# Vulnerability Assessment & Penetration Testing
# Sample Report

This document is a highly confidential which contains all the information regarding the red team engagement that was done by Infopercept Team on ABC  Company.

# Table of Contents

# Copyright



# Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt Ltd (Infopercept). Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept. Any use you make of the information provided, is at your own risk and liability. Infopercept makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

# Document Authorities

| Company | ABC Corporation Ltd. | | | |
|---|---|---|---|---|
| Document Title | Application Security Audit Report | | | |
| Date | | | | |
| Reference | | | | |
| Scope | Application Security Assessment | | | |
| Classification | Public | Internal | Confidential | Secret |
| Document | Proposal | Deliverable | General | |

## Recipients

| Name | Title | Company |
|---|---|---|
| Mr. XYZ | CIO | ABC Corporation Ltd. |

## Document History

| Date | Version | Prepared by | Status |
|---|---|---|---|
| 15/02/2021 | 1.0 | Consultant 1 | Draft Report |
| 17/02/2021 | 1.1 | Consultant 2 | Final Report |

# Overview

ABC Company Ltd. has appointed Infopercept Consulting Pvt. Ltd. a multidisciplinary company specializing in information security assessments to review its Network, with a perspective of evaluating the effectiveness of the technical controls by following ethical hacking procedures.

The information contained in this report is confidential and is intended only for use by the management of ABC Company Ltd. Outsourcing Services. We are not responsible to any other person/ party or for any decision of such person or party based on this report. It is hereby notified that any reproduction, copying or otherwise quoting of this report or any part thereof except for the purpose mentioned herein above can be done only with our prior written permission.

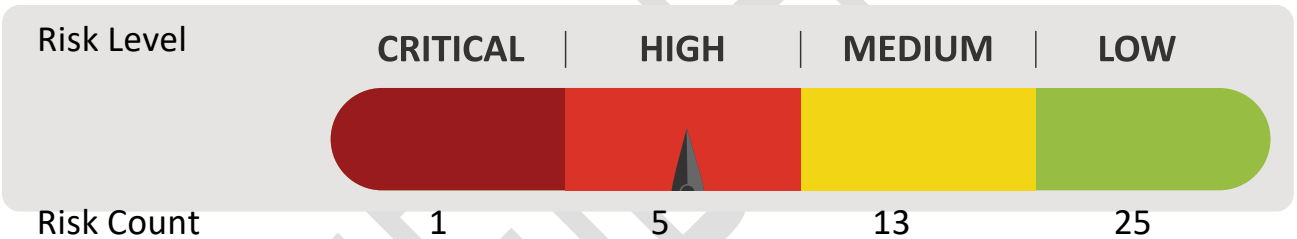
# Sources of Information

We have called for and obtained such data, information etc. as were necessary for the purpose of our assignment which has been made available to us by the management or been found in the public domain.

The information relating to the server details, ip-address, network devices, configuration etc. has been obtained from the Information Technology Team.

# Summary of Findings

The graph below shows a summary of the number of vulnerabilities found for each impact level for the Assessment. A significant number of high impact vulnerabilities were found that should be addressed as a priority.




Total – 44

# 1. Executive Summary

## 1.1 Introduction

Infopercept Cons Pvt. Ltd. conducted an Application Security audit activity for the internal network at ABC Corporation Ltd. The assignment was carried out by Infopercept technical team between the 1st to the 10th of February 2015 with the following goals:

- Identifying security vulnerabilities.
- Providing risk mitigation recommendations for the discovered vulnerabilities.
- Mapping the discovered vulnerabilities to ABC's Information Protection Policy.

This audit report contains:

- The description of the IT Components and its business case
- The security vulnerabilities discovered as a result of the technical application security audit
- The security vulnerabilities discovered as a result of the application process audit
- The risk mitigation strategies that need to be implemented to ensure that the application meets information protection plan (IPP) control compliancy

## 1.2 Scope of The Audit

The vulnerability assessment has been conducted to provide a holistic picture of the securityposture of the systems in the internal network at ABC Company Ltd. Outsourcing Services and with the aim to bring the level of security up to the level of current industry standards.

The following list defines the servers to be scanned for vulnerabilities:

| No. | IP Address | Operating System | Description |
|---|---|---|---|
| 01 | 192.168.10.3 | Windows Server | Terminal Server |
| 02 | 192.168.10.4 | Linux | Eoffice (Webserver) |
| 03 | 192.168.10.6 | Windows Server | HRMS (Webserver) |
| 04 | 192.168.10.7 | Linux | SDUWINDOWS (Development) - Test Server |
| 05 | 192.168.10.11 | Linux | sqlserver (Development) |
| 06 | 192.168.10.12 | Linux | SDU SVN |
| 07 | 192.168.10.13<br>202.137.251.6<br>202.137.251.7 | Windows Server | SDUWINDOWS2 (Webserver) (Development) |
| 08 | 192.168.10.15 | Windows Server | Windows Server (ADS) |
| 09 | 192.168.10.17 | Windows 7 | CADSERVER2 |

