Methodology
Details on the methodologies used to complete the testing (port scanning, nmap etc.)

Limitation
Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, special testing requirements for legacy systems, etc.

Segmentation
Provide details as to the testing methodology and how testing progressed. For example, if the environment did not have any active services, explain what testing was performed to verify restricted access. Document any issues encountered during testing (e.g., interference was encountered as a result of active protection systems blocking traffic).

Summary of test results
Detailed results for vulnerabilities discovered, exploited vulnerabilities and proof of concepts/screenshots, detailed explanations of the implications of findings, business impacts, and risks for each of the identified exposures.

+8801935007700
www.aztechsystemz.com info@aztechsystemz.com
104 Sukrabad, Dhanmondi, Dhaka- 1207, Bangladesh

Recommendations

Remediation recommendations to close the deficiencies identified. Detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies. Security issues that pose an imminent threat to the system are to be reported immediately.

Tools Used

Details of all the tools used and for the purpose & target system and its impact.

Clean up

After testing there may be tasks the tester or customer needs to perform to restore the target environment (i.e., update/removal of test accounts or database entries added or modified during testing, uninstall of test tools or other artifacts, restoring active protectionsystem settings, and/or other activities the tester may not have permissions to perform, etc.). Provide directions on how clean up should be performed and how to verify that security controls have been restored.

Recommendation

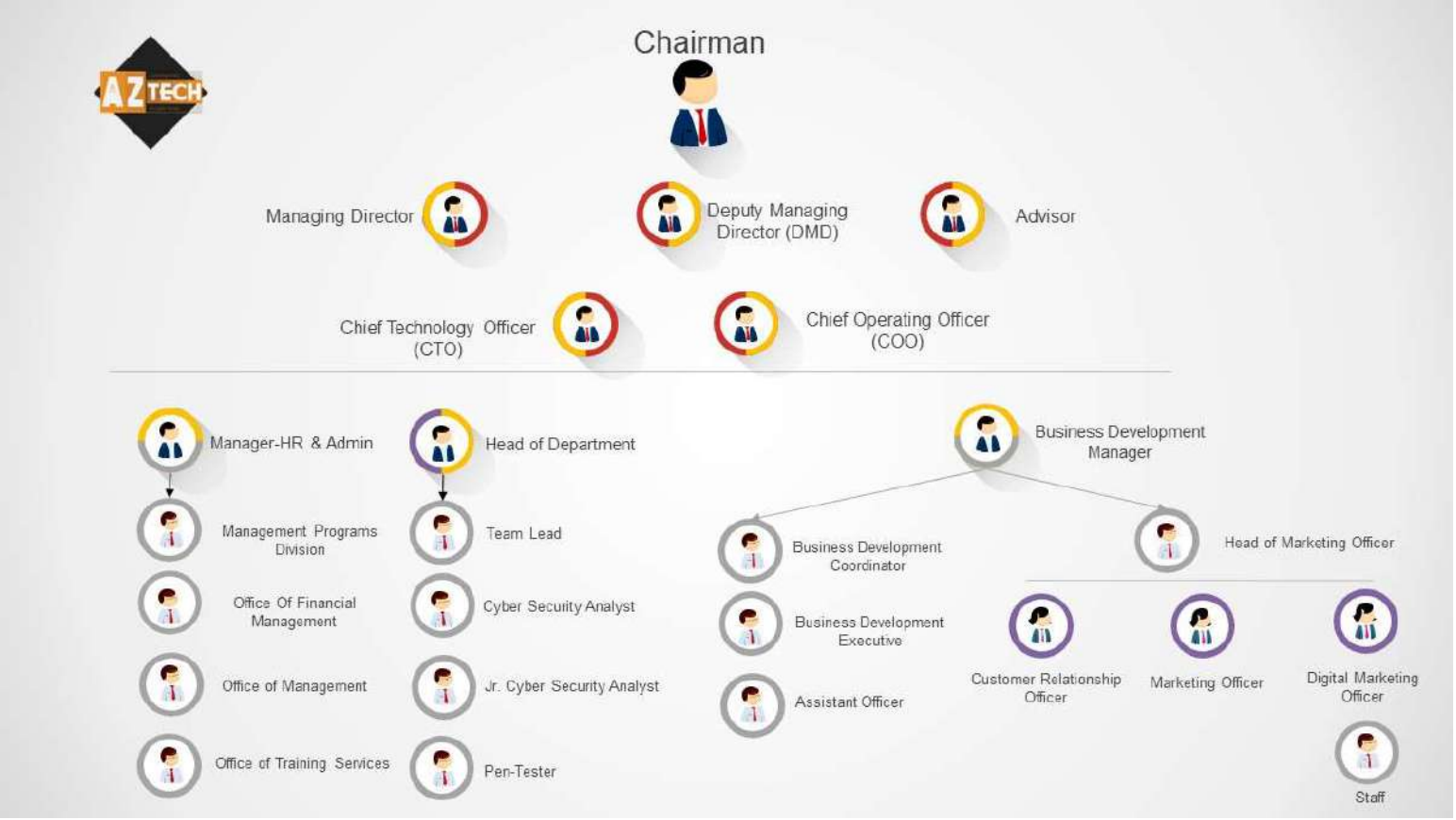
Remediation recommendations to close the deficiencies identified. Detailed steps (wherever/whenever applicable) to be followed while mitigating the reported deficiencies. Security issues that pose an imminent threat to the system are to be reported immediately. In case the primary recommendation is not feasible for NABRD to implement for any reason, vendor would give the alternate recommendations.

