RED TEAMING EXERCISE

2022 | FINAL REPORT

PREPARED BY

CryptoGen Nepal

PREPARED FOR

[redacted]

Confidentiality

In no event shall Cryptogen Nepal be liable to anyone for special, incidental, collateral or consequential damages arising out of the use of this information.

This document contains information, which is confidential and proprietary to Cryptogen Nepal and [redacted] Extreme care should be exercised before distributing copies of this document, or the extracted contents of this document. Cryptogen Nepal is authorizing our point of contact at [redacted] to view and disseminate this document as he/she sees fit in accordance with [redacted] data handling policy and procedures. This document should be marked "[redacted]" and therefore we suggest that this document be disseminated on a "need to know" basis. Address questions regarding the proper and legitimate use of this document to:

CryptoGen Nepal Pvt. Ltd.
Naag Pokhari, Naxal Kathmandu

Disclaimer

The information presented in this document is provided as is and without warranty. Red Teaming Exercise is a "point in time" analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks, and applications.

Document Control

Document Name	Report of Red Teaming Exercise of [redacted]
Security Classification	Confidential
Location	[redacted] Kathmandu 44600

Authorization		
Document Owner	Reviewed by	Authorized by
CryptoGen Nepal	[redacted]	Nirmal Dahal

Amendment Log				
Version	Modification Date	Section	Amendment/ Modification/ Deletion	Brief description of the change
1.0		NIL	NIL	Final Report

Red Team Operators	
Name	Designation
Nirmal Dahal	Chief Technology Officer
[redacted]	Offensive Security Team Lead
[redacted]	Security Analyst

Table of Contents

Introduction

Organizations must today be able to withstand the most recent and advanced cyber-attacks. With the support of a certified and professional Red Teaming Provider, the Red Teaming Assessment is designed to prepare and execute controlled attacks (i.e., threat intelligence based red teaming tests) against the live/production environment without exposing important information.

Red Teaming should not be mistaken as an information system audit or a penetration test as it is a simulation test designed to provide insight into the resilience and efficacy of the implemented cyber security measures and related processes (i.e., detection and response). In contrast to a penetration test (which tests and evaluates one or more specific information assets), red teaming exercise focuses on simulating a targeted and realistic attack against the entire Organization in a controlled manner.

Cryptogen Nepal used the latest attack tactics, techniques, and procedures to compromise the [redacted] aiming to reach the most important and valuable information assets and to test the detection and response capabilities of the [redacted]. The Red Team consists of certified and experienced ethical hackers with in-depth knowledge of all security domains.

Cryptogen Nepal performed a detailed security examination of [redacted] performing Red Teaming Exercise engagement to identify the detection and response capability of Blue Team. The assessment was initiated from 14th June 2022 to 11th July 2022, to identify and fill the security gaps within the infrastructure within [redacted]. As a part of assessment, we created some of the potential targets to perform attack against to identify the vulnerable point.

Summary

Red Team engagements performed by CryptoGen Nepal employs the real-world adversary techniques to target the systems under test. We used 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, 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 analyzing 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.

Throughout the Red Team Assessment Exercise, we observed multiple vulnerabilities that can be chained and exploited to obtain access to the organization. Some of the critical identified vulnerabilities are:

- Weak/ Default Credentials
- OSINT leading to gather employee information via LinkedIn
- Improper network/VLAN segregation
- Weak log processing and handling
- Delay in response of the Blue Team
- Peoples vulnerable to social engineering
- Weak credential handling

High-Level Recommendation

- Change the default credentials and enforce use of complex password
- Implement the proper network segregation with VLAN
- Implement the proper logging solution and don't rely on alerts
- Share credentials in secure manner
- Never leave any ports open if not in use
- Provide user-awareness and training

Scope

The agreed scope included in the Red Team Exercise Assessment but not limited to:

- Physical Infrastructure
- Networks
- Servers
- Peoples
- Endpoint with an IP Address

Control Framework

During the phase of red team assessments, the following industry and regulatory based frameworks was followed:

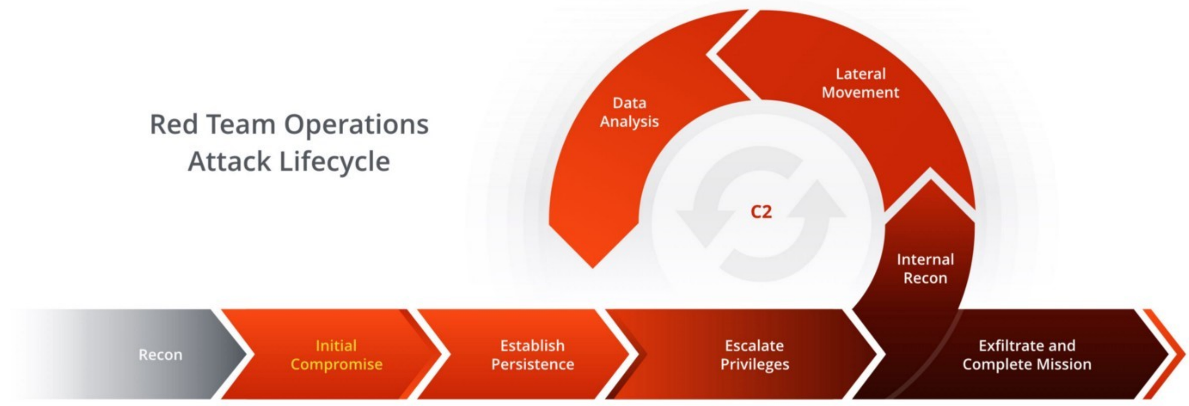
- MITRE ATT&CK Framework.
- Cyber Kill Chain® – Lockheed Martin
- Unified Cyber Kill Chain – Paul Pols
- Purple Team Exercise Framework (PTEF)
- Cyber Operational Resilience Intelligence-led Exercises (CORIE)
- CBEST Intelligence Led Testing – Bank of England

To be specific, the Unified Cyber Kill Chain – Paul Pols was followed during the assessment.

Execution Methodology

Planning objectives

The planning objectives phase is most important phase of the red team assessments. Based on the given scope, and the goal required by the client, we prepared the objectives to act on with a lot of planning to meet the required goals and launch a proper simulated red team attack.



The involved phases during the assessment are:

Initial Reconnaissance

Initial reconnaissance is the process to gather the much possible information about the target. In this phase, we mapped different assets of the target to gain the information using the open-source intelligence gathering (OSINT) techniques.

Initial Compromise

In this Initial Compromise phase, we gained the initial foothold to the organization assets the vulnerability in the assets chaining multiple vulnerabilities altogether. This phase was the major starting point to go further in the internal infrastructure of the organization.

Privilege Escalation

In this phase, we tried to escalate the privilege of their current users to higher level. Getting higher level privilege helped to gain information of the internal network and stable the original initial foothold and was done by identifying the misconfiguration and exploiting it, trying escalation scripts, setting up valid remote logins and many more.

Internal Reconnaissance

In the phase, with the stable foothold and privilege we performed the active reconnaissance on the internal infrastructure of the organization such as Active directory environment, VLANs, firewalls, workstations, restricted areas and many more and started to move laterally on the internal infrastructure.

Compromise

In this phase, we tried to compromise every possible asset in the organization infrastructure. As per the set goals, we exfiltrated the data, perform command and control (C2) activity, physical compromise, etc.

Persistence

In this phase, we used the techniques to keep access to the compromised systems across restarts, credentials changed, intrusion detection that may cause to terminate the compromised system access via obfuscated C2 payloads, advanced scripts and so on. Also, this phase observed the overall detection & response capability of the security team of the organization throughout the red team assessment phase.

Documentation and Reporting

In this phase documentation is created based on findings, used techniques, required goals and the overall attack simulation process & clear report is prepared and provided to the stake holders. Also, debriefing is to be delivered for the clear insights.