The following list defines the network devices to be scanned for vulnerabilities:

| No. | IP Address | Device details | Description |
|---|---|---|---|
| 01 | 172.16.1.31 | Switch | HP L3 Switch |
| 02 | 172.16.1.10<br>202.137.251.3<br>202.137.249.3 | Firewall | Cyber-roam Firewall |
| 03 | 202.137.251.1 | Router | Cisco 2691 Router |

# 2. Report Format

Vulnerability assessment was carried out for each host listed in scope. The discovered vulnerabilities are arranged per host, beginning with the host information followed by the vulnerabilities for that system. Below is a description of how the vulnerabilities per host are listed: -

## HOST Information:

HOST Title – This title shows the scanned host's role and its IP address as shown below

HOST ROLE: X.X.X.X

## Vulnerability Information:

| Compliance of IP Address: | |
|---|---|
| Risk | |
| Abstract | |
| IPMG Control Violation | |
| Reference | |
| Ease of Exploitation | |
| Impact | |
| Recommendations | |

**Vulnerability Title –** A short title that describes the vulnerability. For each vulnerability, the title bar is color coded for a quick identification of the risk level. Title bar color codes are as follows:

Risk Level & Color Code

| |
|---|
| **CRITICAL** |
| **HIGH** |
| **MEDIUM** |
| **LOW** |
| **INFORMATION** |
| **Externally** |

- **Abstract –** Describes the flaw or bugs that cause the vulnerability.
- **IPMG Control Violation –** Provides the ABC IPMG control numbers that are violated.
- **Reference –** Describes the reference for the respective vulnerability found.
- **Ease of Exploitation –** Provides a metric for the skill level required to exploit the vulnerability.

| Metric Skill-level | Metric Skill-level |
|---|---|
| Easy | Casual user |
| Medium | Computer-savvy individual |
| Hard | Determined hacker |

The categories are:

- **Impact –** Describes the possible business impact to ABC if this vulnerability is successfully exploited by an attacker.
- **Recommendation –** Provides solutions or workarounds to mitigate the risk arising from this vulnerability.
- **Proof of Concept –** Screenshots / supporting evidence showing the vulnerability being exploited.

# 3. Vulnerabilities Discovered

## 3.1 CISCO 2691 Router – 202.137.251.1

General Information

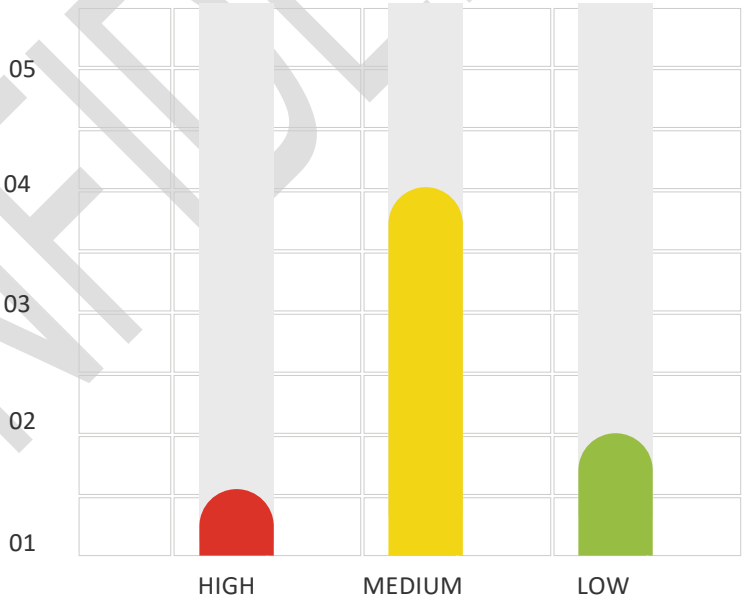
**ABC Company Ltd. have implemented CISCO 2691 Router.**

- Operating System – CISCO IOS 11-15 (identified the same via TCP/IP Fingerprinting Technique)
- The network handle is: ABC COMPANY LTD.
- Network description: ABC Company Ltd., Offshore Outsourcing Unit
- The ISP network handle is: NET-66-198-144-0-1
- ISP Network description: Tata Communications Ltd. PALO-PDI-TATAC

### Vulnerability overview

Below chart summarizes vulnerabilities observed on Cisco Router during assessment.

### Vulnerability overview @ Router



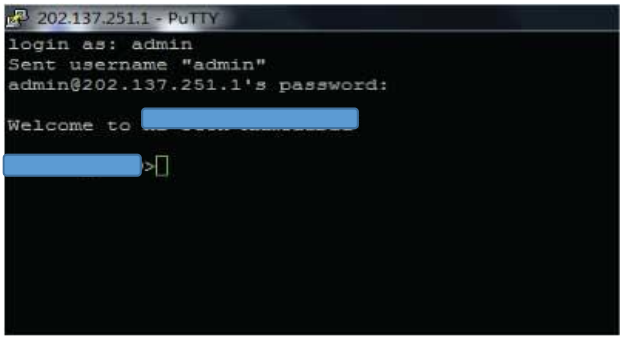

### Open Port Summary

The following summary shows the number of open ports running various services on the terminal server.

