DD/MM/YYYY

INTERNAL VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

hyrrokkin®
WE BUILD BIG BRANDS

contact@hyrrokkin.net | +91-912354-7005

Document Reference

Item	Description
Document Title:	Internal Network Vulnerability Assessment & Penetration Testing Report
Version No:	1.0
Status:	Final
File Name:	ABC_Internal_Network_VAPT_Report_v1.0.pdf
Type:	PDF
Publish Date:	MM/DD/YYYY
Revision Date:	Not Available

Author(s)		
Name	***Functional Section, Department***	***Signature/Date***
Consultant	**Hyrrokkin Lab**	**MM/DD/YYYY**
Reviewed by		
Name	***Functional Section, Department***	***Signature/Date***
Manager	**Hyrrokkin Lab**	**MM/DD/YYYY**
Approved by		
Name	***Functional Section, Department***	***Signature/Date***
Manager	**Hyrrokkin Lab**	**MM/DD/YYYY**

Control Page

Document Amendment Record			
Change No.	**Date**	**Prepared by**	**Brief Explanation**
1.0	**MM/DD/YYYY**	**Consultant**	**Initial Draft**

Table of Contents

1. Introduction

This report details the results of the internal network vulnerability assessment and penetration testing conducted by Hyrrokkin for ABC on their Internal network.

The Hyrrokkin team carried out the vulnerability assessment and penetration testing activities within a restrained environment and time as specified by ABC. The assessment was conducted through remote connection to one of their systems, from DD/MM/YYYY until DD/MM/YYYY. The tests were conducted without any credential that is, taking a black box approach. This simulates the activities of an external attacker launching cyber-attacks. Additionally, all tests performed were non-destructive as required by ABC.

The subsequent sections of this document provide details on vulnerabilities identified, overall impact and recommendation on ABC's network. The detailed technical findings section constitutes identified vulnerabilities with recommendations to mitigate security risks associated with them.

Our opinion provided in this report is valid for the period during which the assessment was carried out and is based on the information provided for the assessment. Projection of any conclusions based on our findings for future periods and application versions are subject to the risk that the validity of such conclusions may be altered because of changes made to the network systems or applications or system or the failure to make the changes to the network systems, application, system when required. Furthermore, the findings in this report reflect the conditions observed during the assessment and do not necessarily reflect current conditions, which may change subsequently.

2. Scope

The Scope of the assessment was to perform below assessments for the following IPs.

Vulnerability Assessment:

S. No.	IP	Operating System	Type
1	192.168.xx.xx	Windows 10 Pro	Desktop
2	192.168.xx.xx	Windows 10 Pro	Desktop
3	192.168.xx.xx	Windows 10 Pro	Desktop
4	192.168.xx.xx	Windows 10 Pro	Desktop
5	192.168.xx.xx	Windows 10 Pro	Desktop
6	192.168.xx.xx	Windows 10 Pro	Desktop
7	192.168.xx.xx	Windows 10 Pro	Desktop
8	192.168.xx.xx	Windows 10 Pro	Desktop
9	192.168.xx.xx	Windows 10 Pro	Desktop
10	192.168.xx.xx	Windows 10 Pro	Desktop
11	192.168.xx.xx	Windows 10 Pro	Desktop

Penetration Testing:

S. No.	IP	Operating System	Type
1	192.168.xx.xx	SonicWALL firewall	Firewall
2	192.168.xx.xx	Windows Server 2012 R2	Domain Controller
3	192.168.xx.xx	Windows Server 2012 R2	Server

The following source IP was used to perform the testing.

S. No.	IP	Operating System
1	192.168.xx.xx	Windows 10 Pro

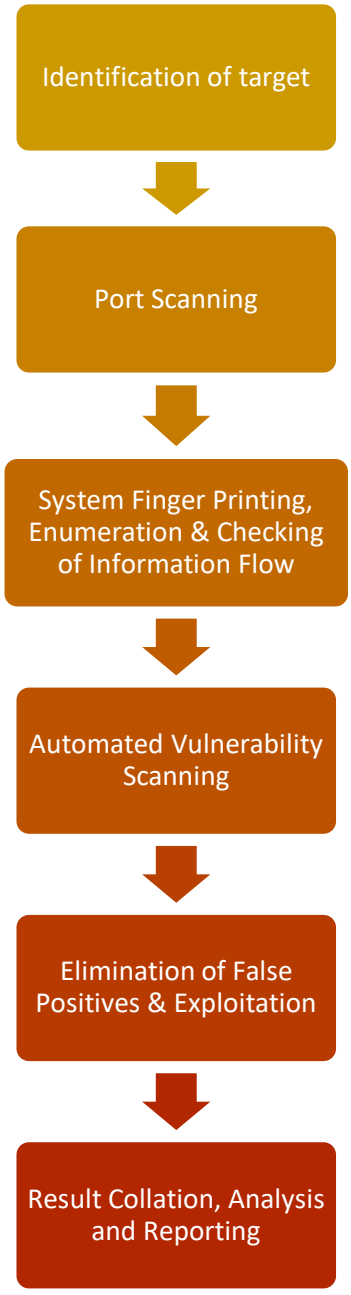
3. Limitations

The penetration testing activities were to be conducted using a black box approach in a fully restricted secure environment. Additionally, all tests performed were non-destructive as required by ABC and no denial-of-service tests were conducted against the application. A time-boxed approach was followed where the activities were carried out within a fixed time frame.