Approach and Findings

Physical Security

We were able to get inside by opening the access control door with the door remote available at the reception door. We pasted the 'Red Team' sticker within the table to show our presence.

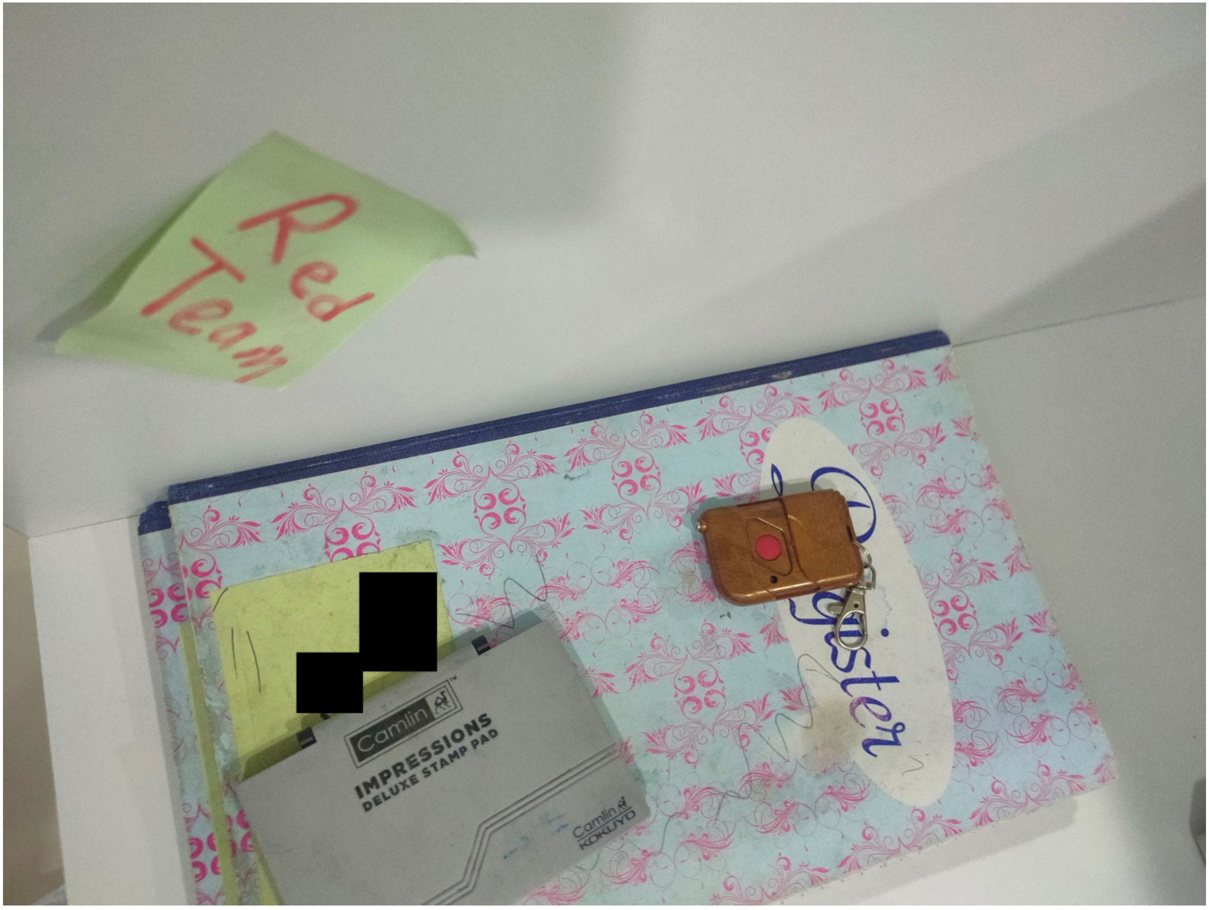


Figure 1: Accessing door with door remote

Also, we were able to enter the server room using the card of one of the [redacted] staff without interruption. We were not asked any queries on why we entered and what was the purpose of the visit. Also, the surveillance camera was not found inside the server room and visitor log is not maintained.

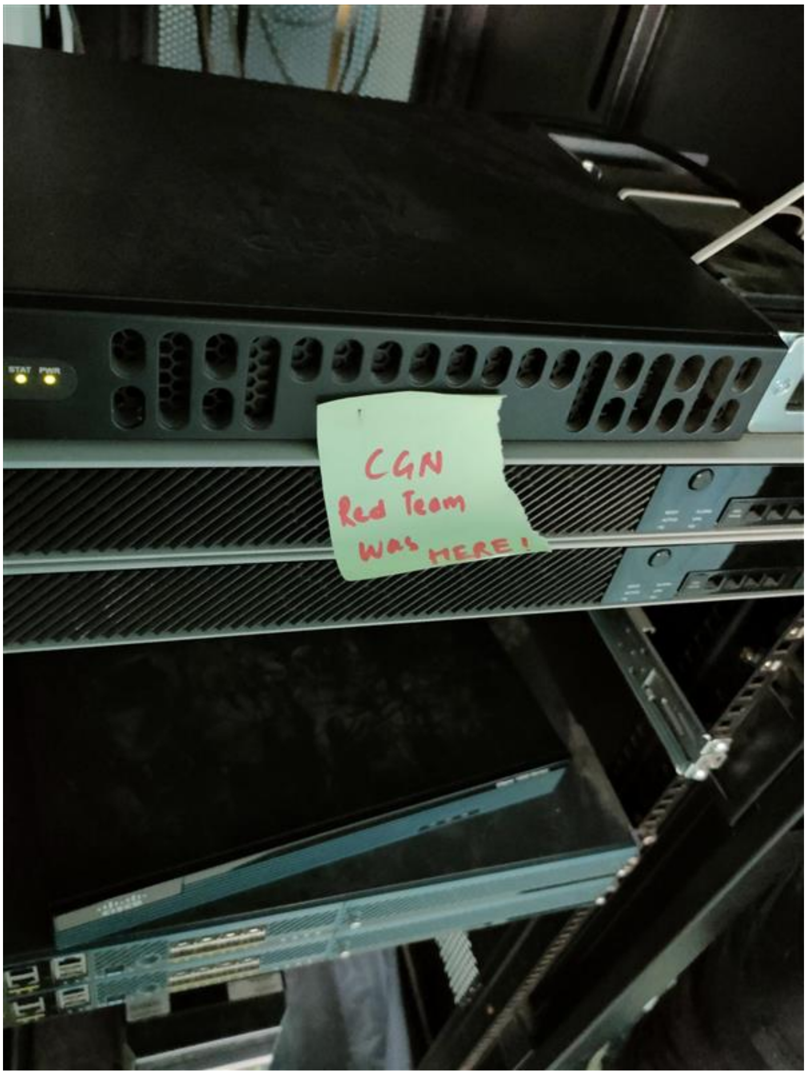


Figure 2: Entered into the server room.

