CYBERSRC® CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

NETWORK SECURITY TESTING SERVICES

NETWORK SECURITY TESTING SERVICES

OVERVIEW

The Network Vulnerability Assessment and Network Penetration Testing (Network VAPT), is an assessment procedure conducted by security experts on your network to identify possible vulnerabilities that attackers may exploit.

It allows the organization to manage a prioritized list of identified vulnerabilities in their network and understand how to fix them so that they are ensured to be one step ahead of possible attackers. The primary objective of a network VAPT is to identify exploitable security loopholes in systems and network devices so that security vulnerabilities can be fixed before adversaries identify and exploit them.

COMMON VULNERABILITIES FOUND IN NETWORK INFRASTRUCTURE INCLUDE

MALWARE (MALICIOUS SOFTWARE)

Malware is a malicious software that is unknowingly purchased, downloaded, or installed. The use of malware to exploit network vulnerabilities continue to rise hitting an all-time high of 812.67 million infected devices in 2018.Malware is often deployed through phishing emails. In short, threat actors send emails to employees containing links to websites or embed attachments within the email itself. If an action is taken, such as clicking the link or downloading the attachment, the malicious code is executed and you can consider yourself breached.

The most common types of malware include:

- Viruses
- Key loggers
- Worms
- Trojans
- Ransomware
- Logic Bombs
- Bots/Botnets
- Adware & Spyware
- Rootkits

MISCONFIGURED FIREWALLS/ OPERATING SYSTEMS

One of the most significant threats to an organization is exposing your internal network or servers to the internet. When exposed, threat actors are easily able to spy on your traffic, steal data, or compromise your network.

OUTDATED OR UNPATCHED SOFTWARE

Software developers are constantly coming out with new patches to fix bugs and errors to reduce vulnerabilities. Some applications are millions of lines of code long making vulnerabilities an inevitable part of software deployment. As a result, developers deploy patches to software to remediate these vulnerabilities, although patches may also be performance or feature upgrades.

SOCIAL ENGINEERING ATTACKS

Social engineering attacks have become a popular method used by threat actors to easily bypass authentication and authorization security protocols and gain access to a network. These attacks have increased significantly in the last 5 years becoming a lucrative business for hackers. Internal users pose the greatest security risk to an organization typically because they’re uneducated or unaware of the threat. Accidentally downloading an attachment or clicking a link to a website with malicious code can cost thousands in damages.

The most common types of social engineering attacks include:

- Spam
- Pharming
- Tailgating
- Shoulder surfing
- Dumpster diving
- Phishing emails
- Spear phishing
- Whaling
- Vishing

CHALLENGES IN NETWORK PENTESTING

LIMITATION OF TIME

Often, penetration testing is carried out as a time boxed assessment that needs to be completed in a predefined time period. The testing team has to identify potential threats and vulnerabilities, and produce results within this specified time period.

LIMITATION OF SCOPE

Some organizations selectively perform security testing, which means they do not test everything. This may be due to a lack of resources, budget constraints, poor security policies, or other factors. Similarly, penetration testers have limited scope and they often have to leave many parts of the system unchecked because of these constraints.

LIMITATION OF ACCESS

Often the testing team has restricted access to the target environment in a pen test. For example, networks are often divided into segments and the penetration testing has access to only those specific segments that have servers or are accessible from the internet so that the team can simulate a real-work attack. However, such a pen test with limited access will not be able to reveal configuration issues and potential vulnerabilities on its entire network.

OUR DETAILED APPROACH

There are a variety of methodologies used when it comes to effective penetration testing. Some or all of these methodologies may be used depending upon the network system type.

BLACK BOX

A penetration test that is black box is conducted without knowledge of any information related to the technical aspects of a network. This type of test requires penetration testers to conduct comprehensive network exploration in an effort to determine the best way to organize a simulated attack. It is a simulation of a more realistic exploit on a network. This method is used by businesses that want to stay on top of what hackers are capable of doing within a very short period of time.

