PALADION
HIGH SPEED CYBER DEFENSE

Paladion's Letter of Opinion

EQ2 Internal Network Security Assessment

Paladion carried out an extensive audit of EQ2 LLC's INTERNAL network and its systems comprising of the 3 IP addresses from the perspective of a remote adversary on Oct 11th, 2017 and on Oct 25th, 2017. This test reveals a remote adversary's view of the network and will help understand security preparedness against evolving threats.

Our assessment results conclude that EQ2 LLC's INTERNAL network assets has been deployed and configured with sufficient security controls implemented to protect against adversaries. Our assessment identified no critical or high-risk findings in the network assets.

Paladion's assessment methodology, tests performed and tools used are presented below.

Methodology

Paladion's approach to network security assessment is a structured 2 step process that requires a high level of manual testing and automated scanning. Each of the steps is discussed below.

Port Scanning And OS & Service Fingerprinting

Scanning can be considered to be a logical extension of Information Gathering. We make use of tools such as network/host scanners, war dialers, etc to locate systems and attempt to discover open ports.

The primary objective in scanning a target network is to identify the IPs that respond to probes and are accessible, the limits of the network, and to assess the perimeter defenses.

Fingerprinting the operating system and services running on a host is important as it provides the scope for determining the vulnerabilities and carrying out further attacks. Discovery of the fingerprints by themselves do not constitute security findings, but they will be used to identify any known vulnerabilities on the targeted host.

Our penetration test focuses on uncovering any vulnerability that an adversary may potentially exploit.

Vulnerability Identification, Validation, And Demonstration

Vulnerability identification is a critical phase in the penetration test process. This phase aims to identify all vulnerabilities on the targeted hosts. This phase makes use of tools such as vulnerability scanners, enumeration tools, etc to discover vulnerabilities on the target hosts. The results of the vulnerability scanners are then manually validated and verified to remove false positives.

In addition, based on the fingerprints of the Operating System and Software identified in the previous phase, we will use vulnerability databases to obtain details of vulnerabilities affecting the platform.

This phase also involves manual testing, which employs various tools that are specific to the services that have been identified as accessible on the target host. These tests are designed to uncover vulnerabilities beyond those discovered by the automated tools. They are also used to demonstrate some of the findings from the automated tools. During the manual testing phase, we attempt to access the network/system through default user accounts and enumerated shares.

Tests Performed

Here's a list of all tests performed on the EQ2 LLC's network and its systems.

1. Bypass Authentication	2. Default Passwords
3. Command Injection	4. Cross Site Scripting
5. Cross Site Tracing	6. Cryptographic Strength Validation
7. Directory Traversal	8. DNS Records
9. Port Scanning	10. Hard Coded Secrets
11. HTML Source Code Analysis	12. LDAP Injection
13. OS Fingerprinting	14. Password Guessing
15. Sensitive Error Messages	16. Server/Service Fingerprinting
17. SNMP Scan	18. SQL Injection
19. SSL Configuration	20. Vulnerable Sample Applications On Server
21. Web Server Vulnerability Scan	22. XPATH Injection

Tool List

Here's the list of tools that we used for the Security Assessment of the Internal network assets.

No.	Tool	Purpose
1.	Burp Suite	Web Application Security Testing Framework
2.	Dnsscan	Finger printing tool for open recursive resolvers
3.	httprint	Web server fingerprinting
4.	Nessus	Automated Network Vulnerability Scanner
5.	Nikto	Web vulnerability scanner
6.	Nmap	Port scanner and Service Fingerprinting Tool
7.	Qualys	Automated Network Vulnerability Scanner
8.	WinHex	Memory Reading tool
9.	Wireshark	Network Sniffer and Packet Analyzer

Additional Support Tools Used

No.	Tool	Purpose
1.	J2SDK and JRE	Java framework needed for many tools to run
2.	Putty	Client used to connect to an SSH server
3.	GreenShot	Used to take quick screenshots using predefined hotkeys
4.	TFTP client	Client used to connect to a tftp server
5.	VNC Client	Client used to connect to a running VNC server
6.	WinSCP	Client used to connect to an FTP/SFTP server

Disclaimer

This letter of opinion is valid for the period during which the assessment was carried out and it's based on the hosted system, and software applications provided by EQ2 LLC. Projection of any conclusions based on our findings for future periods and application versions is subject to the risk that the validity of such conclusions may be altered by the changes made to the application or systems or the failure to make the changes to the system when required.

Balaji Venkatasubramanian
AVP & Delivery Head – Security Testing
Paladion

Head Office: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-703-8713934

Bangalore: +91-80-42543444, **Doha:** +97433559018, **Dubai:** +971-4-2595526, **Kuala Lumpur:** +60-3-7660-4988, **London:** +44(0)2071487475, **Mumbai:** +9102233655151, **Riyadh:** +966(0)114725163, **Virginia:** +1-703-8713934

sales@paladion.net | www.paladion.net