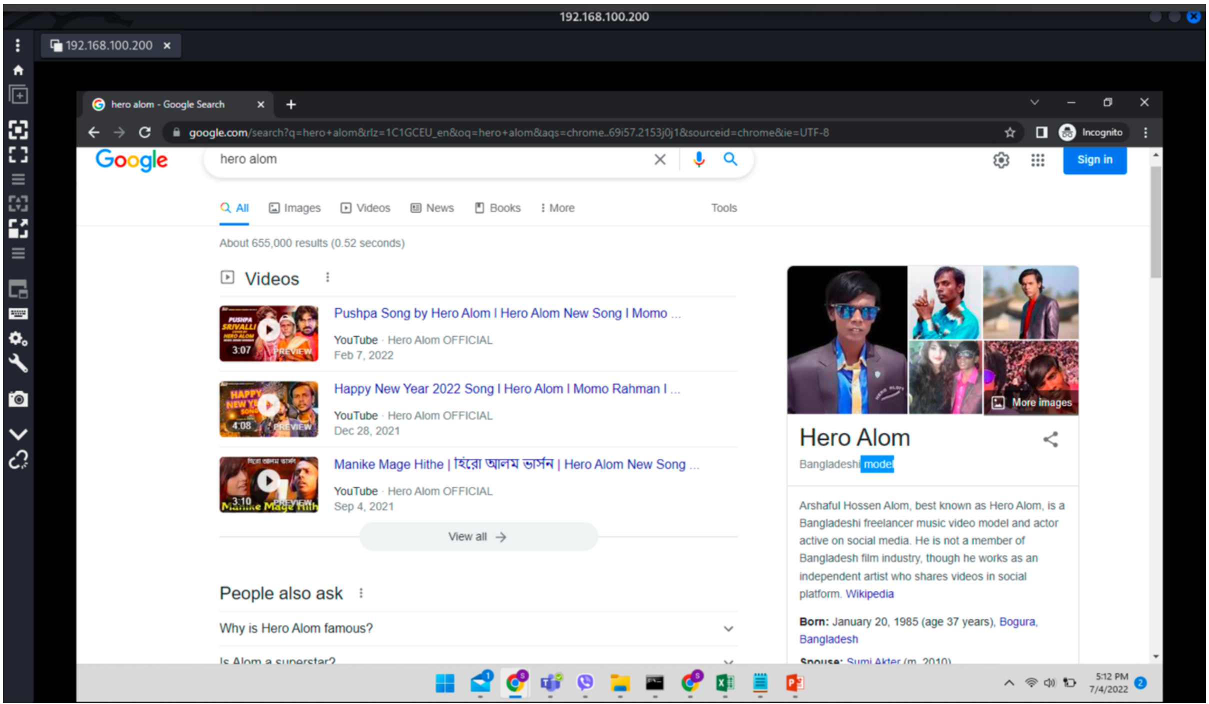
Network Security

After connecting in our access point at [redacted] WIFI", we started searching for available network ranges inside the organization. As we were in 192.[redacted]/24 subnet, we started searching for available network ranges with hit-and-trial basis. Using tool like Angry IP Scanner, we were able to identify the alive hosts in the subnet and started lateral movement within the network to identify the vulnerabilities which could lead us to initial foothold. The identified network ranges are:

- 192.168.[redacted]/24
- 192.168.[redacted]/24
- 192.168.[redacted]/24
- 192.168.[redacted]/24
- 192.168[redacted]/24
- 192.168.[redacted]/24

We performed alive hosts using set of tools such as nmap and techniques like ping sweep, DHCP broadcast, etc.

After identifying the live hosts, we performed half-open port scan to avoid detection from the security team and identified that the user 'S[redacted]k' has the VNC open with no authentication, which we used to gather more information about more targets. During the duration, we noticed the use of weak and guessable credentials like [redacted]@123 in sensitive portals like Nutanix Central.


192.168.100.200
hero alom - Google Search
google.com/search?q=hero+alom&rlz=1C1GCEU_en&oq=hero+alom&aqs=chrome..69i57.2153j0j1&sourceid=chrome&ie=UTF-8
Incognito
Google
hero alom
Sign in
All
Images
Videos
News
Books
More
Tools
View all
More images
5:12 PM
7/4/2022

About 655,000 results (0.52 seconds)

Videos

Pushpa Song by Hero Alom I Hero Alom New Song I Momo ...
YouTube · Hero Alom OFFICIAL
Feb 7, 2022

Happy New Year 2022 Song I Hero Alom I Momo Rahman I ...
YouTube · Hero Alom OFFICIAL
Dec 28, 2021

Manike Mage Hithe | হিরো আলম ভার্সন | Hero Alom New Song ...
YouTube · Hero Alom OFFICIAL
Sep 4, 2021

People also ask

Why is Hero Alom famous?

Is Alom a superstar?

Hero Alom

Bangladeshi model

Arshaful Hossen Alom, best known as Hero Alom, is a Bangladeshi freelancer music video model and actor active on social media. He is not a member of Bangladesh film industry, though he works as an independent artist who shares videos in social platform. Wikipedia

Born: January 20, 1985 (age 37 years), Bogura, Bangladesh

Spouse: Sumi Akter (m. 2010)

Figure 3: S[redacted]'s workstation with VNC

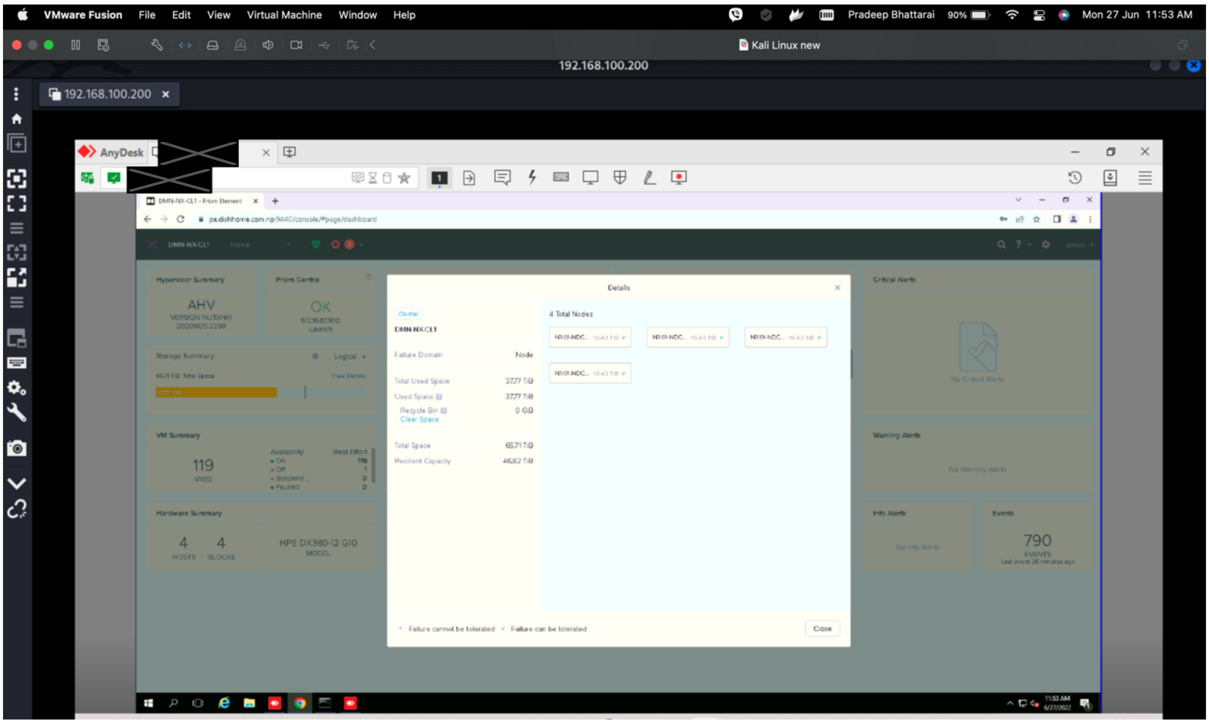
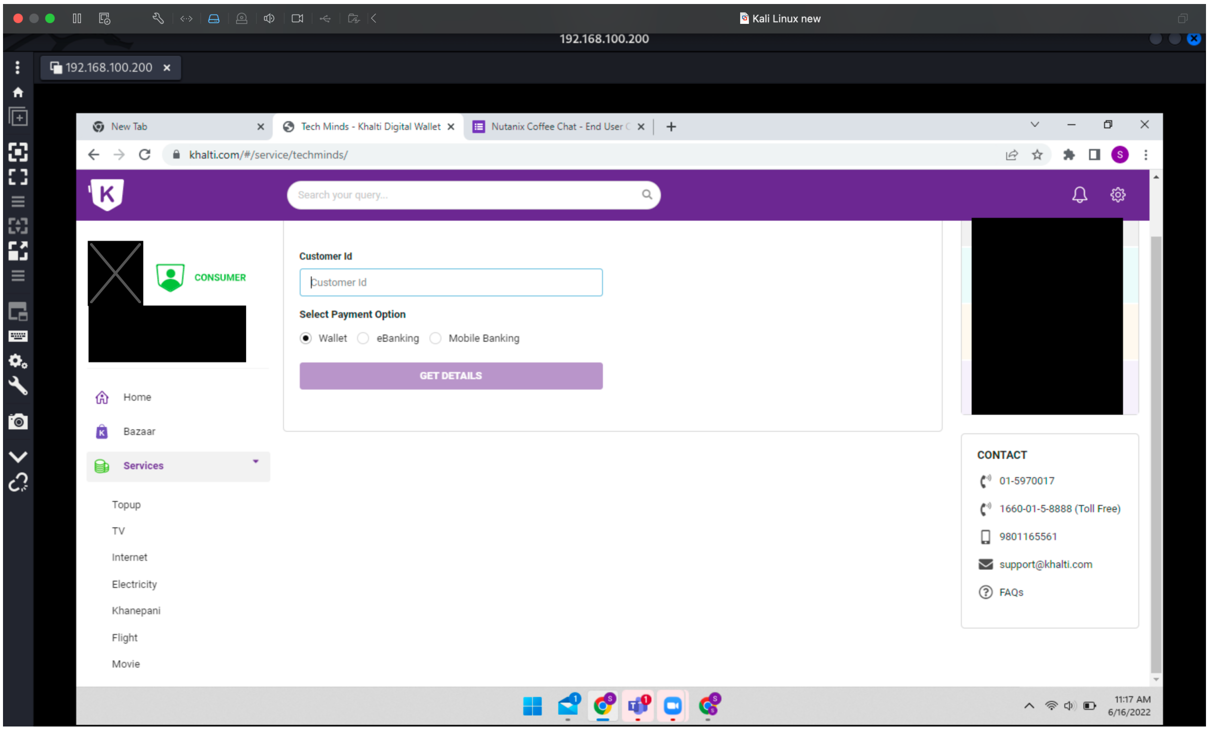