| Protocol | Port No | Service | Protocol | Port No | Service |
|---|---|---|---|---|---|
| TCP | 123 | ntp | UDP | | |
| | 161 | snmp | | | |
| | 23 | Telnet | | | |

| 1. Clear Text Telnet Service is enabled on Router | |
|---|---|
| Applicability | TELNET (Cisco) on TCP port 23. |
| Risk | High |
| Abstract | We have observed that clear text telnet service was enabled on routers. Due to vulnerabilities present in clear text telnet service it was possible to have an unauthorized access on Router. |
| Ease of Exploitation | Medium |
| Ease of Exploitation | Hard |
| Impact | Due to the lack of encryption provided by the Telnet protocol, an attacker who is able to monitor a Telnet session would be able to view all of the authentication credentials and data passed in the session. The attacker could then attempt to gain access to the device using the authentication credentials extracted from the session and potentially gain access under the context of that user. Since Telnet is commonly used for network device administration this could gain the attacker an administrative level of access. |
| Recommendations | We recommend that the Telnet service should be disabled. If remote administrative access is required then we recommend that a cryptographically secure alternative, such as SSH, should be used instead. If Telnet has to be used then we recommend that network filtering should be employed to restrict access to the service from only those specific devices that need the access.<br><br>Telnet must be disabled on Cisco Router devices for each transport line that the service is enabled. If supported, the SSH protocol can also be enabled using the same command. This can be configured using the following command: transport input [none \| ssh] |

| 2. UDP Constant IP Identification Field Fingerprinting Vulnerability | |
|---|---|
| Applicability | NA |
| Risk | Medium |
| Abstract | The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system. |
| Reference | CVE-2002-0510 |
| Ease of Exploitation | Medium |
| Impact | Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP<br>Identification field of 0.<br>By exploiting this vulnerability, a malicious user can discover the operating system and approximate kernel version of the host. This information can then be used in further attacks against the host. |
| Recommendations | Please verify the dependency of UDP services and later on recommendation can be provided. |

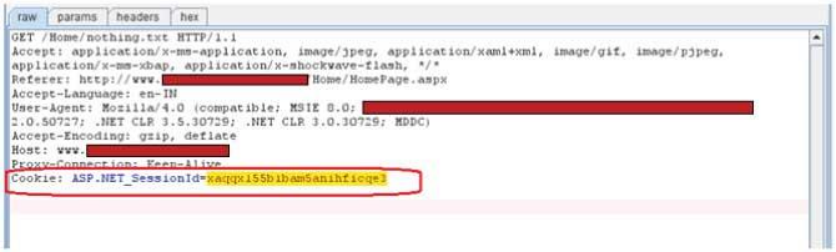



| 3. Remote Management Service Accepting Unencrypted Credentials Detected | |
|---|---|
| Applicability | Telnet on TCP port 23. |
| Risk | Low |
| Abstract | A remote management service that accepts unencrypted credentials was detected on target host. Services like Telnet, FTP, HTTP with basic auth are checked. |
| Reference | Telnet Banner:<br>Welcome to ABC Company Ltd. Ahmedabad<br>User Access Verification<br>Username: |
| Ease of Exploitation | Medium |
| Impact | If an attacker is able to intercept network traffic, he will gain access to the service credentials. |
| Recommendations | Use alternate services that provide encryption if possible. |

| 4. Improper Session Management | |
|---|---|
| Risk | Medium |
| Abstract | Proper authentication and session management is critical to web application security. Flaws in this area most frequently involve the failure to protest credentials and session tokens through their lifecycle. |
| IPMG Control Violation | |
| Reference | http://www.technicalinfo.net/papers/WebBasedSessionManagement.html<br>http://msdn.microsoft.com/enus/library/aa480476.aspx#pagexplained0002_aspnetforms |
| Ease of Exploitation | Low |
| Impact | These flaws can lead to the hijacking of user or administrative accounts, undermine authorization and accountability controls, and cause privacy violations. |
| Recommendations | Regenerate a new session upon successful authentication. Any session token used prior to login should be discarded and only the new token should be assigned for the user till the user logs out. This session token should be properly invalidated when the user logs out. |

## Proof of Concept

enter user ID and password, capture the request using proxy tool. Observe the session token.


| 5. Auto complete feature of the browser | |
|---|---|
| Risk | Medium |
| Abstract | For websites that user frequently visit, user find it helpful to have Firefox or Internet Explorer store commonly entered information such as usernames and passwords, email addresses, phone numbers and more. With the information stored, the web browser will then insert the information into the appropriate fields when completing forms. All mainstream web browsers have a built-in auto complete function. |
| IPMG Control Violation | |
| Reference | http://msdn.microsoft.com/library/default.asp?url=/workshop/author/forms/autocomplete_ovr.asp#security<br>https://community.broadcom.com/home |
| Ease of Exploitation | Low |
| Impact | Password can be steeled from auto complete feature |
| Recommendations | Set autocomplete to OFF.<br>< form autocomplete="off"> - for all form fields,< input autocomplete="off" /><br>- for just one field |

