



Penetration Testing Services Technical Description

Cyber 51 LTD.

DOCUMENT CLASSIFICATION:

PUBLIC

Copyrighted Material

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distance learning, in any form or by any means such as any information storage, transmission, or retrieval system, without prior written permission from the author.



Table of Contents

NETWORK PENETRATION TEST.....3

WHY? 3

METHODOLOGY 3

Foot printing / Network Mapping 3

Scanning and enumeration..... 4

Vulnerability Analysis..... 7

Exploitation 8

Reporting..... 9

WEB APPLICATION PENETRATION TEST 10

WHY? 10

METHODOLOGY 11

Configuration Management Analysis 11

Analysis of Authentication..... 11

Session Management Analysis 12

Analysis of Authorization..... 12

Data Validation Analysis..... 12

Analysis of Web Services..... 13

Reporting..... 14



Network Penetration Test

Why?

Individuals and businesses enjoy and rely on modern communication methods, collaboration services and benefit from new opportunities the Internet age has created. However, Cyber Crime is on the rise too and has led governments to form complete new authorities to tackle Cyber Warfare and malicious activity. We at Cyber 51 play our part in making the Internet and modern communications a more secure space.

Hackers attack both private and corporate systems on a daily basis. The attacker can be stationed anywhere in the world and needs just internet access and the appropriate tools. The threat is real and it happens thousands of times a day. Many attacks take place undetected and result in the theft and destruction of valuable data.

The solution: Penetration Tests and Network Security Audits. Cyber 51 will, with the legal permission of the network owner, attack customer systems in the same way as a Hacker. In doing so, Cyber 51 is able to expose security holes in the system.

The benefit: The customer is made aware of the Security holes that exist and could be exploited by a hacker with malicious intent to gain unauthorized access to the customer network. In addition, Cyber 51 will prepare a plan of action and, if the customer wishes, implement the closure of these holes.

Methodology

Foot printing / Network Mapping

The process of foot printing is a completely non-intrusive activity performed in order to get the maximum possible information available about the target organization and its systems using various means, both technical as well as non-technical. This involves searching the internet, querying various public repositories ("whois" databases, domain registrars, Usenet groups, mailing lists, etc.).

Also, our Security Testing Consultants will look to obtain as much detail as possible of the current topology and network profile. This can consist of information around IP addressing, gathering public domain information about the business, Ping sweeps, port scanning etc.

This information is then compiled and subsequently analyzed for further areas of investigation.



- **Information Gathering**

- **Expected results**

- Domain names
 - Servers names
 - IP addresses
 - Network Topology
 - Information about ISP
 - Internet presence
 - Company Profile

- **Tasks:**

- Examine and gather information about domain registries.
 - Find IP addresses Blocks
 - Names and locations of DNS servers
 - Use of multiple traces in order to identify systems and devices between.
 - Identify email addresses related to the company.
 - Identify newsgroups, Forums and boards where information related to the company is located.
 - Examine web pages and scripts source codes
 - Examine email headers

Scanning and enumeration

The scanning and enumeration phase will comprise of: identifying live systems, open / filtered ports found, services running on these ports, mapping router / firewall rules, identifying the operating system details, network path discovery, etc.

This phase involves a lot of active probing of the target systems.



After successfully identifying the open ports, services behind them will be fingerprinted, either manually or by using readily available tools. Then, the penetration tester will confirm the exact name and version of the services running on the target system and the underlying Operating System before including the same in the final report.

- **Services identification on systems**

- **Expected Results**

- Ports open, closed and filtered
- IP addresses of live systems
- IP addresses of internal networks
- Asset Services
- Map the Network
- List tunneled and encapsulated protocols discovered
- List supported routing protocols
- Application type and patch level
- Type of operating systems

- **Tasks**

- Collection of responses from network
- Test TTL / fire walking firewall
- Use ICMP and reverse lookup to determine the existence of machines on network
- Use TCP fragments with FIN, NULL and XMAS on ports 21, 22,25,80 and 443 of the hosts found on the network
- Use TCP SYN on ports 21, 22, 25, 80 and 443 of the hosts found on the network.
- Attempt connections on DNS servers