4. Assessment Overview

The assessment provides a point-in-time security analysis and resultant recommendations for improving the security of ABC, its environment and consisted of the following activities.

4.1 Methodology for Network Vulnerability Assessment & Penetration Testing



Identification of Target

The scope as provided by ABC is taken as the target for the penetration testing.

Port Scanning

Port Scanning is one of the most popular reconnaissance techniques used to discover open ports. A variety of scans are used to check for every possible occurrence of open ports.

System Finger Printing, Enumeration & Checking of Information Flow

Various passive and active techniques are used to determine the operating system, services running on the server and their versions. This helps in identifying the OS and the service-related vulnerabilities. It also helps in identifying if any web applications are hosted on the server.

Automated Vulnerability Scanning

Various passive and active techniques are used to determine the operating system, services running on the server and their versions. This helps in identifying the OS and the service-related vulnerabilities.

Eliminating False Positives & Exploitation

Based on the information gathered in the above steps, vulnerabilities and risks are tested. False positives are filtered, and their impacts are considered while rating the vulnerabilities. Exploitable vulnerabilities are exploited to gain access to system level privileges.

Result Collation, Analysis and Reporting

Once the assessment is complete, the results are collated and analyzed to prepare a report. It details the identified the vulnerabilities, risk, mitigation criteria and proof of concept with screen shots of the exploited vulnerability.

5. Risk Rating

Impact	Description
Critical	A security breach that exposes a major security risk with a direct exploit (without user involvement). If exploited, the security threat might cause major damage to the application, network devices, and systems. The likelihood of such an attack occurring is high, considering the /architecture/business-logic/complexity/availability of the exploit.
High	A vulnerability wherein an attacker might have the ability to execute commands on the application, systems or retrieve and modify private information. Security issues are defined as a risk that puts the application, network, and/or data related to the organization in immediate danger.
Medium	Findings indicate a more serious security matter that should be remedied appropriately within a short amount of time which may affect the application, network systems, and data.
Low	Findings usually indicate a minor/informational security risk that does not pose an immediate or Short-term danger. Also, an observational point in certain systems or applications and web servers.

6. Open Ports and Service Enumeration

This phase includes port scanning and service fingerprinting to acquire all possible open port information about the target. The below table provides information on the ports that are open for the servers included in the scope.

Tab 6.1: Open Ports and Service Enumeration

Sr. No	IP Address	Open Ports	Service	Version
1	192.168.xx.xx	135	Msrpc	
		139	netbios-ssn	
		445	microsoft-ds	
		3389	ms-wbt-server	
		5650	Unknown	
		5700	http	
		49664	Msrpc	
		49665	Msrpc	
		49666	Msrpc	
		49667	Msrpc	
		49668	Msrpc	
		49669	Msrpc	
		49670	Msrpc	
		49676	Msrpc	
2	192.168.xx.xx	135	Msrpc	
		139	netbios-ssn	
		445	microsoft-ds	
		3389	ms-wbt-server	
		5650	unknown	
		5700	http	
		49664	msrpc	
		49665	msrpc	
		49666	msrpc	
		49667	msrpc	
		49668	msrpc	
		49674	msrpc	
		49693	msrpc	
		49695	msrpc	
3	192.168.xx.xx	135	msrpc	
		139	netbios-ssn	
		445	microsoft-ds?	
		5040	unknown	

		5650	unknown	
		7680	pando-pub?	
		49664	msrpc	
		49665	msrpc	
		49666	msrpc	
		49668	msrpc	
		49669	msrpc	
		49681	msrpc	
		49687	msrpc	
		49704	msrpc	
		49708	msrpc	
4	192.168.xx.xx	135	msrpc	
		139	netbios-ssn	
		445	microsoft-ds	
		5650	unknown	
		5700	http	
		49664	msrpc	
		49665	msrpc	
		49666	msrpc	
		49667	msrpc	
		49669	msrpc	
		49675	msrpc	
		49679	msrpc	
		49684	msrpc	
		49691	msrpc	
5	192.168.xx.xx	135	msrpc	
		139	netbios-ssn	
		445	microsoft-ds?	
		5040	unknown	
		5357	http	
		5650	unknown	
		7680	pando-pub?	
		49664	msrpc	
		49665	msrpc	
		49666	msrpc	
		49667	msrpc	
		49668	msrpc	
		49669	msrpc	
		49670	msrpc	

7. Summary of Findings

7.1 Vulnerability Statistics

The below graph shows a summary of the number of vulnerabilities found during the assessment performed against different severity level.