## Proof of Concept

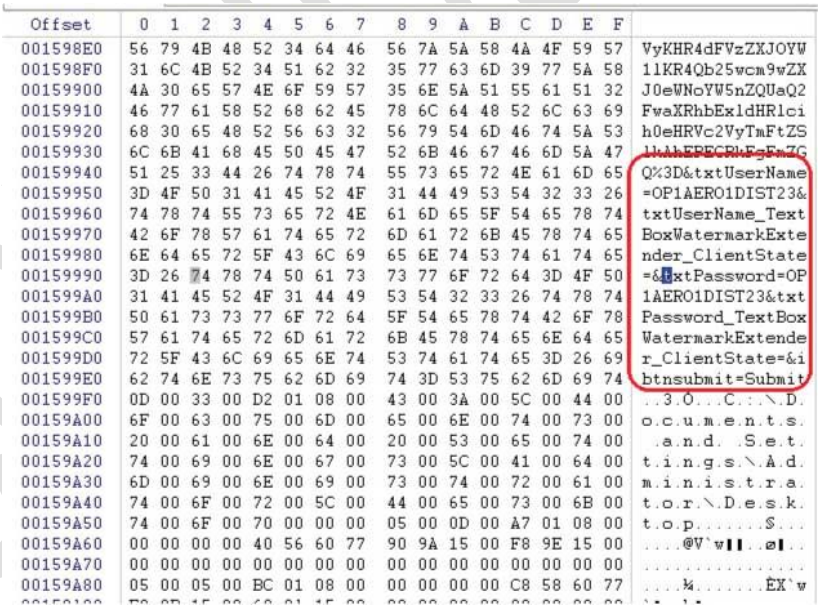
Go to login page enter user credentials and click on submit button. Observe the popup box will appear asking for saving the password.


| 6. Password staying in browser memory |
|---|

| | |
|---|---|
| Risk | Low |
| Abstract | The request on the login page containing the username and password of the user is also stored in the browser's memory. The browser's memory can be read with the use of memory reading tools. In this application the encryption is same every time for a particular password, so if a user left his browser window open after logout, an adversary can steal the password from the memory. |
| IPMG Control Violation | |
| Reference | https://owasp.org/index.php/Cryptography<br>https://owasp.org/index.php/Guide_to_Cryptography |
| Ease of Exploitation | Low |
| Impact | Password can be gained by an attacker |
| Recommendations | The password can be read from the memory if it is being sent in clear text. Using the salted hash technique for password transmission will solve this issue.<br><br>Do not create cryptographic algorithms. Only use approved public algorithms such as AES, RSA public key cryptography, and SHA-256 or better for hashing<br><br>Do not use weak algorithms, such as MD5 / Sha1. Favour safer alternatives, such as SHA-256 or better<br><br>Ensure that encryption is random<br><br>Ensure that encrypted data stored on disk is not easy to decrypt |

## Proof of Concept

Login into the application with valid username and password and browse the application. Now, log out from the application and leave the browser window open. Now Run the browser memory reading tool to read the browser's memory and observe that the username and password is visible in clear text.



| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 001598E0 | 56 | 79 | 4B | 48 | 52 | 34 | 64 | 46 | 56 | 7A | 5A | 58 | 4A | 4F | 59 | 57 | VyKHR4dFVzZXJOYW |
| 001598F0 | 31 | 6C | 4B | 52 | 34 | 51 | 62 | 32 | 35 | 77 | 63 | 6D | 39 | 77 | 5A | 58 | 1lKR4Qb25wcm9wZX |
| 00159900 | 4A | 30 | 65 | 57 | 4E | 6F | 59 | 57 | 35 | 6E | 5A | 51 | 55 | 61 | 51 | 32 | J0eWNoYW5nZQUaQ2 |
| 00159910 | 46 | 77 | 61 | 58 | 52 | 68 | 62 | 45 | 78 | 6C | 64 | 48 | 52 | 6C | 63 | 69 | FwaXRhbExldHRlci |
| 00159920 | 68 | 30 | 65 | 48 | 52 | 56 | 63 | 32 | 56 | 79 | 54 | 6D | 46 | 74 | 5A | 53 | h0eHRVc2VyTmFtZS |
| 00159930 | 6C | 6B | 41 | 68 | 45 | 50 | 45 | 47 | 52 | 6B | 46 | 67 | 46 | 6D | 5A | 47 | lkAhEPEGRkFgFmZG |
| 00159940 | 51 | 25 | 33 | 44 | 26 | 74 | 78 | 74 | 55 | 73 | 65 | 72 | 4E | 61 | 6D | 65 | Q%3D&txtUserName |
| 00159950 | 3D | 4F | 50 | 31 | 41 | 45 | 52 | 4F | 31 | 44 | 49 | 53 | 54 | 32 | 33 | 26 | =OP1AERO1DIST23& |
| 00159960 | 74 | 78 | 74 | 55 | 73 | 65 | 72 | 4E | 61 | 6D | 65 | 5F | 54 | 65 | 78 | 74 | txtUserName_Text |
| 00159970 | 42 | 6F | 78 | 57 | 61 | 74 | 65 | 72 | 6D | 61 | 72 | 6B | 45 | 78 | 74 | 65 | BoxWatermarkExte |
| 00159980 | 6E | 64 | 65 | 72 | 5F | 43 | 6C | 69 | 65 | 6E | 74 | 53 | 74 | 61 | 74 | 65 | nder_ClientState |
| 00159990 | 3D | 26 | 74 | 78 | 74 | 50 | 61 | 73 | 73 | 77 | 6F | 72 | 64 | 3D | 4F | 50 | =&txtPassword=OP |
| 001599A0 | 31 | 41 | 45 | 52 | 4F | 31 | 44 | 49 | 53 | 54 | 32 | 33 | 26 | 74 | 78 | 74 | 1AERO1DIST23&txt |
| 001599B0 | 50 | 61 | 73 | 73 | 77 | 6F | 72 | 64 | 5F | 54 | 65 | 78 | 74 | 42 | 6F | 78 | Password_TextBox |
| 001599C0 | 57 | 61 | 74 | 65 | 72 | 6D | 61 | 72 | 6B | 45 | 78 | 74 | 65 | 6E | 64 | 65 | WatermarkExtende |
| 001599D0 | 72 | 5F | 43 | 6C | 69 | 65 | 6E | 74 | 53 | 74 | 61 | 74 | 65 | 3D | 26 | 69 | r_ClientState=&i |
| 001599E0 | 62 | 74 | 6E | 73 | 75 | 62 | 6D | 69 | 74 | 3D | 53 | 75 | 62 | 6D | 69 | 74 | btnsubmit=Submit |
| 001599F0 | 0D | 00 | 33 | 00 | D2 | 01 | 08 | 00 | 43 | 00 | 3A | 00 | 5C | 00 | 44 | 00 | ..3.Ò...C.:.\.D. |
| 00159A00 | 6F | 00 | 63 | 00 | 75 | 00 | 6D | 00 | 65 | 00 | 6E | 00 | 74 | 00 | 73 | 00 | o.c.u.m.e.n.t.s. |
| 00159A10 | 20 | 00 | 61 | 00 | 6E | 00 | 64 | 00 | 20 | 00 | 53 | 00 | 65 | 00 | 74 | 00 | .a.n.d. .S.e.t. |
| 00159A20 | 74 | 00 | 69 | 00 | 6E | 00 | 67 | 00 | 73 | 00 | 5C | 00 | 41 | 00 | 64 | 00 | t.i.n.g.s.\.A.d. |
| 00159A30 | 6D | 00 | 69 | 00 | 6E | 00 | 69 | 00 | 73 | 00 | 74 | 00 | 72 | 00 | 61 | 00 | m.i.n.i.s.t.r.a. |
| 00159A40 | 74 | 00 | 6F | 00 | 72 | 00 | 5C | 00 | 44 | 00 | 65 | 00 | 73 | 00 | 6B | 00 | t.o.r.\.D.e.s.k. |
| 00159A50 | 74 | 00 | 6F | 00 | 70 | 00 | 00 | 00 | 05 | 00 | 0D | 00 | A7 | 01 | 08 | 00 | t.o.p.....§... |
| 00159A60 | 00 | 00 | 00 | 00 | 40 | 56 | 60 | 77 | 90 | 9A | 15 | 00 | F8 | 9E | 15 | 00 | ....@V`w..ø.. |
| 00159A70 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 00159A80 | 05 | 00 | 05 | 00 | BC | 01 | 08 | 00 | 00 | 00 | 00 | 00 | C8 | 58 | 60 | 77 | ....¼.....ÈX`w |

### Main Report – Servers

# 3.2 Terminal Server – 192.168.0.3

### General Information

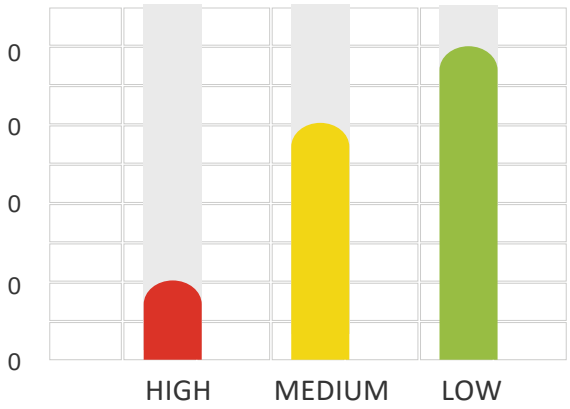
**Terminal server is hosted on windows platform.**

- Operating System: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
- Database Hosted: Microsoft SQL Server 2008 R2 SP1

- FQDN: TERMINALSRV.ABC Company Ltd.os.net
- Ethernet card: 80:c1:6e:62:cf:48: Hewlett Packard

## Vulnerability overview

Below chart summarizes vulnerabilities observed on terminal server during assessment.