Figure 4: S[redacted]'s screen



[redacted]

Customer Id

Customer Id

Select Payment Option

● Wallet ○ eBanking ○ Mobile Banking

GET DETAILS

[redacted]

CONTACT

01-5970017

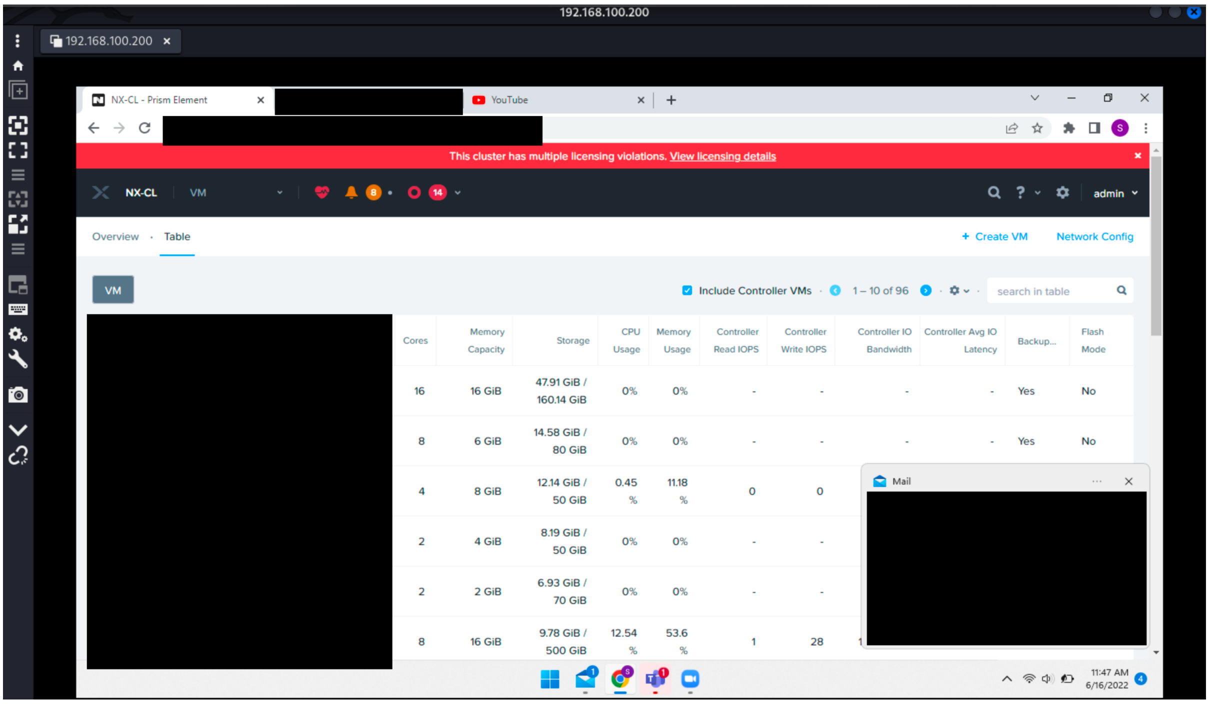
1660-01-5-8888 (Toll Free)

9801165561

support@khalti.com

FAQs

Figure 5: Screenshot accessing Khalti



[redacted]

[redacted]

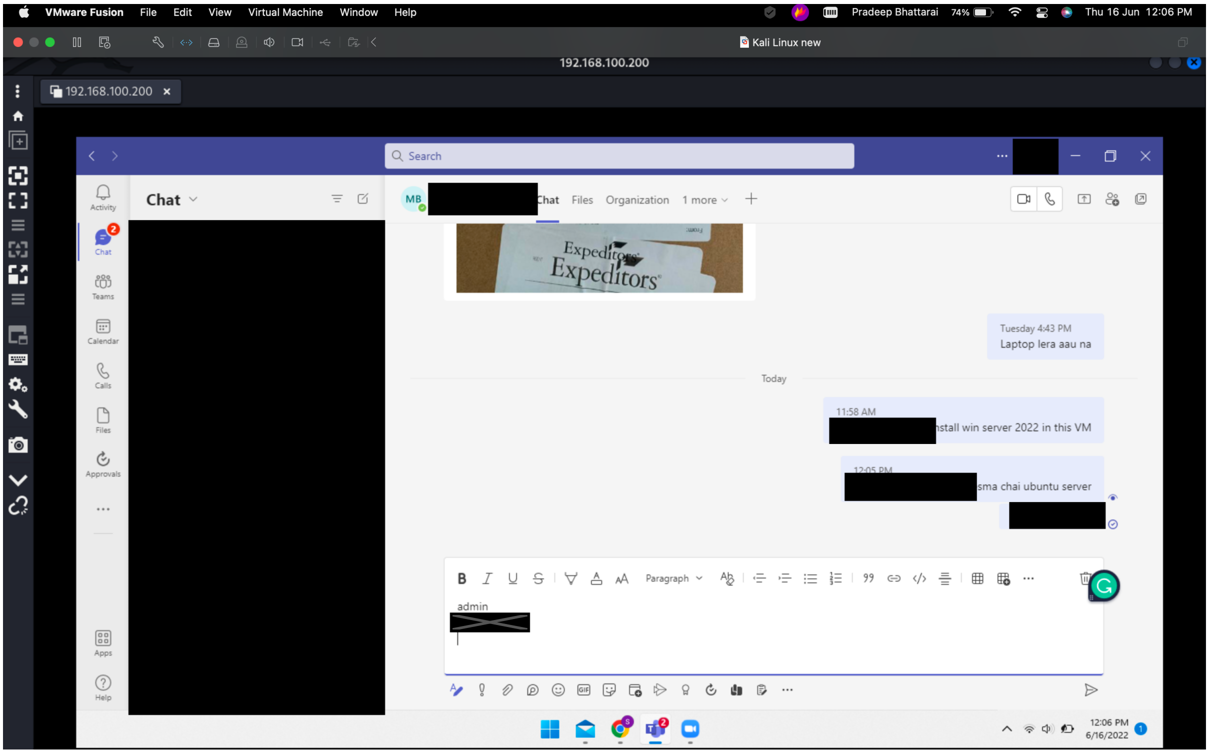
This cluster has multiple licensing violations. View licensing details