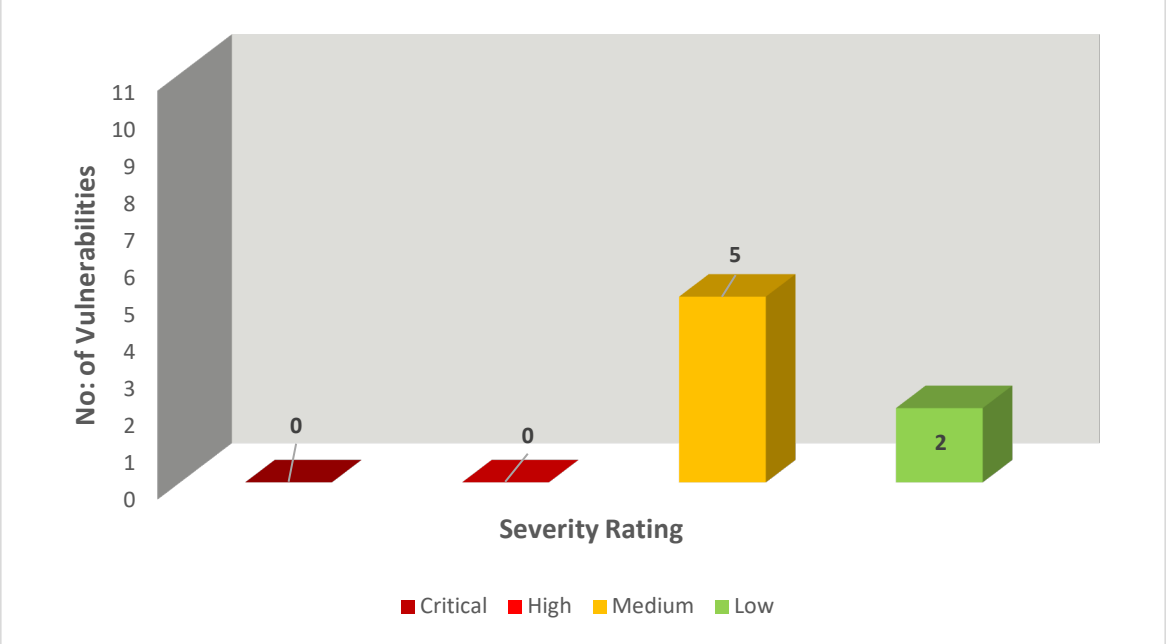


Figure 7.1.1 – Vulnerability assessment statistics

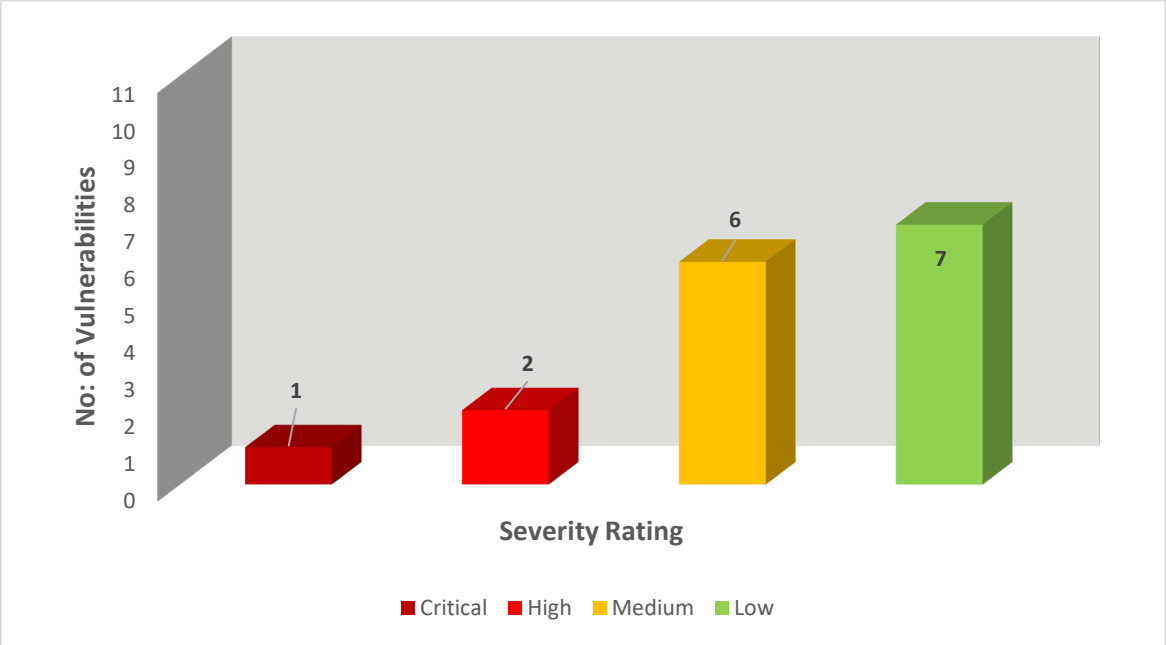


Figure 7.1.2 – Penetration testing statistics

7.2 Technical Vulnerabilities

Technical vulnerabilities discovered during the vulnerability assessment are listed as follows:

S. No.	Technical Vulnerabilities Found	Severity Rating
1	SMB Multiple Information Disclosure Vulnerability	Medium
2	SMB Signing Not Enforced Vulnerability	Medium
3	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	Medium
4	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure (BEAST)	Medium
5	SSL Self-Signed Certificate	Medium
6	Use of Weak RC4 Cipher Vulnerability	Low
7	SSL - LUCKY13 Vulnerability	Low

Technical vulnerabilities discovered during the penetration testing are listed as follows:

