ASSESSMENT - DETAILED REPORT

Client Name: **ABC Inc.**
Partner Name: **XYZ Technology**
Prepared By: **First Last**
Prepared On: **13th April 2020**

Contents

Anti-Spam Configuration Details

Domain Name	SPF	DMARC
@abcinc.com	✓	✗

Dark Web Exposure Details

User Name	Credential	Breach Source	Publish Date
User1@abcinc.com	a6ef6adeebc273bb7dd92daaffb22f49		Sep 26 2019
User2@ abcinc.com	hfjn1	Not Disclosed	Feb 06 2019
User3@abcinc.com	hearts96a	Not Disclosed	Feb 06 2019
User4@abcinc.com	hfjn1	Not Disclosed	Jan 29 2019
User5@abcinc.com	hearts96a	Not Disclosed	Jan 29 2019
User6@abcinc.com	hfjn1	Not Disclosed	Jan 25 2019
User7@abcinc.com	045896ea7ed2c0866cef8ee908681ad4	Not Disclosed	May 10 2018
User8@abcinc.com	hfjn1	Not Disclosed	Dec 22 2017
User9@abcinc.com	smuckers	Not Disclosed	Dec 22 2017
User10@abcinc.com	hfjn1	Not Disclosed	Oct 18 2017
User11@abcinc.com	hearts96a	Not Disclosed	Aug 30 2017
User12@abcinc.com	27feca0e17c0f9e09c326191c3b0498e	last.fm	Oct 25 2016
User13@abcinc.com	3/CS13pZp4M=	adobe.com	Oct 21 2016

CRITICAL HIGH MEDIUM LOW INFO

Endpoint Health Details

Machine Name	IP Address	Machine Type	Operating System	Firewall Protection	Advanced Protection	DNS Protection	Remote Desktop Disabled	Open Vulnerabilities
SERVER1	192.168.16.2	Server	Microsoft Windows Server 2008 R2 Standard	✓	×	×	×	76
DESKTOP1	192.168.2.8	Desktop	Microsoft Windows 10 Pro	✓	×	×	✓	97
DESKTOP2	192.168.11.186	Desktop	Microsoft Windows 10 Pro	✓	×	×	✓	32
DESKTOP3	192.168.16.6	Desktop	Microsoft Windows 10 Pro	🔍	🔍	🔍	🔍	102
DESKTOP4	192.168.16.248	Desktop	Microsoft Windows 10 Pro	✓	×	×	✓	0
DESKTOP5	192.168.2.96	Desktop	Microsoft Windows 10 Pro	✓	×	×	✓	45
DESKTOP6	192.168.254.10	Desktop	Microsoft Windows 10 Pro	🔍	🔍	🔍	🔍	22
DESKTOP7	192.168.2.6	Desktop	Microsoft Windows 10 Pro	✓	×	×	✓	0

🔍 Could not be determined/scanned/found.

Users with Possible Policy Violations Details*

User Name	User Role	Last Login Timestamp	Password Required	Password Changeable	Password Complexity Enabled	Password Expiring in Less than 90 Days	Remote Desktop Access Enabled
SERVER1\server1	Administrator	N/A	✓	✓	×	✓	✓
SERVER1\user1	Guest	04/07/2020 9:18:45 PM	✓	×	×	✓	✓
DESKTOP1\user2	User	04/06/2020 7:53:48 PM	✓	✓	×	×	✓
DESKTOP3\user3	Administrator	N/A	✓	✓	×	✓	✓
SERVER1\user4	Administrator	04/08/2020 8:57:14 PM	✓	✓	×	×	✓
DESKTOP4\user5	Administrator	02/17/2020 2:35:51 AM	✓	✓	×	×	✓
SERVER1\user6	Administrator	06/12/2019 4:18:15 PM	✓	✓	×	✓	✓

User Name	User Role	Last Login Timestamp	Password Required	Password Changeable	Password Complexity Enabled	Password Expiring in Less than 90 Days	Remote Desktop Access Enabled
SERVER1\user7	Administrator	12/06/2019 12:56:39 AM	✓	✓	×	✓	✓
DESKTOP5\user16	User	N/A	✓	✓	×	✓	✓
DESKTOP6\user17	User	06/13/2019 6:53:22 PM	✓	×	×	✓	✓
SERVER1\user8	Administrator	11/21/2018 8:00:54 PM	✓	✓	×	×	✓
SERVER1\user9	User	04/02/2020 9:23:36 PM	✓	×	×	✓	✓
SERVER1\user10	User	03/23/2020 1:25:34 PM	✓	✓	×	✓	✓
SERVER1\user11	User	N/A	×	×	×	✓	✓
SERVER1\user12	Administrator	04/02/2020 7:46:43 PM	✓	✓	×	✓	✓
DESKTOP7\user18	User	06/14/2019 1:07:37 PM	✓	✓	×	✓	✓
SERVER1\user13	User	03/27/2020 8:25:34 PM	✓	×	×	✓	✓
DESKTOP3\user20	Administrator	01/07/2020 4:48:51 AM	×	✓	✓	✓	✓

*** If the Domain Controller is not part of the IP range scanned, the report may not contain information of all the Domain Users.**