☑ Include Controller VMs 1 – 10 of 96 search in table

[redacted]	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Backup...	Flash Mode
[redacted]	16	16 GiB	47.91 GiB / 160.14 GiB	0%	0%	-	-	-	-	Yes	No
[redacted]	8	6 GiB	14.58 GiB / 80 GiB	0%	0%	-	-	-	-	Yes	No
[redacted]	4	8 GiB	12.14 GiB / 50 GiB	0.45 %	11.18 %	0	0				
[redacted]	2	4 GiB	8.19 GiB / 50 GiB	0%	0%	-	-				
[redacted]	2	2 GiB	6.93 GiB / 70 GiB	0%	0%	-	-				
[redacted]	8	16 GiB	9.78 GiB / 500 GiB	12.54 %	53.6 %	1	28	1			

[redacted]

Figure 6: Screenshot accessing Nutanix portal



VMware Fusion File Edit View Virtual Machine Window Help
Pradeep Bhattarai 74% Thu 16 Jun 12:06 PM
Kali Linux new
192.168.100.200
Search
Chat
MB
Chat Files Organization 1 more
Activity
Chat
Teams
Calendar
Calls
Files
Approvals
Apps
Help
Paragraph
12:06 PM
6/16/2022

[redacted]

[redacted]

Tuesday 4:43 PM
Laptop lera aau na

Today

11:58 AM
[redacted]nstall win server 2022 in this VM

12:05 PM
[redacted]sma chai ubuntu server

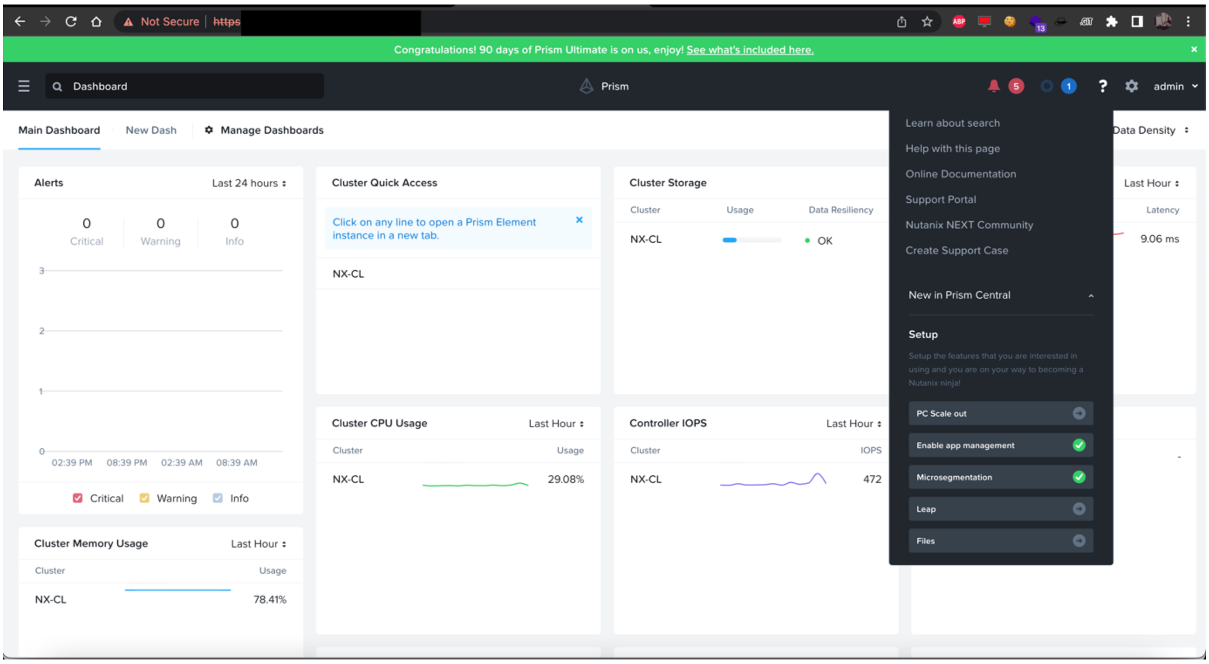
[redacted]

admin
[redacted]

Figure 7: Screenshot of creds being shared in plain text

Accessing Nutanix

Using the common and easy to guess password ‘P[redacted]3’, we were able to log in into the Nutanix portal at 1[redacted]0, 1[redacted]2, 1[redacted]0.



Congratulations! 90 days of Prism Ultimate is on us, enjoy! See what's included here.

Alerts — Last 24 hours: 0 Critical, 0 Warning, 0 Info

Cluster Quick Access: Click on any line to open a Prism Element instance in a new tab. NX-CL

Cluster	Usage	Data Resiliency
NX-CL		OK

Cluster	Latency
	9.06 ms

Setup the features that you are interested in using and you are on your way to becoming a Nutanix ninja!