S. No.	Technical Vulnerabilities Found	Severity Rating
1	Network Backup Service with Default Credentials	Critical
2	PHP Multiple Vulnerabilities	High
3	Obsolete PHP Version Vulnerability	High
4	SMB Multiple Information Disclosure Vulnerability	Medium
5	SMB Signing Not Enforced Vulnerability	Medium
6	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	Medium
7	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure (BEAST)	Medium
8	SSL Self-Signed Certificate	Medium
9	Vulnerable JavaScript Library	Medium
10	Web Server Information Disclosure Vulnerability	Low
11	Default Page Information Disclosure Vulnerability	Low

S. No.	Technical Vulnerabilities Found	Severity Rating
12	Click-Jacking Vulnerability	Low
13	Unsafe HTTP Methods Enabled	Low
14	Use of Weak RC4 Cipher Vulnerability	Low
15	SSL - LUCKY13 Vulnerability	Low
16	SSL-TLS LogJam Vulnerability	Low

8. Detailed Findings I – Vulnerability Assessment (Desktop Systems)

8.1 SMB Multiple Information Disclosure Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/445) 192.168.xx.xx(TCP/445) 192.168.xx.xx(TCP/445)
Vulnerability	SMB Multiple Information Disclosure Vulnerability
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N CVSS 3.0 Score: 5.4
Identifier	CWE-200: Information Exposure
Description	Adversary found that multiple information disclosure like SMB version, system up time and system physical address are exposed in the SMB.
Impact	Successful exploitation of this vulnerability will aid the attacker in further attack.
Recommendation	It is recommended the following actions to be taken: • Disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing. • Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. • Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. • Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources. • Apply the Principle of Least Privilege to all systems and services.
References	https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

8.2 SMB Signing Not Enforced Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/445) 192.168. xx.xx TCP/445) 192.168. xx.xx (TCP/445)
Vulnerability	SMB Signing Not Enforced Vulnerability
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N CVSS 3.0 Score: 5.4
Identifier	CWE-16: Configuration
Description	Adversary found that signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Impact	Attacker can perform the man-in the-middle attack between the user and SMB server.
Recommendation	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
References	https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-not-required https://www.tenable.com/plugins/nessus/57608

8.3 SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Affected IP(s)	192.168 xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389)
Vulnerability	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CVE-2016-2183
Description	The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers.
Impact	A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Recommendation	It is recommended to reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.
References	https://www.cvedetails.com/cve/CVE-2016-2183/ https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info/ https://wiki.crashtest-security.com/prevent-ssl-lucky13

8.4 SSL/TLS Protocol Initialization Vector Implementation Information Disclosure (BEAST)

Affected IP(s)	192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389)
Vulnerability	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure (BEAST)
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CVE-2011-3389
Description	Adversary found that the target are vulnerable to BEAST Short for Browser Exploit Against SSL/TLS, BEAST is a browser exploit against SSL/TLS. This attack leverages weaknesses in cipher block chaining (CBC) to exploit the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol.
Impact	The CBC vulnerability can enable man-in-the-middle (MITM) attacks against SSL in order to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server.
Recommendation	Disable TLS 1.0 and have users connect using TLS 1.1 or TLS 1.2 protocols which are immune to the BEAST attack.
References	https://www.cvedetails.com/cve/CVE-2011-3389/ https://blog.qualys.com/ssllabs/2011/10/17/mitigating-the-beast-attack-on-tls

8.5 SSL Self-Signed Certificate

Affected IP(s)	192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389)
Vulnerability	SSL Self-Signed Certificate
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CWE-297: Improper Validation of Certificate with Host Mismatch
Description	During the testing it was found out that server is using self-signed SSL certificate. The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Self-signed certificates on internal sites (e.g., employee portals) still result in browser warnings. Many organizations advise employees to simply ignore the warnings, since they know the internal site is safe, but this can encourage dangerous public browsing behavior. Employees accustomed to ignoring warnings on internal sites may be inclined to ignore warnings on public sites as well, leaving them, and your organization, vulnerable to malware and other threats.
Impact	The security warnings associated with self-signed SSL Certificates drive away potential clients for fear that the website does not secure their credentials. Both brand reputation and customer trust are damaged.
Recommendation	It is recommended to purchase or generate a proper SSL certificate for this service from the trusted Certificate Authority.
References	https://www.fastwebhost.in/blog/ssl-self-signed-certificate-warning/

8.6 Use of Weak RC4 Cipher Vulnerability

Affected IP(s)	192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389)
Vulnerability	Use of Weak RC4 Cipher Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 3.7
Identifier	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
Description	It was observed that the application uses RC4 cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
Impact	If plaintext is repeatedly encrypted, and an attacker is able to obtain many ciphertexts, the attacker may be able to derive the plaintext.
Recommendation	The following are recommendations that will mitigate the vulnerability: • Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. • Consider using TLS 1.3 with AES-GCM suites subject to browser and web server support.
References	https://www.acunetix.com/vulnerabilities/web/rc4-cipher-suites-detected/