- Use TCP SYN (half open) to list ports that are closed or open filtered all hosts on the network found
 - Use TCP fragments to ports and services available in the host
 - Use UDP packets to list all open ports found on the network host
 - Try to identify the Standard protocols
 - Try to identify non-standard protocols
 - Try to identify encrypted protocols
 - Identify date, time and System Up-Time
 - Identify the predictability of TCP sequence numbers
 - Identify the predictability of TCP sequence number ISN
- **Service identification:**
 - **Expected Results**
 - Type of services
 - Application version and type that offers the service
 - **Tasks**
 - Match each open port with its corresponding service
 - Identify the Server Up-Time and patches applied
 - Identify the application that provides the service through the use of fingerprinting and banners
 - Identify the version of the application
 - Use UDP based services and Trojans attempt to make connections to the services found



- **System Identification:**

- **Expected Results**

- Type of operating system
 - Patch Level
 - Type of system
 - Enumeration System

- **Tasks**

- Examine system responses to determine your operating system
 - Check the prediction of TCP sequence numbers

Vulnerability Analysis

After successfully identifying the target systems and gathering the required details from the above phases, a penetration tester will try to find any possible vulnerabilities existing in each target system.

During this phase a penetration tester will use automated tools to scan the target systems for known vulnerabilities. These tools have their own databases consisting of latest vulnerabilities and their details.

During this phase a penetration tester will also test the systems by supplying invalid inputs, random strings, etc., and check for any errors or unintended behavior in the system output.

By doing so there are many possibilities, the penetration tester may come across unidentified vulnerabilities.

Penetration tester will not rely only on automated tools for this activity



- **Vulnerability testing**

- **Expected Results**

- Type of applications and services listed by vulnerability
 - Patch Level of systems and applications
 - List of vulnerabilities that can cause denial of service
 - List of areas secured by obscurity

- **Tasks**

- Integrate the most popular scanners, hacking tools and exploits in this test
 - Measure the goal with these tools
 - Try to identify vulnerabilities in a system and application type d
 - Perform redundant testing with at least two of the most popular scanners
 - Identify the vulnerabilities of the operating system
 - Identify application vulnerabilities
 - Check the vulnerabilities found by using exploits

Exploitation

During this phase a penetration tester will try to find exploits for the various vulnerabilities found in the previous phase.

Quite often, successful exploitation of vulnerability might not lead to root (administrative) access. In such a scenario additional steps need to be taken, further analysis is required to access the risk, that particular vulnerability may cause to the target system.

Example attack scenarios in this phase include, but aren't limited to:

- buffer overflows
- application or system configuration problems
- modems
- routing issues



- DNS attacks
- address spoofing
- share access and exploitation of inherent system trust relationships.

Potential vulnerabilities will be systematically tested for weakness and overall risk. The strength of captured password files will be tested using password-cracking tools. Individual user account passwords may also be tested using dictionary-based, automated login scripts. In the event that an account is compromised, we will attempt to elevate privileges to that of super user, root, or administrator level.

Our Security Consultants will maintain detailed records of all attempts to exploit vulnerabilities and activities conducted during the attack phase.

Reporting

The last phase in the entire activity is the reporting phase. This phase can occur in parallel to the other three stages or at the end of the Attack stage.

The final report will be prepared keeping in mind both Management as well as Technical aspects, detailing all the findings with proper graphs, figures, etc. so as to convey a proper presentation of the vulnerabilities and it's impact to the business of the target organization.

An executive summary, describing in brief, the activities performed, findings, and high-level recommendations will be provided.

Also detailed technical descriptions of the vulnerabilities and the recommendations to mitigate them will be documented in this report. All the security holes found and exploited will be accompanied with proper Proof-of-Concept by means of screenshots of the successful exploits, or any other such methods.

This report will consist in an Executive report containing, without being limited to: conclusions, recommendations, statistics, and hacking methodology brief, and a Technical Report containing without being limited to: Information Gathering, Network Information, Analysis and Attack results of accomplished tasks.



Web Application Penetration Test

Why?

Web applications have become increasingly vulnerable to different forms of hacker attacks. According to a Gartner Report, 75% of attacks today occur at the application level. A Forrester survey states that “people are now attacking through applications, because it’s easier than through the network layer.”

Despite common use of defenses such as firewalls and intrusion detection or prevention systems, hackers can access valuable proprietary and customer data, shutdown websites and servers and defraud businesses, as well as introduce serious legal liability without being stopped or, in many cases, even detected.

To counteract this problem, Cyber 51 Ltd. offers a comprehensive security risk assessment solution - Web Application Penetration Testing - to identify, analyze and report vulnerabilities in a given application. As part of this service, Cyber 51 Ltd. attempts to identify both inherent and potential security risks that might work as entry points for the hacker. We believe vulnerabilities could be present in a web application due to inadvertent flaws left behind during development, security issues in the underlying environment and misconfigurations in one or more components like database, web server etc.