## Open Port Summary

The following summary shows the number of open ports running various services on the terminal server.

| Protocol | Port No | Service | Protocol | Port No | Service |
|---|---|---|---|---|---|
| TCP | 80 | http | UDP | | |
| | 135 | Microsoft Windows RPC (epmap) | | | |
| | 139 | netbios-ssn | | | |
| | 389 | LDAP | | | |
| | 443 | ssl/http | | | |
| | 5900 | vnc server | | | |
| | 7080 | web server via TLS V1 | | | |
| | 7444 | | | | |
| | 8443 | | | | |
| | 10443 | | | | |
| | 21100 | | | | |
| | 8080 | | | | |
| | 10000 | | | | |
| | 27354 | | | | |
| | 47001 | Apache Tomcat | | | |
| | 64351 | Backup Agent | | | |

## Vulnerabilities Discovered

| 1. VMware Security Updates for vCenter Server | |
|---|---|
| Applicable to | 192.168.10.3 (tcp/443) |

| | |
|---|---|
| Risk | Critical |
| Abstract | The remote host has a virtualization management application installed that isaffected by multiple vulnerabilities. |
| Reference | CVE CVE-2012-2733<br>CVE CVE-2012-4534<br>CVE CVE-2013-3107 |
| Ease of Exploitation | High |
| Impact | The version of VMware vCenter installed on the remote host is 5.1 prior to update 1. It therefore is potentially affected by the following vulnerabilities:<br>When deployed in an environment that uses Active Directory with anonymous LDAP binding enabled, VMware vCenter doesn't properly handle login credentials. (CVE-2013-3107)<br>The bundled version of Oracle JRE is earlier than 1.6.0_37 and thus, is affected by multiple security issues.<br>The bundled version of Apache Tomcat is affected by multiple issues. (CVE2012-2733, CVE-2012-4534) |
| Recommendations | The workaround is to discontinue the use of AD anonymous LDAP binding if it is enabled in your environment. AD anonymous LDAP binding is not enabled by default. We recommend upgrading VMware vCenter 5.1 update<br>1 or later. |

## 3.3 EOffice (Web) Server – 192.168.0.4

### General Information

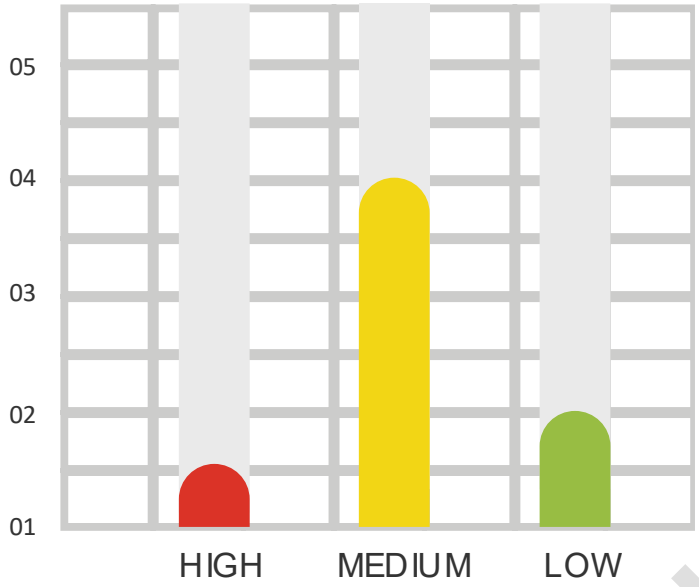
**Terminal server is hosted on linux platform.**

- Operating System: Linux 2.6.9 - 2.6.30
- The remote web server type is : Apache/2.2.0 (Unix) PHP/4.4.2
- The remote host is running a Backup Agent that uses the Network Data Management Protocol (NDMP)
- Remote operating system : KYOCERA Printer Linux Kernel 2.6, Method : SinFP
- SSH version : SSH-1.99-OpenSSH_3.9p1, SSH supported authentication : publickey,gssapi-withmic,password
- The remote web server type is : Apache/2.2.0 (Unix) PHP/4.4.2
- We were able to identify the following PHP version information : Version : 4.4.2, Source : Server: Apache/2.2.0 (Unix) PHP/4.4.2, Source : http://192.168.10.4/ver2/info.php
- MYSQL server information: Version : 4.0.25-log, Protocol : 10 ,Server Status :
- SERVER_STATUS_AUTOCOMMIT Server Capabilities :

    - CLIENT_LONG_FLAG (Get all column flags)
    - CLIENT_CONNECT_WITH_DB (One can specify db on connect)
    - CLIENT_COMPRESS (Can use compression protocol) o CLIENT_TRANSACTIONS (Client knows about transactions)

### Vulnerability overview

Below chart summarizes vulnerabilities observed on terminal server during assessment.




## Open Port Summary

The following summary shows the number of open ports running various services on the web server.

| Protocol | Port No | Service | Protocol | Port No | Service |
|---|---|---|---|---|---|
| TCP | 80 | TCP | UDP | 123 | NTP |
| | 3306 | MYSQL | | 111 | rpcbind |
| | 22 | SSH | | 904 | RPC |
| | 21 | FTP | | | |
| | 111 | sunrpc ONC RPC portmapper | | | |
| | 113 | ident | | | |
| | 199 | smux | | | |
| | 10000 | ndmp | | | |
| | 907 | RPC | | | |

| 1. Linux Multiple statd Packages Remote Format String | |
|---|---|
| Applicable to | 192.168.10.4 (udp/904) |
| Risk | Critical |
| Abstract | The remote service is vulnerable to a buffer overflow. |
| Reference | CVE CVE-2000-0666<br>CVE CVE-2000-0800 |
| Ease of Exploitation | Medium |
| Impact | rpc.statd in the nfs-utils package in various Linux distributions does not properly cleanse untrusted format strings, which allows remote attackers to gain root privileges. The remote statd service could be brought down with a format string attack - it now needs to be restarted manually. This means that an attacker may execute arbitrary code due to a bug in this daemon. |
| Recommendations | Upgrade to the latest version of rpc.statd. |