WHITE BOX

White Box penetration testing occurs when network professionals have gathered all data and information associated with a network and its architecture. This type of pen test is more like an audit and provides a comprehensive approach to security testing. This form of pen testing is used by businesses that want to ensure every single aspect of their network is as secure as possible.

GREY BOX

This approach to penetration testing is performed according to internal information for a network including technical documents, user privilege credentials, and more. Based on the internal information collected, a highly sophisticated network attack can be launched to determine what can happen when hackers gain access to sensitive information. Grey Box pen tests are a common approach that provides detailed security testing that takes place over a shorter period of time than the more involved process of White Box pen tests. These are the main methodologies used in penetration testing. Other network monitoring tests such as intrusion detection, packet sniffing, and other methods are also often deployed to determine the status of network security.

SOME OF THE TOOLS USED

- NMAP
- Nessus
- Metasploit
- Wireshark

BENEFITS OF NETWORK PENTESTING

1 Data Breach Prevention

When a pen test is performed properly and in a benign manner to simulate a network exploit, your business will stay on top of whether or not there are potential security risks within your network. The pen test is very similar to a disaster recovery or fire drill to ensure your business is prepared in the event of a catastrophe.

2 Security Control Testing

Network security professionals are well trained in other security controls used on your business network. The controls include encryption processes, firewalls, data loss prevention, layered security processes, and much more. A network security specialist has the knowledge and expertise to conduct the proper penetration tests to ensure the network security controls are working.

3 Gap Analysis Maintenance

Network security professionals are well trained in other security controls used on your business network. The controls include encryption processes, firewalls, data loss prevention, layered security processes, and much more. A network security specialist has the knowledge and expertise to conduct the proper penetration tests to ensure the network security controls are working.

4 Application Security

Whenever your business implements a new application, it is important to perform a security assessment before putting the application to use in your business environment. If the application's main purpose is to handle sensitive data, it makes perfect sense to have a network security professional perform the security assessment to prevent an inadvertent data breach. This makes the investment in a network security professional more cost effective than if sensitive data such as customer or medical information were to be exposed as a result of a vulnerability in the software application.

5 Compliance

Depending upon your industry, the compliance requirements for data security such as those for the Payment Card Industry (PCI DSS) and others can be very strict. A network security professional can ensure your system remains in compliance with specific standards and requirements for your industry. They can also suggest effective alternatives in the event of there being any issues within your business network.

CASE STUDIES

Background

- Client is one of the leading KPO company
- The client has been in the industry for over 22+ years with a global presence across 50+ countries
- VAPT is important for the organization to know the potential threats in the application which can affect the organization's business.

Objectives

- Assessment of the application and Network for pentesting
- Identify the vulnerabilities
- Identification of the malicious file/ backdoor/ service in Network and safeguard the remaining data and system.
- Expert recommendations and guidance to cover up gaps and improve information security posture

Challenges

- The client did not have any expertise for security testing of Network Infrastructure
- The client lacked required knowledge of tools used for security testing network

Our Role

- Network VAPT for the company's infrastructure which included servers, LT & Desktop and firewall
- Retesting of Network infrastructure
- VAPT reporting and legal advisory

Result/ Benefits

- Successful security testing of Network infrastructure
- Organization gain comprehensive knowledge on the threat action in their network
- Detailed report of VAPT and recommendation with preventive measure
- Consultancy on action items required to cover up identified gaps

Industry Sector

KPO

Service Utilized

Network VAPT

Business Areas Challenges

IT & Technology

HOW CAN CYBERSRC® HELP?

Pen test deliverables include a series of reports that reveal how security issues were identified and confirmed during the test to determine how the issues should be fixed. Once a penetration test has been completed, the report reveals a list of all network vulnerabilities that were discovered during the test. In most cases, the report will also provide recommendations on how to fix the issues.

A typical penetration testing report will include a complete review of the project, the techniques and methodologies used during the test, security risk levels in order of priority, recommendations for fixing the issues, and suggestions for tightening up network security as a whole.