8.7 SSL - LUCKY13 Vulnerability

Affected IP	192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389) 192.168. xx.xx (TCP/3389)
Vulnerability	SSL - LUCKY13 Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N CVSS 3.0 Score: 2.6
Description	LUCKY13 is a timing attack that can be used against implementations of the TLS protocol using the cipher block chaining mode of operation. The vulnerability affects the TLS 1.1 and 1.2 specifications as well of certain forms of earlier versions. The attack allows a full plaintext recovery for connections made through OpenSSL.
Impact	An attacker can exploit this vulnerability to read the plaintext of a TLS encrypted session. The attack is a more advanced padding oracle which exploits different calculation times depending on the plaintext being padded with one or two bytes or containing an incorrect padding.
Recommendation	Reconfigure the affected application, to avoid the use of CBE cipher suites instead use AEAD cipher suites such as AES-GCM. Alternatively, place limitations on the number of requests be processed over the same TLS connection to mitigate this vulnerability.
References	https://www.cvedetails.com/cve/CVE-2013-0169/

9. Detailed Findings II – Penetration Testing (Firewall & Servers)

9.1 Network Backup Service with Default Credentials

Affected IP(s)	192.168.xx.xx(TCP/4040)
Vulnerability	Network Backup Service With Default Credentials
Severity	Critical
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CVSS 3.0 Score: 8.8
Identifier	CWE-284: Improper Access Control
Description	It's possible to access the XYZ network backup application by using the default credentials. You should change these defaults directly from the XYZ Administration. It is recommended to change the defaults password as soon as possible.
Impact	An attacker can access the backup server to Backup, restore or delete sensitive backup files affecting confidentially, integrity and availability.
Recommendation	It is recommended to set strong password and avoid using default password.
Proof of Concept	Below screenshot shows how adversary connects to the application with default credentials. Figure 9.1.1 – Default password obtained from webpage.  Figure 9.1.2 – Successful login with default password. 

Post Exploitation	Below screenshots shows the post exploitation done on the server. Figure 9.1.3 – Obtained gmail password from SMTP settings.  Figure 9.1.4 – Successful login to gmail.  Figure 9.1.6 – Cloud backup server using the obtained credentials  Figure 9.1.7 – Cloud server containing critical information. 
References	https://www.acunetix.com/vulnerabilities/web/tag/default-credentials/

9.2 PHP Multiple Vulnerabilities

Affected IP(s)	192.168.xx.xx (TCP/4040)
Vulnerability	PHP Multiple Vulnerabilities
Severity	High
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CVSS 3.0 Score: 7.5
Identifier(s)	CVE-2016-10166, CVE-2019-6977, CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024, CVE-2018-19518, CVE-2018-19935, CVE-2018-20783, CVE-2018-5711, CVE-2018-5712
Description	It was found that the target servers use PHP. According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.40. It is, therefore, affected by the following vulnerabilities: - An integer underflow condition exists in _gdContributionsAlloc function in gd_interpolation.c. An unauthenticated, remote attacker can have unspecified impact via vectors related to decrementing the u variable. (CVE-2016-10166) - A heap-based buffer overflow condition exists in gdImageColorMatch due to improper calculation of the allocated buffer size. An attacker can exploit this, via calling imagecolormatch function with crafted image data as parameters. (CVE-2019-6977) - A heap-based buffer over-read exists in the xmlrpc_decode function due to improper validation of input data. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to cause a heap out-of-bounds read or read-after-free condition, which could result in a complete system compromise. (CVE-2019-9020) - A heap-based buffer over-read exists in the PHAR reading functions in the PHAR extension, due to improper implementation of memory operations. An unauthenticated, remote attacker can exploit this, via persuading a user to parse a specially crafted file name on the targeted system, to disclose sensitive information. (CVE-2019-9021) - Multiple heap-based buffer over-read instances exist in mbstring regular expression functions due to improper implementation of memory operations. An unauthenticated, remote attacker can exploit this by sending a specially crafted regular expression that contains multibyte sequences, to cause a condition that could allow the attacker to completely compromise the target system. (CVE-2019-9023)

	- An out-of-bounds read error exists in the xmlrpc_decode function due to improper implementation of memory operations. An unauthenticated, remote attacker can exploit this, via a hostile XMLRPC server to cause PHP to read from memory outside of allocated areas. (CVE-2019-9024) - An arbitrary command injection vulnerability exists in the imap_open function due to improper filters for mailbox names prior to passing them to rsh or ssh commands. An authenticated, remote attacker can exploit this by sending a specially crafted IMAP server name to cause the execution of arbitrary commands on the target system. (CVE-2018-19518) - A denial of service (DoS) vulnerability exists in ext/imap/php_imap.c. An unauthenticated, remote attacker can exploit this issue, via an empty string in the message argument to the imap_mail function, to cause the application to stop responding. (CVE-2018-19935) - A heap buffer over-read exists in the phar_parse_pharfile function. An unauthenticated, remote attacker can exploit this to read allocated or unallocated memory past the actual data when trying to parse a .phar file. (CVE-2018-20783) - A potential infinite loop in gdImageCreateFromGifCtx. (CVE-2018-5711) - A reflected XSS in .phar 404 page exists due to improper validation of user-supplied input before returning it to users. An unauthenticated, remote attacker can exploit this, by convincing a user to click a specially crafted URL, to execute arbitrary script code in a user's browser session. (CVE-2018-5712)
Impact	If exploited successfully an attacker execute remote commands or cause denial of service condition or disclose sensitive information.
Recommendation	Upgrade to PHP version 5.6.40 or later.
Proof of Concept	Below screenshot shows that the target server uses vulnerable PHP version Figure 9.2.1 – Showing the PHP version for 5.6.x 
References	https://www.php.net/eol.php https://www.php.net/ChangeLog-5.php#5.6.39