Management Development Program

The board Development program is focused on improving and reinforcing the initiative capacities of a worker. This guarantees the advancement of the social abilities of the first-level administrators to streamline their mentality with regards to client the executives. We accept that qualities and trust show an expansion in spirit that makes for a more agreeable and useful work environment. High assurance betters the organization's culture and establishes a climate that representatives appreciate being in and assists them with working better.

A rapidly felt advantage of the board advancement preparing is the improvement of abilities and information in the advancement stages. Building an information base and range of abilities assists with cultivating a motivated group of people in the work environment. The organization places emphasis on directing the meetings as per the divisions. Back to back plans and meetings are led both in-house and to support the workers; the organization conducts out-entryway meetings at the same time.

Organogram


Chairman
Managing Director
Deputy Managing Director (DMD)
Advisor
Chief Technology Officer (CTO)
Chief Operating Officer (COO)
Manager-HR & Admin
Management Programs Division
Office Of Financial Management
Office of Management
Office of Training Services
Head of Department
Team Lead
Cyber Security Analyst
Jr. Cyber Security Analyst
Pen-Tester
Business Development Manager
Business Development Coordinator
Business Development Executive
Assistant Officer
Head of Marketing Officer
Customer Relationship Officer
Marketing Officer
Digital Marketing Officer
Staff

General Information of Legal Status of AZTech Systemz Ltd.

Registration No	C-177898
Registration as Legal Entity	Private Limited Company
Percentage of Ownership	100% Private
Tax Payers Identification Number (TIN)	391277913989/Taxes Circle-316(Company)
BIN	0049889770402
Enlisted with other Organization	Board of Investment (BOI)
Membership/Association	Bangladesh Association of Software Information Service (BASIS) E- Commerce Associate of Bangladesh (e-CAB) Bangladesh Computer Samity (BCS) Board of Investment (BOI)

Contact Information

Contact Person

Dr. Touhid Bhuiyan
Director & COO
E-Mail: touhidbhuiyan@aztechsystemz.com

Office Address

104, Sukrabad, Dhanmondi, Dhaka-1205

Website: www.aztechsystemz.com
E-Mail: info@aztechsystemz.com
Mobile: +8801935007700