## Vulnerabilities Discovered

| 2. Apache 2.2 < 2.2.15 Multiple Vulnerabilities |
|---|

| | |
|---|---|
| Applicable to | 192.168.10.4 (tcp/80)<br>Version source: Server: Apache/2.2.0 Installed version : 2.2.0 |
| Risk | Critical |
| Abstract | The remote web server is affected by multiple vulnerabilities. |
| Reference | CVE-2007-6750<br>CVE-2009-3555<br>CVE-2010-0408<br>CVE-2010-0425<br>CVE-2010-0434 |
| Ease of Exploitation | Medium |
| Impact | According to its banner, the version of Apache 2.2 installed on the remote host is older than 2.2.15. Such versions are potentially affected by multiple vulnerabilities:<br><br>A TLS renegotiation prefix injection attack is possible. (CVE-2009-3555)<br>The 'mod_proxy_ajp' module returns the wrong status code if it encounters an error which causes the back-end server to be put into an error state. (CVE-2010-0408)<br>The 'mod_isapi' attempts to unload the 'ISAPI.dll' when it encounters various error states which could leave callbacksin an undefined state. (CVE-2010-0425)<br>A flaw in the core sub-request process code can lead to sensitive information from a request being handled by the wrong thread if a multi-threaded environment is used. (CVE-2010-0434)<br>Added 'mod_reqtimeout' module to mitigate Slowloris attacks. (CVE2007-6750) |
| Recommendations | We would recommend to update the Apache web server |

| 3. MySQL Unsupported Version Detection | |
|---|---|
| Applicable to | 192.168.10.4 (tcp/80)<br>Installed version : 4.0.25-log<br>Supported versions : 5.1.x / 5.5.x<br>End of support date : December 31, 2008 |
| Risk | Critical |
| Abstract | The remote host is running an unsupported version of a database server |
| Reference | https://www.mysql.com/support/supportedplatforms/database.html<br>https://www.mysql.com/support/eol-notice.html |
| Ease of Exploitation | Medium |
| Impact | According to its version, the installation of MySQL on the remote host is no longer supported. As a result, it is likely to contain security vulnerabilities. |
| Recommendations | Upgrade to a version of MySQL that is currently supported. |

| 4. Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow | |
|---|---|
| Applicable to | 192.168.10.4 (tcp/80) |
| Risk | Critical |
| Abstract | The remote web server is affected by buffer overflow vulnerability |
| Reference | CVE-2009-2412<br>OSVDB:56765<br>CWE:189 |
| Ease of Exploitation | Medium |
| Impact | According to its self-reported banner, the version of Apache 2.2 installed on the remote host is older than 2.2.13. As such, it includes a bundled version of the Apache Portable Runtime (APR) library that contains a flaw in 'apr_palloc()' that could cause a heap overflow. |

| | |
|---|---|
| | Note that the Apache HTTP server itself does not pass unsanitized, userprovided sizes to this function so it could only be triggered through some other application that uses it in a vulnerable way. |
| Recommendations | Upgrade to Apache 2.2.13 or later. |

| 5. CGI Generic SQL Injection | |
|---|---|
| Applicable to | 192.168.10.4 (tcp/80) |
| Risk | High |
| Abstract | A web application is potentially vulnerable to SQL injection<br>+ The following resources may be vulnerable to SQL injection :<br>+ The 'clslcUser_userId' parameter of the /ver2/lcForgotPassword.php CGI :<br>/ver2/lcForgotPassword.php [clslcUser_userId='+convert(int,convert(varch ar,0x7b5d))+']<br><br>-------- output --------<br><td width="100%" height="100%" valign="top"><br><!-- HEADER (End) --><br /><br>Fatal error: Error Executing Query: You have an error in your SQ L syntax. Check the manual that corresponds to your MySQL server versio n for the right syntax to use near '\' convert(int,convert(varchar,0x7b5 d)) \'' at line 13 in /home/eoffice/eoffice/ver2/classes/lcConnect.cl s.php on line 79<br /><br>----------<br>/ver2/lcForgotPassword.php [curYear=&curSecond=&curMonth=&clslcUser_user Id='+convert(int, convert(varchar,0x7b5d))+'&clslcUser_returnUrl=lcForgot Password.php&clslcUser_email=&clslcUser_action=&Submit=Submit&curAtt Mark intime=&curAttMarkouttime=&curAttStatus=&curDay=&curHour=&curMinu te=] ---- ---- output --------<br><td width="100%" height="100%" valign="top"><br><!-- HEADER (End) --><br /><br>Fatal error: Error Executing Query: You have an error in your SQ L syntax. Check the manual that corresponds to your MySQL server versio n for the right syntax to use near '\' convert(int,convert(varchar,0x7b5 d)) \'' at line 13 in /home/eoffice/eoffice/ver2/classes/lcConnect.cl s.php on line 79<br /> |
| Reference | CWE:810, 89, 20, 77, 209, 203, 717, 713, 722, 751 & 801 |
| Ease of Exploitation | Medium |
| Impact | By providing specially crafted parameters to CGIs, We were able to get an error from the underlying database. This error suggests that the CGI is affected by SQL injection vulnerability. An attacker may exploit this flaw to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system. |
| Recommendations | Modify the relevant CGIs so that they properly escape arguments |