When conducting a Web Application Penetration Testing assignment, Cyber 51 Ltd. adopts a strong technology and process-based approach supported by a well-documented methodology to identify potential security flaws in the application and underlying environment. Adherence to industry standards such as OWASP, customized tests based on technology and business logic, skilled and certified security engineers, risk assessment on the vulnerabilities found, scoring system based on CVSS (Common Vulnerability Scoring System) make us different from the other vendors in this space.

Customers would benefit from web application penetration testing on the application as it gives an in-depth analysis of your current security posture, recommendations for reducing exposure to currently identified vulnerabilities are highlighted and it allows the customer to make more informed decisions, enabling management of the company’s exposure to threats. The security assessment report submitted on completion of the engagement provides a detailed and prioritized mitigation plan to help customers in addressing security issues in a phased manner.



Methodology

Configuration Management Analysis

The infrastructure used by the Web application will be evaluated from a security perspective.

The tests to be performed are as follows:

- TLS and SSL tests.
- Security Testing over the listener of management system databases.
- Testing the configuration of the infrastructure and its relationship with the Web application, vulnerability analysis, analysis of authentication mechanisms and identification of all the ports used by the Web application.
- Testing the application settings, search through directories and regular files, comments from developers and the eventual acquisition and operational analysis of logs generated by the application.
- Searching for old files, backups, logs of operations and other files used by the Web application.
- Search and test management interfaces or web application related infrastructure.
- Test various HTTP methods supported and the possibilities of XST (Cross-Site Tracing).

Analysis of Authentication

We will evaluate the various mechanisms and aspects of the web application authentication.

The tests to be performed are as follows:

- Credentials management
- Enumeration of users and user accounts easily identifiable.
- Proof of identification credentials brute force, based on information found or inferred.
- Testing the authentication mechanisms looking for evasion
- Logouts mechanisms and weaknesses associated with the Internet browser cache.
- Strength tests over captchas and test multi-factor authentication.



Session Management Analysis

We will evaluate the different mechanisms and management aspects of web application sessions.

The tests to be performed are as follows:

- Session management scheme will be tested.
- CSRF (Cross-Site Request Forgery).
- Test attributes Cookies.
- Setting sessions.
- Evidence of attributes exposed session and repetition.

Analysis of Authorization

We will evaluate the various mechanisms and aspects of web application authorization.

The tests to be performed are as follows:

- Privilege escalation.
- "Path Traversal"
- Evidence of evasion of clearance mechanisms.
- Testing the "business logic" of the Web application, avoiding, altering, or cheating their relationships within the application.

Data Validation Analysis

We will evaluate the various repositories, access and protection mechanisms related to the validation of data used by the Web application.

The tests to be performed are as follows:

- Test various XSS (Cross Site Scripting) and "Cross Site Flashing."
- SQL Injection tests.
- LDAP injection tests.



- Evidence of ORM injection.
- XML Injection tests.
- SSI injection testing.
- Testing XPath Injection.
- Injection Test IMAP / SMTP.
- Evidence Code Injection.
- Injection Test Operating System Commands.
- Evidence of buffer overflow.
- Evidence of Splitting / Smuggling of HTTP.
- Evidence of evasion of clearance mechanisms.
- Evidence of privilege escalation.

Analysis of Web Services

We will evaluate the web application services related to SOA (Service Oriented Architecture):

The tests to be performed are as follows:

- Security testing of WSDL.
- Evidence of structural Security of XML.
- Testing of security at XML content.
- Test HTTP GET parameters / REST.
- Tests with contaminated SOAP attachments.
- Repeat testing of web services.
- Testing AJAX Web application vulnerabilities regarding this technology.



Reporting

The last phase in the entire activity is the reporting phase. This phase can occur in parallel to the other three stages or at the end of the Attack stage.

The final report will be prepared keeping in mind both Management as well as Technical aspects, detailing all the findings with proper graphs, figures, etc. so as to convey a proper presentation of the vulnerabilities and it's impact to the business of the target organization.

An executive summary, describing in brief, the activities performed, findings, and high level recommendations will be provided.

Also detailed technical descriptions of the vulnerabilities and the recommendations to mitigate them will be documented in this report. All the security holes found and exploited will be accompanied with proper Proof-of-Concept by means of screenshots of the successful exploits, or any other such methods.

This report will consist of an Executive report containing, without being limited to: conclusions, recommendations, statistics, and hacking methodology brief, and a Technical Report containing without being limited to: Information Gathering, Network Information, Analysis and Attack results of accomplished tasks.