There is also a report for presentation to management which explains in non-technical terms how the risks can affect business continuity and potential financial losses that can be incurred as the result of a breach. This part of the report may also include the IT investments which may be necessary to improve network security.

ABOUT US

CyberSRC® forays into domains of Cyber Security, Data Privacy, Assurance and Governance. Our aim is to assist enterprises, MSMEs, SMEs & others enhance their capabilities for cybersecurity defence, minimise enterprise security and assurance risks, manage security operations and achieve regulatory compliance. Our team consists of several consultants and advisors. We have collaborated with multi-partners in order to provide support for end-to-end security solutions and implementation support.

WHY CYBERSRC®?

We are team of qualified professionals with rich experience of multiple industries such as Manufacturing, BFSI, Insurance, Healthcare, NBFCs & others. Our consultants are industry experts and have proven track records, some of the renowned certificates that our consultants hold such as CISA, CISSP, COBIT, CEH, CCNA, OSCP, ISO 9001 LA/LI, ISO 27001, ITIL LA/LI, PMP, to name a few. We believe in adding value to your business which is enabled through our Centre of Excellence (Coe) and, we have end-to-end capability for Program Build – Operations – Transformation. We have the ability to jump start and execute projects in Managed Services mode globally and flexible delivery models. Our Vision is to be one of the World's most trusted advisory & solution provider for Cyber Security, Data Protection an Assurance practices.

WHAT WE DO

SECURITY ASSESSMENT SERVICES

1. Vulnerability and Penetration Testing Services

- Web Application VA/PT
- Mobile Application VA/PT
- Network Security VA/PT
- Database Security Assessment
- Cloud Security Assessment
- Wireless/WIFI Devices Assessment
- API & Web Services

2. Source Code Review

3. Configuration Review and Hardening Testing

4. Firewall/ Network Devices Security Review

SPECIALISED CYBER SECURITY SERVICES

1. External Threat Intelligence

- Phishing Domain Detection
- Rogue Applications Detection
- Source Code Leaks
- Social Media Abuse
- Brand Abuse
- Dark Web Monitoring
- Take Down support

2. Phishing Campaigns/ Stimulation

- Phishing
- Smishing
- Vishing

3. Incident response & Malware Analysis

4. Forensics Analysis

5. Root Cause Analysis

6. Red Teaming Exercise

7. Honeypot as Service

- Web Attack Mitigation
- Network Attack Mitigation
- Shadow Surveillance

CONSULTING, COMPLIANCE AND & AUDIT SERVICES

1. ISO Compliance

- ISO 27001 ISMS
- ISO 9001 QMS
- ISO 27701 PIMS

2. Information System Assurance & Audit

- **RBI**
  - Payment & Settlement Systems (PSS)
  - NBFC
  - Co-Operative Banks
  - Prepaid Payment Instruments PPI
  - CISA
  - P2P Lending
- **IRDA ISNP**
- **SEBI**
- **AADHAAR**
  - UIDAI AADHAAR
  - ESIGN ASP
- **OTHER**
  - GST SUVIDHA PROVIDER
  - NPCI

3. Regulatory Compliance

- PCI DSS
- SOX
- SOC 1, SOC 2 & SOC 3

4. Privacy Compliance

- General Data Protection
- Regulation (GDPR)
- ISO 27701 PIMS
- California Consumer Privacy Act (CCPA)
- Brazilian General Data Protection Law (LGPD)
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- Singapore Personal Data Protection Act (PDPA)
- Health Insurance Portability and Accountability Act (HIPAA)

5. Risk Management

- Virtual Chief Information Security Officer (V-CISO)
- Third Party Risk Management
- IT Risk Management

CONTACT US

CYBERSRC®
CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

+91 9718933141, 0120-4160448

info@cybersrcc.co

www.cybersrcc.com

Head Office: Unit 605, 6th Floor, World Trade Tower, Sector 16, Noida (UP)- 201301
Other Office:
London (UK): Kemp House 152-160 City Road, London, UK (EC1V 2NX)