Cluster CPU Usage — Last Hour

Cluster	Usage
NX-CL	29.08%

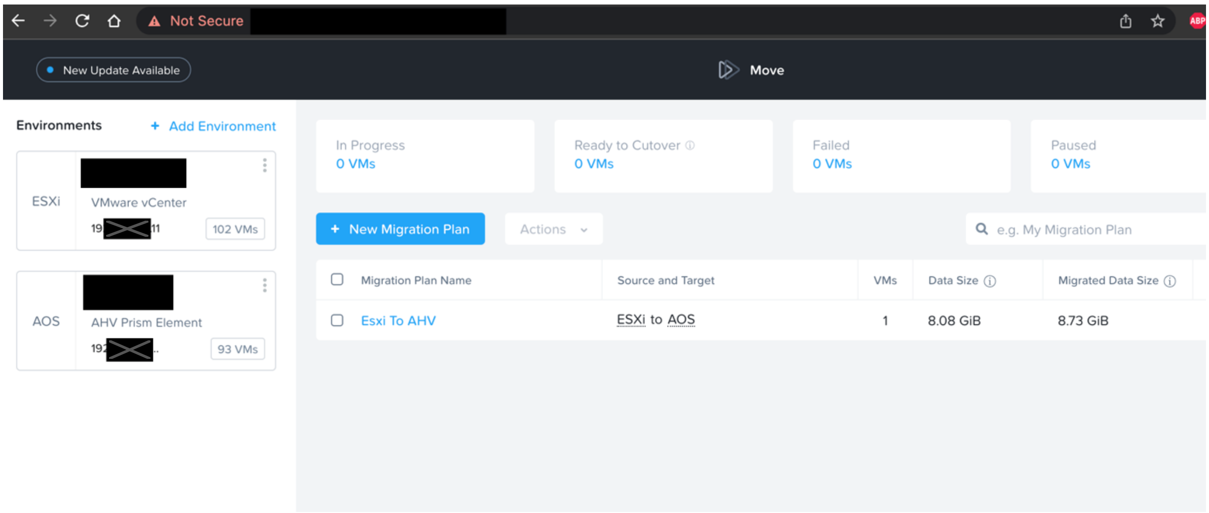
Controller IOPS — Last Hour

Cluster	IOPS
NX-CL	472

Cluster Memory Usage — Last Hour

Cluster	Usage
NX-CL	78.41%

Figure 8: Accessing portal with same creds

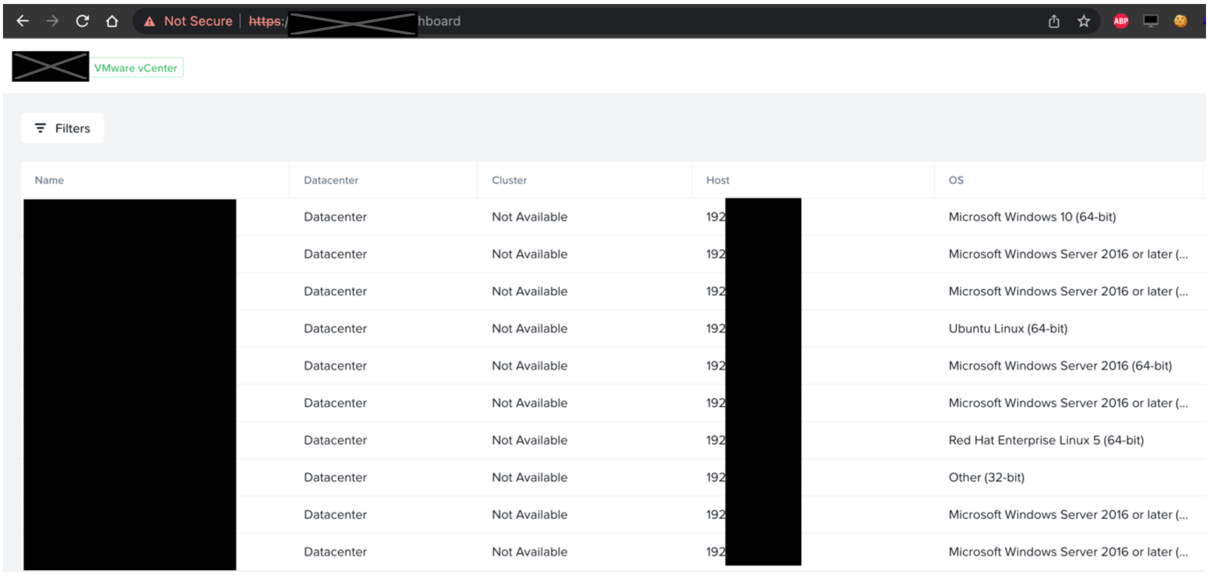


ESXi	[redacted]	VMware vCenter	19[redacted]11	102 VMs
AOS	[redacted]	AHV Prism Element	19[redacted].	93 VMs

In Progress 0 VMs | Ready to Cutover 0 VMs | Failed 0 VMs | Paused 0 VMs

Migration Plan Name	Source and Target	VMs	Data Size	Migrated Data Size
Esxi To AHV	ESXi to AOS	1	8.08 GiB	8.73 GiB

Figure 9: Accessing portal with same creds



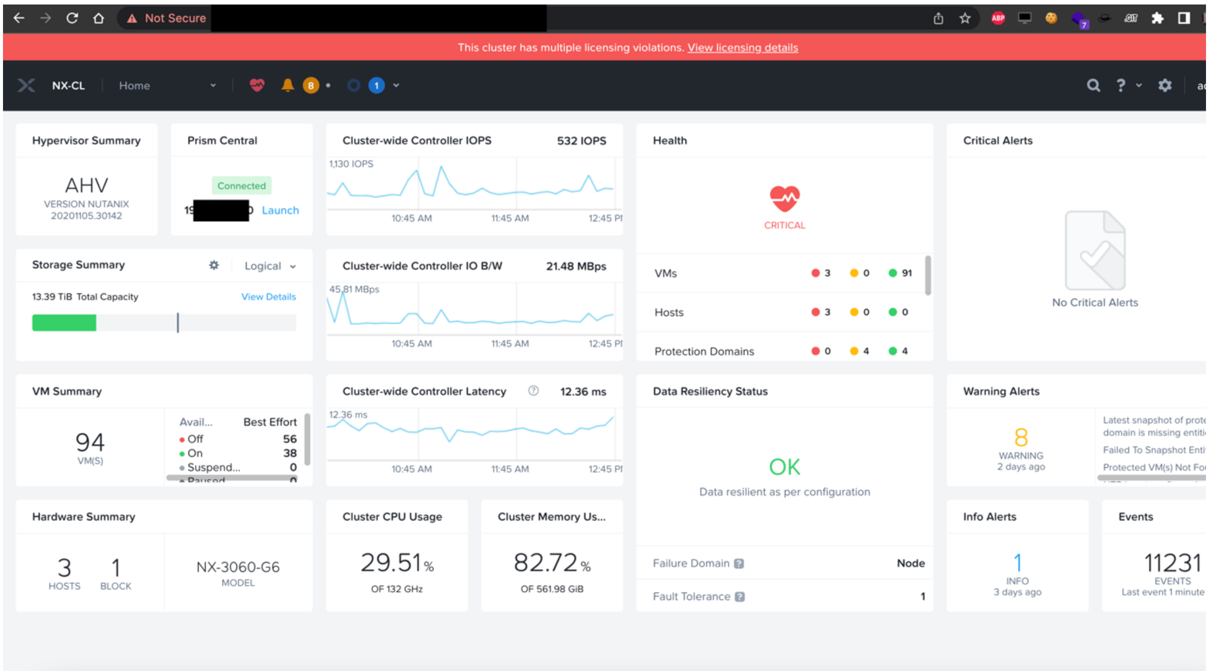
Not Secure | ~~https:/~~[redacted]hboard

[redacted] VMware vCenter

Filters

Name	Datacenter	Cluster	Host	OS
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows 10 (64-bit)
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows Server 2016 or later (...
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows Server 2016 or later (...
[redacted]	Datacenter	Not Available	192[redacted]	Ubuntu Linux (64-bit)
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows Server 2016 (64-bit)
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows Server 2016 or later (...
[redacted]	Datacenter	Not Available	192[redacted]	Red Hat Enterprise Linux 5 (64-bit)
[redacted]	Datacenter	Not Available	192[redacted]	Other (32-bit)
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows Server 2016 or later (...
[redacted]	Datacenter	Not Available	192[redacted]	Microsoft Windows Server 2016 or later (...

Figure 10: Viewing additional information about other potential targets



Not Secure [redacted]

This cluster has multiple licensing violations. View licensing details

NX-CL | Home

Hypervisor Summary: AHV VERSION NUTANIX 20201105.30142

Prism Central: Connected 19[redacted]0 Launch

Cluster-wide Controller IOPS 532 IOPS

Storage Summary Logical
13.39 TiB Total Capacity View Details

Cluster-wide Controller IO B/W 21.48 MBps

VM Summary: 94 VM(S)

Avail...	Best Effort
● Off	56
● On	38
● Suspend...	0

Cluster-wide Controller Latency 12.36 ms

Hardware Summary: 3 HOSTS 1 BLOCK NX-3060-G6 MODEL

Cluster CPU Usage 29.51% OF 132 GHz

Cluster Memory Us... 82.72% OF 561.98 GiB

Health: CRITICAL

	●	●	●
VMs	3	0	91
Hosts	3	0	0
Protection Domains	0	4	4

Data Resiliency Status: OK
Data resilient as per configuration
Failure Domain: Node
Fault Tolerance: 1

Critical Alerts: No Critical Alerts

Warning Alerts: 8 WARNING 2 days ago
Latest snapshot of prote
domain is missing entiti
Failed To Snapshot Enti
Protected VM(s) Not Fo