9.3 Obsolete PHP Version Vulnerability

Affected IP(s)	192.168.xx.xx (TCP/4040)
Vulnerability	Obsolete PHP Version Vulnerability
Severity	High
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CVSS 3.0 Score: 7.5
Identifier	CWE-16: Using Components with Known Vulnerabilities
Description	According to banner, the installed version of the PHP is 5.6.31 which is out dated version and its support was ended by the vendor.
Impact	Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Recommendation	It is recommended to update the PHP to 7.4.5 or the latest one.
Proof of Concept	Below screenshot shows unsupported version of PHP Figure 9.3.1 – Unsupported PHP version 
References	http://php.net/supported-versions.php https://www.php.net/eol.php

9.4 SMB Multiple Information Disclosure Vulnerability

Affected IP(s)	192.168.xx.xx (TCP/445) 192.168.xx.xx (TCP/445)
Vulnerability	SMB Multiple information Disclosure Vulnerability
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N CVSS 3.0 Score: 5.4
Identifier	CWE-200: Information Exposure
Description	Adversary found that multiple information disclosure like SMB version, system up time and system physical address are exposed in the SMB.
Impact	Successful exploitation of this vulnerability will aid the attacker in further attack.
Recommendation	It is recommended the following actions to be taken: • Disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing. • Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. • Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. • Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources. • Apply the Principle of Least Privilege to all systems and services.
Proof of Concept	Below screenshot shows that multiple information obtian from SMB service. Figure 9.4.1 – SMB version one detected.  Figure 9.4.2 – SMB version two detected with system run time.

	 Figure 9.4.3 – SMB host name exposure.  Figure 9.4.4 – netbios information exposure. 
References	https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

9.5 SMB Signing Not Enforced Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/445)
Vulnerability	SMB Signing Not Enforced Vulnerability
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N CVSS 3.0 Score: 5.4
Identifier	CWE-16: Configuration
Description	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
Impact	Attacker can perform the man-in the-middle attack between the user and SMB server.
Recommendation	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
Proof of Concept	Below screenshot shows that SMB signing not required. Figure 9.5.1 – SMB signing disabled in 192.168.xx.xx. 
References	https://www.rapid7.com/db/vulnerabilities/cifs-smb-signing-not-required https://www.tenable.com/plugins/nessus/57608

9.6 SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Affected IP(s)	192.168.xx.xx(TCP/3389) 192.168.xx.xx (TCP/3389)
Vulnerability	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CVE-2016-2183
Description	The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers.
Impact	A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Recommendation	It is recommended to reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.
Proof of Concept	Below screenshot shows that the sweet32 vulnerability exist. Figure 9.6.1 – Image show that server uses 64bit cipher suites on 192.168.xx.xx 
References	https://www.cvedetails.com/cve/CVE-2016-2183/ https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info/ https://wiki.crashtest-security.com/prevent-ssl-lucky13

9.7 SSL/TLS Protocol Initialization Vector Implementation Information Disclosure (BEAST)

Affected IP(s)	192.168.xx.xx (TCP/3389) 192.168.xx.xx (TCP/3389)
Vulnerability	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure (BEAST)
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CVE-2011-3389
Description	Adversary found that the target are vulnerable to BEAST Short for Browser Exploit Against SSL/TLS, BEAST is a browser exploit against SSL/TLS. This attack leverages weaknesses in cipher block chaining (CBC) to exploit the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol.
Impact	The CBC vulnerability can enable man-in-the-middle (MITM) attacks against SSL in order to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server.
Recommendation	Disable TLS 1.0 and have users connect using TLS 1.1 or TLS 1.2 protocols which are immune to the BEAST attack.
Proof of Concept	Below screenshot shows that the beast vulnerability exist. Figure 9.7.1 – Image show that website is vulnerable to beast. 
References	https://www.cvedetails.com/cve/CVE-2011-3389/ https://blog.qualys.com/ssllabs/2011/10/17/mitigating-the-beast-attack-on-tls

9.8 SSL Self-Signed Certificate

Affected IP(s)	192.168.xx.xx (TCP/443) 192.168.xx.xx (TCP/4433) 192.168.xx.xx (TCP/3389) 192.168.xx.xx (TCP/3389)
Vulnerability	SSL Self-Signed Certificate
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CWE-297: Improper Validation of Certificate with Host Mismatch
Description	During the testing it was found out that server is using self-signed SSL certificate. The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Self-signed certificates on internal sites (e.g., employee portals) still result in browser warnings. Many organizations advise employees to simply ignore the warnings, since they know the internal site is safe, but this can encourage dangerous public browsing behavior. Employees accustomed to ignoring warnings on internal sites may be inclined to ignore warnings on public sites as well, leaving them, and your organization, vulnerable to malware and other threats.
Impact	The security warnings associated with self-signed SSL Certificates drive away potential clients for fear that the website does not secure their credentials. Both brand reputation and customer trust are damaged.
Recommendation	It is recommended to purchase or generate a proper SSL certificate for this service from the trusted Certificate Authority.
Proof of Concept	Below screenshot shows that the target is vulnerable to multiple SSL related issue. Figure 9.8.1 – Image show that 192.168.50.1 is vulnerable to multiple SSL related issue.
References	https://www.fastwebhost.in/blog/ssl-self-signed-certificate-warning/