User Login Details*

User Name	User Role	Last Login Timestamp	Last Login Status
SERVER1\server1	Administrator	N/A	Never
SERVER1\user1	Administrator	N/A	Never
DESKTOP1\user2	User	N/A	Never
SERVER1\user3	User	N/A	Never
SERVER1\user4	User	03/06/1970 11:23:47 AM	90+ Days
SERVER1\user5	Administrator	11/21/2018 8:00:54 PM	90+ Days
DESKTOP2\user6	Administrator	03/03/2019 11:56:23 PM	90+ Days
DESKTOP3\user7	Administrator	06/12/2019 4:18:15 PM	90+ Days
DESKTOP3\user8	User	06/13/2019 6:53:22 PM	90+ Days
DESKTOP4\user9	User	06/14/2019 1:07:37 PM	90+ Days

User Name	User Role	Last Login Timestamp	Last Login Status
DESKTOP5\user10	User	06/14/2019 9:25:03 PM	90+ Days
DESKTOP6\user11	User	07/30/2019 2:24:38 PM	60 - 90 Days
DESKTOP6\user12	Administrator	11/04/2019 8:31:44 PM	60 - 90 Days
DESKTOP7\user13	Administrator	11/05/2019 12:33:12 AM	30 - 60 Days

*** If the Domain Controller is not part of the IP range scanned, the report may not contain information of all the Domain Users.**

Endpoint Hygiene/Asset Details

Machine Name	IP Address	Machine Type	Operating System	Missing Patches	Basic AV Protection	Backup Configured	OS Up-to-Date	Asset Age	HDD Space Utilized
SERVER1	192.168.16.2	Server	Microsoft Windows Server 2008 R2 Standard	3	✓	×	×	2.3 Years	39%
DESKTOP1	192.168.2.8	Desktop	Microsoft Windows 10 Pro	5	✓	×	✓	5.1 Years	91%
DESKTOP2	192.168.11.186	Desktop	Microsoft Windows 10 Pro	2	✓	×	✓	2.7 Years	27%
DESKTOP3	192.168.16.6	Desktop	Microsoft Windows 10 Pro	0	✓	×	✓	1.9 Years	87%
DESKTOP4	192.168.16.248	Desktop	Microsoft Windows 10 Pro	1	✓	×	✓	4.4 Years	46%
DESKTOP5	192.168.2.96	Desktop	Microsoft Windows 10 Pro	0	🔍	🔍	✓	6.8 Years	45%
DESKTOP6	192.168.254.10	Desktop	Microsoft Windows 10 Pro	8	✓	🔍	✓	3.6 Years	59%
DESKTOP7	192.168.2.6	Desktop	Microsoft Windows 10 Pro	13	✓	×	✓	2.3 Years	75%

🔍 Could not be determined/scanned/found.

Open Vulnerability Details

CVE ID	Vulnerability Name/Description	CVSS Score (Risk Level)	Impacted Endpoints	Deprecated?	References
CVE-2010-3782	obs-server before 1.7.7 allows logins by 'unconfirmed' accounts due to a bug in the REST api implementation.	8.8 (HIGH)	SERVER1, DESKTOP2	-	http://lists.opensuse.org/opensuse-security-announce/2011-02/msg00001.html
CVE-2013-7486	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev27 and 7.4.x before 7.4.0-rev20 allows remote attackers to inject arbitrary web script or HTML via the body of an email. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	6.1 (MEDIUM)	SERVER1, DESKTOP1, DESKTOP7	-	http://packetstormsecurity.com/files/124185/Open-Xchange-frontend6-6.22.4-backend-7.4.0-Cross-Site-Scripting.html http://seclists.org/bugtraq/2013/Nov/127 http://www.securitytracker.com/id/1029394
CVE-2014-0104	In fence-agents before 4.0.17 does not verify remote SSL certificates in the fence_cisco_ucs.py script which can potentially allow for man-in-the-middle attackers to spoof SSL servers via arbitrary SSL certificates.	5.9 (MEDIUM)	DESKTOP2, DESKTOP5, DESKTOP7	-	https://access.redhat.com/security/cve/cve-2014-0104 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-0104 https://bugzilla.suse.com/show_bug.cgi?id=CVE-2014-0104 https://security-tracker.debian.org/tracker/CVE-2014-0104
CVE-2013-3945	The MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a nband tag.	7.8 (HIGH)	DESKTOP7	Yes	https://exchange.xforce.ibmcloud.com/vulnerabilities/89805 https://www.irfanview.com/history_old.htm

Missing Patch Details

Patch Name/Description	Patch Classification?	Patch Severity	Application Name	Impacted Endpoints	Reboot Required?
Security Update for Windows Server 2008 R2 x64 Edition (KB2585542)	Security Update	Critical	Windows Server 2008 R2	SERVER1, DESKTOP2	Yes
Security Update for Windows 10 Pro x64 Edition (KB2585543)	Security Update	Critical	Windows 10 Pro	SERVER1, DESKTOP1, DESKTOP7	Yes
Security Update for Windows 7 x64 Edition (KB2585544)	Update	High	Windows 7	DESKTOP2, DESKTOP5, DESKTOP7	No
Google Chrome not up-to-date	Other	Not Applicable	Google Chrome	DESKTOP7	Not Applicable