Info Alerts: 1 INFO 3 days ago

Events: 11231 EVENTS Last event 1 minute

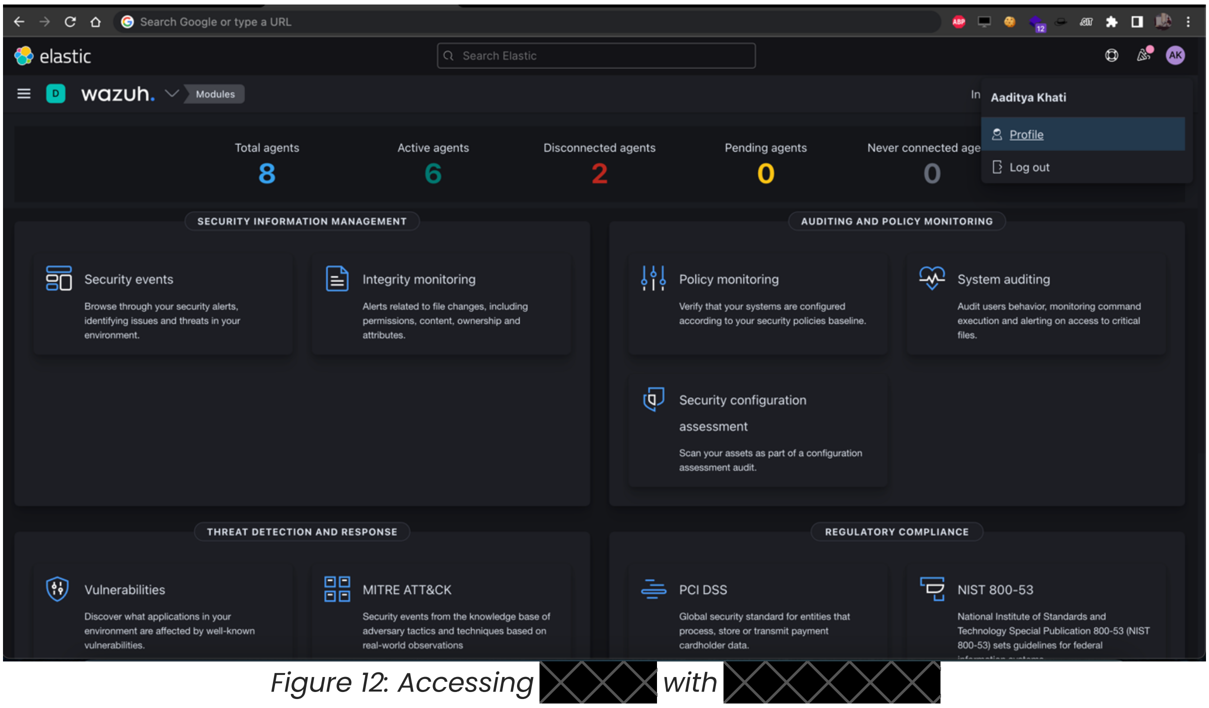
Figure 11: Accesing nutanix portal

Accessing [redacted]

We identified [redacted] at [redacted] and we were able to log in with weak credentials like first name as username and password. For this, we social engineered ‘[redacted]’ to extract his credentials and identified the credential pattern. The credentials with same pattern were now used to obtain access at [redacted] on [redacted]. The identified credentials are:

- [redacted]

We created a custom dashboard named 'RED TEAM WAS HERE' and to gain persistence, we created our own user.



Total agents	Active agents	Disconnected agents	Pending agents	Never connected age
8	6	2	0	0

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE

Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.

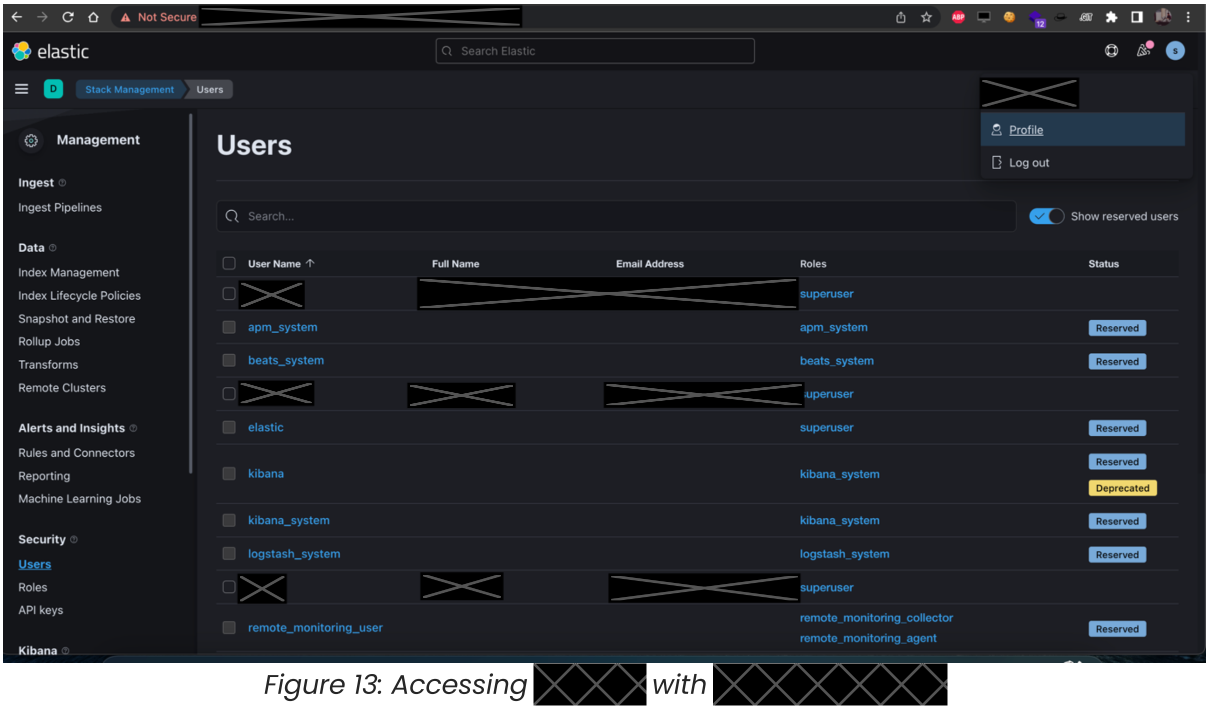
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE

PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.

NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal

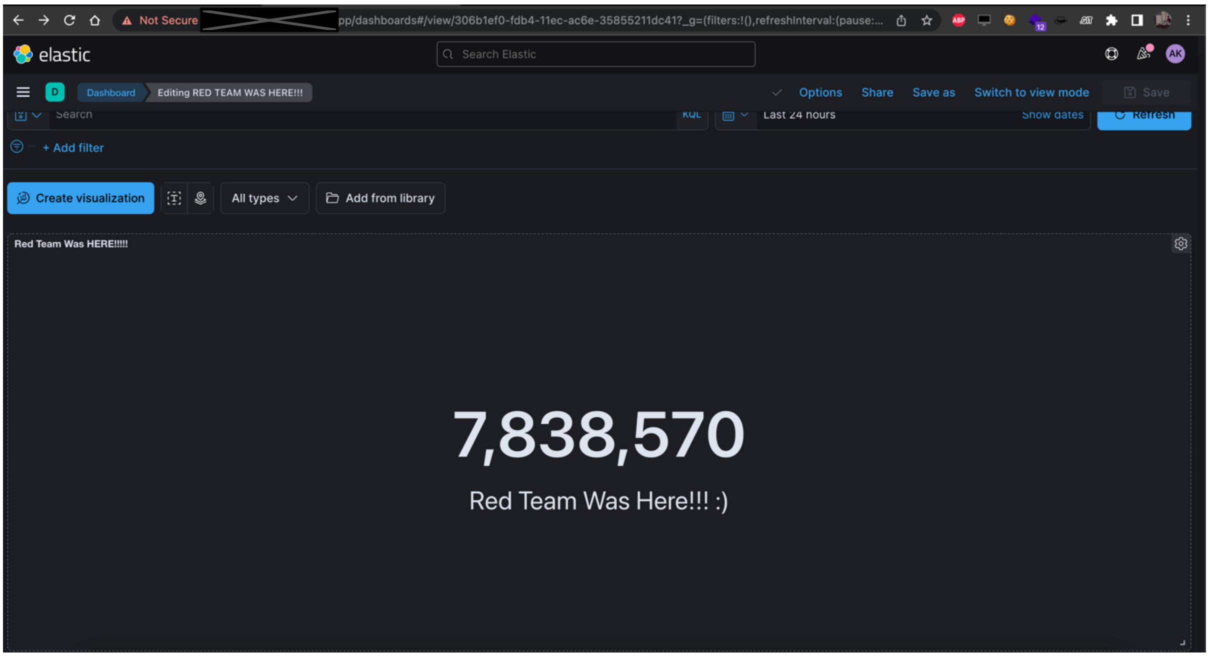
Figure 12: Accessing [redacted] with [redacted]