9.9 Vulnerable JavaScript Library

Affected IP(s)	192.168.xx.xx (TCP/4040)
Vulnerability	Vulnerable JavaScript Library Used
Severity	Medium
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 5.3
Identifier	CWE-16: Using Components with Known Vulnerabilities
Description	The server is using a vulnerable JavaScript library. One or more vulnerabilities were reported for this version of the JavaScript library.
Impact	An attacker can exploit vulnerabilities affected by the obsolete JavaScript libraries.
Recommendation	Upgrade jQuery JavaScript library to latest available version.
Proof of Concept	Below screenshot shows that the vulnerable jquery library in use Figure 9.9.1 – Showing vulnerable version jquery usage. 
References	https://jquery.com/download/ https://snyk.io/test/npm/jquery/1.11.1

9.10 Web Server Information Disclosure Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/4040) 192.168.xx.xx(TCP/80)
Vulnerability	Web Server Information Disclosure Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N CVSS 3.0 Score: 2.6
Identifier	CWE-200: Information Exposure
Description	Adversary were able to enumerate the following: • Web Server – IIS, PHP The enumerated versions numbers are: • IIS 8.x • PHP 5.6.xx Information disclosure is when an application fails to properly protect important information from parties that are not supposed to have access to such information in normal circumstances. These types of issues are allowed attackers to gather information which can be used later in the attack lifecycle, in order to achieve more than they could if they didn't get access to such information.
Impact	An attacker exploiting this vulnerability can obtain access to information which may be used to launch further attacks.
Recommendation	The following are recommendations that will mitigate the vulnerability: • The web server does not send out response headers that reveal information about the backend technology type or version. • All the services running on the server's open ports do not reveal information about their builds and versions. • Configure the web server to disallow directory listing and the web application always shows a default web page.
Proof of Concept	Below screenshot shows detailed informations disclosed by server header informations Figure 9.10.1 – PHP version disclosed through server header

	 Figure 9.10.2 – PHP version disclosed through server header 
References	https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/

9.11 Default Page Information Disclosure Vulnerability

Affected URL(s)	192.168.xx.xx(TCP/80)
Vulnerability	Default Page Information Disclosure Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV: N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N CVSS 3.0 Score: 2.6
Identifier	CWE-200: Information Exposure
Description	The target server was found to be having default page or files exposed outside. "Default web page" information disclosure vulnerability is useful to detect unused Web server that are active on a server. The flaw is due to misconfiguration of Server, which allows to access default pages when the server is not used. Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks.
Impact	The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.
Recommendation	Generally, change the name of the default web page for your domain. - For IIS:

Affected URL(s)	192.168.xx.xx(TCP/80)
	• From the Administrative Tools menu, click Internet Information Services (IIS) Manager. • In IIS Manager, click the server name node, and then scroll to locate the Default Document icon. • Double click Default Document. - For Apache: If you have permission to edit the master configuration files Edit the files httpd.conf and srm.conf file and do the following: • Find this line. • DirectoryIndex index.html • and change it as follows: • DirectoryIndex index.shtml index.html Changing The Default Page using .htaccess • If you are unable to edit your master configuration files, you can use this directive from .htaccess. • Just edit the .htaccess file located in your main HTML directory. • If you do not have this file, feel free to create it! • To change the default page, either edit the existingDirectoryIndex line or add the following: DirectoryIndex index.shtml index.html • This will make index.shtml the default page - For Other: Delete or remove the sample pages.
Proof of Concept	Below screenshot shows exposed default page. Figure 9.11.1 – Default page found in 192.168.xx.xx 
References	https://www.valencynetworks.com/kb/web-server-default-welcome-page.html https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_microsoft_iis_default_page

9.12 Click-Jacking Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/80) 192.168.xx.xx(TCP/4040)
Vulnerability	Click-Jacking Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 3.7
Identifier	CWE-693: Protection Mechanism Failure
Description	The server didn't return an X-Frame-Options header which means that the target could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page inside a frame or 'iframe'. Clickjacking happens when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.
Impact	An attacker can trick the authenticated user to perform certain actions in the context of the application and the victim will not be aware of the activities made from his/her account. This attack is usually combined with other attacks like CSRF etc. where the attacker requires an interaction from the user. An attacker can trick victims to click on a vulnerable CSRF link using the Clickjacking vulnerability.
Recommendation	Configure the web server to include an X-Frame-Options header which will prevent the page to be drawn inside an 'iframe' tag. One way to do this is to add the HTTP Response Header manually to every page. A possibly simpler way is to implement a filter that automatically adds the header to every page. There are three possible values for the X-Frame-Options header: • DENY- which any domain from framing the content. • SAMEORGIN - which only allows the current site to frame the content. • ALLOW-FROM uri- which permits the specified 'uri' to frame this page.
Proof of Concept	Below screenshot shows that page is framed in an iframe and is prone to click jacking vulnerability. Figure 9.12.1 – Showing website prone to clickjacking

	
References	https://en.wikipedia.org/wiki/Clickjacking https://www.owasp.org/index.php/Clickjacking https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