| 6. HTTP TRACE / TRACK Methods Allowed | |
|---|---|
| Applicable to | 192.168.10.4 (tcp/80) |
| Risk | Medium |
| Abstract | Debugging functions are enabled on the remote web server. |
| Reference | BID 9506<br>BID 9561<br>BID 11604<br>BID 33374<br>BID 37995<br>CVE CVE-2003-1567 |

| | |
|---|---|
| | CVE CVE-2004-2320<br>CVE CVE-2010-0386<br>XREF OSVDB:877<br>XREF OSVDB:3726<br>XREF OSVDB:5648<br>XREF OSVDB:50485<br>XREF CERT:288308<br>XREF CERT:867593<br>XREF CWE:16 |
| Ease of Exploitation | Exploitable with Metasploit |
| Impact | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. |
| Recommendations | Disable these methods. To disable these methods, add the following lines for each virtual host in your configuration file :<br>RewriteEngine on<br>RewriteCond %{REQUEST_METHOD} ^(TRACE\|TRACK)<br>RewriteRule .* - [F]<br>Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive. |

| **7. OpenSSH < 4.2 Multiple Vulnerabilities** | |
|---|---|
| Applicable to | 192.168.10.4 (tcp/22) |
| Risk | Low |
| Abstract | The remote SSH server has multiple vulnerabilities. |
| Reference | BID 14727<br>BID 14729<br>BID 19289<br>CVE CVE-2005-2797<br>CVE CVE-2005-2798<br>CVE CVE-2006-0393<br>XREF OSVDB:19141<br>XREF OSVDB:19142<br>XREF OSVDB:27745 |
| Ease of Exploitation | Hard |
| Impact | According to its banner, the version of OpenSSH installed on the remote host has the following vulnerabilities :<br><br>X11 forwarding may be enabled unintentionally when multiple forwarding requests are made on the same session, or when an X11 listener is orphaned after a session goes away. (CVE-2005-2797)<br><br>GSSAPI credentials may be delegated to users who log in using something other than GSSAPI authentication if 'GSSAPIDelegateCredentials' is enabled.(CVE-2005-2798)<br><br>Attempting to log in as a nonexistent user causes the authentication process to hang, which could be exploited to enumerate valid user accounts. Only OpenSSH on Mac OS X 10.4.x is affected. (CVE-2006-0393)<br><br>Repeatedly attempting to log in as a nonexistent user could result in a denial of service. Only OpenSSH on Mac OS X 10.4.x is affected. (CVE-2006-0393) |
| Recommendations | According to its banner, the version of OpenSSH installed on the remote host has the following vulnerabilities :<br><br>Upgrade to OpenSSH 4.2 or later. For OpenSSH on Mac OS X 10.4.x, apply Mac OS X Security Update 2006-004. |

# 4. Auditor's End Notes

During course of the audit, the auditors identified certain points that could be potential security concerns. As these points relate to the application architecture as a whole, they have not been included as individual vulnerabilities.

This section gives a brief description of each of these points.

## 4.1 Distributed Database Architecture

The architecture of the application relies on a 'distributed database' mechanism, where each CFA has a portion of the database stored locally. All updates are made to this database and then synchronized using the SFTP server as a medium. This raises a few concerns:

- The local databases contain more information than is required for the CFA to do their job.
- There is no automated process for performing synchronization. It is not specified when updates are supposed to be pushed to the server. This can result in disparities in the information available across locations.
- The confidential information in the local databases is completely outside ABC's security control

## 4.2 Client Security

The security of the client infrastructure appears to be very weak. Specifically:

- A large number of the client systems are legacy Windows 98 systems, which do not have adequate security mechanisms at the operating-system level.
- The use of dial-up and regular ISP connections for the synchronization of data results in ABC's data traveling over insecure networks. Despite the use of SSL encryption, this poses a significant risk. The use of a proper VPN solution is recommended.

| No. | Action Item | Responsibility | Time-line | Rating |
|---|---|---|---|---|
| 01 | The application must be modified to validate all user inputs so that only legitimate data can be entered. | | | |
| 02 | The application must ensure that password fields are hidden behind asterisks to prevent involuntary disclosure of the password. | | | |
| 03 | The application should ask the user to enter the old password before being allowed to change it. | | | |



**About Infopercept** - Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

**Imprint**
© Infopercept Consulting Pvt. Ltd.

**Created Date**
Oct 2023

**Contact Detail**
sos@infopercept.com
www.infopercept.com/sample-report