9.13 Unsafe HTTP Methods Enabled

Affected IP(s)	192.168.xx.xx(TCP/80) 192.168.xx.xx(TCP/4040)
Vulnerability	Unsafe HTTP Methods Enabled
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 3.7
Identifier	CWE: 749 Exposed Dangerous Method or Function
Description	It was observed that unsafe methods like TRACE or OPTIONS are enabled.
Impact	Having unsafe HTTP methods increases the attack surface. The OPTIONS methods are mainly used for debugging purposes and this method can be used by the attacker to gain additional information
Recommendation	In general, it is recommended to disable unsafe HTTP methods such as TRACE and OPTIONS.
Proof of Concept	Below screenshot shows that HTTP methods such as TRACE or OPTIONS. Figure 9.13.1 – unsafe method enabled on 192.168.xx.xx(80) 

	Figure 9.13.2 – unsafe method enabled on 192.168.xx.xx(4040) 
References	https://www.acunetix.com/vulnerabilities/web/options-method-is-enabled/ https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/options-method-enabled/

9.14 Use of Weak RC4 Cipher Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/3389) 192.168.xx.xx(TCP/3389)
Vulnerability	Use of Weak RC4 Cipher Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 3.7
Identifier	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
Description	It was observed that the application uses RC4 cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
Impact	If plaintext is repeatedly encrypted, and an attacker is able to obtain many ciphertexts, the attacker may be able to derive the plaintext.
Recommendation	The following are recommendations that will mitigate the vulnerability: • Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. • Consider using TLS 1.3 with AES-GCM suites subject to browser and web server support.
Proof of Concept	Below screenshot shows that the server supports rc4 cipher suites Figure 9.14.1 – This image shows that RC4 cipher suite is detected

	
References	https://www.acunetix.com/vulnerabilities/web/rc4-cipher-suites-detected/

9.15 SSL - LUCKY13 Vulnerability

Affected IP	192.168.xx.xx(TCP/443) 192.168.xx.xx (TCP/4433) 192.168.xx.xx (TCP/3389) 192.168.xx.xx (TCP/3389)
Vulnerability	SSL - LUCKY13 Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:N CVSS 3.0 Score: 2.6
Description	LUCKY13 is a timing attack that can be used against implementations of the TLS protocol using the cipher block chaining mode of operation. The vulnerability affects the TLS 1.1 and 1.2 specifications as well of certain forms of earlier versions. The attack allows a full plaintext recovery for connections made through OpenSSL.
Impact	An attacker can exploit this vulnerability to read the plaintext of a TLS encrypted session. The attack is a more advanced padding oracle which exploits different calculation times depending on the plaintext being padded with one or two bytes or containing an incorrect padding.
Recommendation	Reconfigure the affected application, to avoid the use of CBE cipher suites instead use AEAD cipher suites such as AES-GCM. Alternatively, place limitations on the number of requests be processed over the same TLS connection to mitigate this vulnerability.
Proof of Concept	Below screenshot shows that the lucky13 vulnerability exist. Figure 9.15.1 – Image show that website is vulnerable to lucky13.

Affected IP	192.168.xx.xx(TCP/443) 192.168.xx.xx (TCP/4433) 192.168.xx.xx (TCP/3389) 192.168.xx.xx (TCP/3389)
	
References	https://www.cvedetails.com/cve/CVE-2013-0169/

9.16 SSL-TLS LogJam Vulnerability

Affected IP(s)	192.168.xx.xx(TCP/3389) 192.168.xx.xx(TCP/3389)
Vulnerability	SSL-TLS LogJam Vulnerability
Severity	Low
CVSS Score	CVSS 3.0 Metrics: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS 3.0 Score: 3.7
Identifier	CVE-2015-4000
Description	The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection.
Impact	An attacker can exploit this vulnerability to read the plaintext of a TLS encrypted session. The attack is a more advanced padding oracle which exploits different calculation times depending on the plaintext being padded with one or two bytes or containing an incorrect padding.
Recommendation	It is recommended to disable export cipher suites, and instead deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE).
Proof of Concept	Below screenshot shows that the target is vulnerable to LogJam attack. Figure 9.16.1 – Image show that 192.168.xx.xx is vulnerable to LogJam.

	 Figure 9.16.2 – Image show that 192.168.xx.xx is vulnerable to LogJam 
References	https://www.tenable.com/plugins/lce/801945 https://weakdh.org/

10. Conclusion

It is a well-known fact that no organization can claim 100 % security due to ever-changing threat and vulnerability scenarios. New vulnerabilities surface daily and both seasoned and casual attacker can exploit these vulnerabilities to cause serious harm to the organizations.
The vulnerabilities identified if exploited by an attacker may cause:

- Sensitive data leakage or exposure from backup servers.
- Risk of confidentiality, integrity and availability of data.
- Man, in the middle attacks through weak or obsolete SSL encryption.

We recommend that ABC to create a detailed plan for closure of the gaps found during this assessment. The closure plan should be tested before making any changes to the production environment.
We recommend adopting a best practice approach which ensures that all new vulnerabilities are identified in a timely manner and closed before they are exploited by an attacker. This will assist in securing the information of ABC.
We thank ABC for giving us this opportunity and we assure full assistance in securing their information in the long run.