Users

User Name	Full Name	Email Address	Roles	Status
[redacted]	[redacted]		superuser	
apm_system			apm_system	Reserved
beats_system			beats_system	Reserved
[redacted]	[redacted]	[redacted]	uperuser	
elastic			superuser	Reserved
kibana			kibana_system	Reserved Deprecated
kibana_system			kibana_system	Reserved
logstash_system			logstash_system	Reserved
[redacted]	[redacted]	[redacted]	superuser	
remote_monitoring_user			remote_monitoring_collector remote_monitoring_agent	Reserved

Figure 13: Accessing [redacted] *with* [redacted]



Red Team Was HERE!!!!

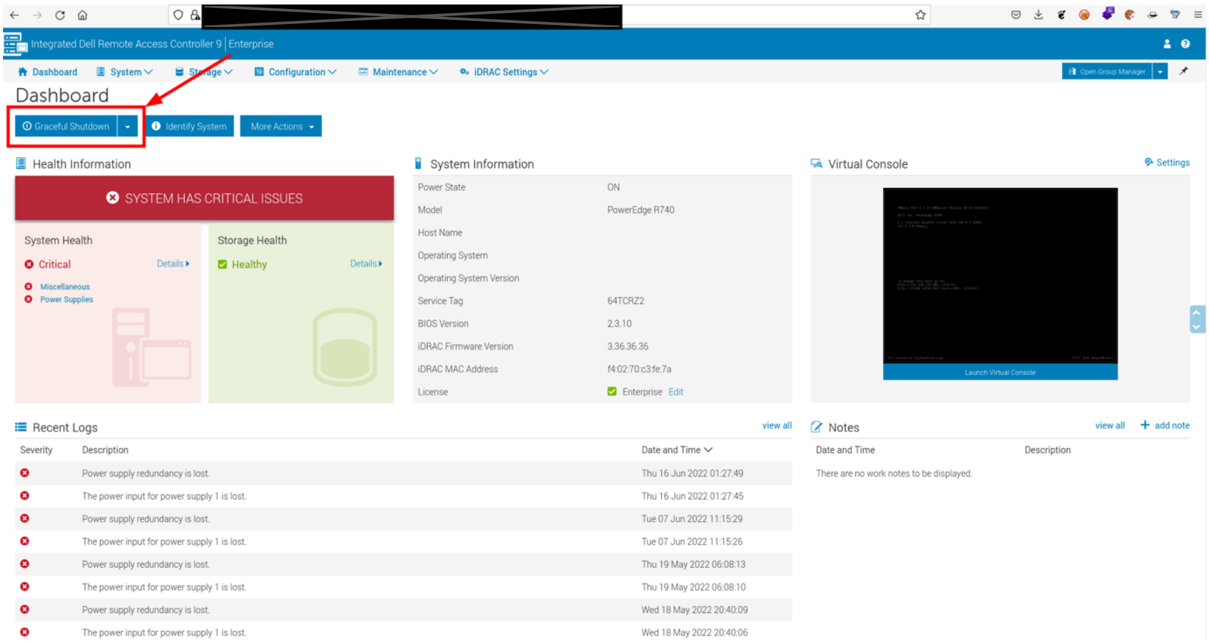
7,838,570

Red Team Was Here!!! :)

Figure 14: Leaving our message

Accessing iDRAC

Throughout the assessment, we were able to gain access to the Dell Remote Access Controller (iDRAC). Publicly available iDRAC username and password (root:calvin) was used to gain access at 192[redacted]0.



[redacted]

System Information

Power State	ON
Model	PowerEdge R740
Host Name	
Operating System	
Operating System Version	
Service Tag	64TCRZ2
BIOS Version	2.3.10
iDRAC Firmware Version	3.36.36.36
iDRAC MAC Address	f4:02:70:c3:fe:7a
License	✓ Enterprise Edit

Recent Logs

Severity	Description	Date and Time
☒	Power supply redundancy is lost.	Thu 16 Jun 2022 01:27:49
☒	The power input for power supply 1 is lost.	Thu 16 Jun 2022 01:27:45
☒	Power supply redundancy is lost.	Tue 07 Jun 2022 11:15:29
☒	The power input for power supply 1 is lost.	Tue 07 Jun 2022 11:15:26
☒	Power supply redundancy is lost.	Thu 19 May 2022 06:08:13
☒	The power input for power supply 1 is lost.	Thu 19 May 2022 06:08:10
☒	Power supply redundancy is lost.	Wed 18 May 2022 20:40:09
☒	The power input for power supply 1 is lost.	Wed 18 May 2022 20:40:06

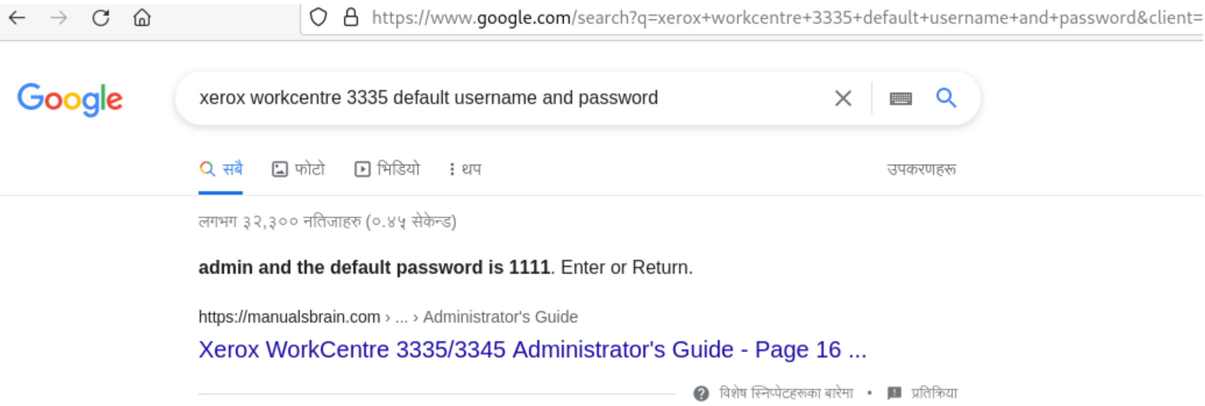
Notes

Date and Time	Description
There are no work notes to be displayed.	

Figure 15: Gaining access to iDRAC

Accessing Printer

The printer (Xerox Workcentre 3335) was accessed with the set of publicly available credentials.



https://www.google.com/search?q=xerox+workcentre+3335+default+username+and+password&client=

xerox workcentre 3335 default username and password

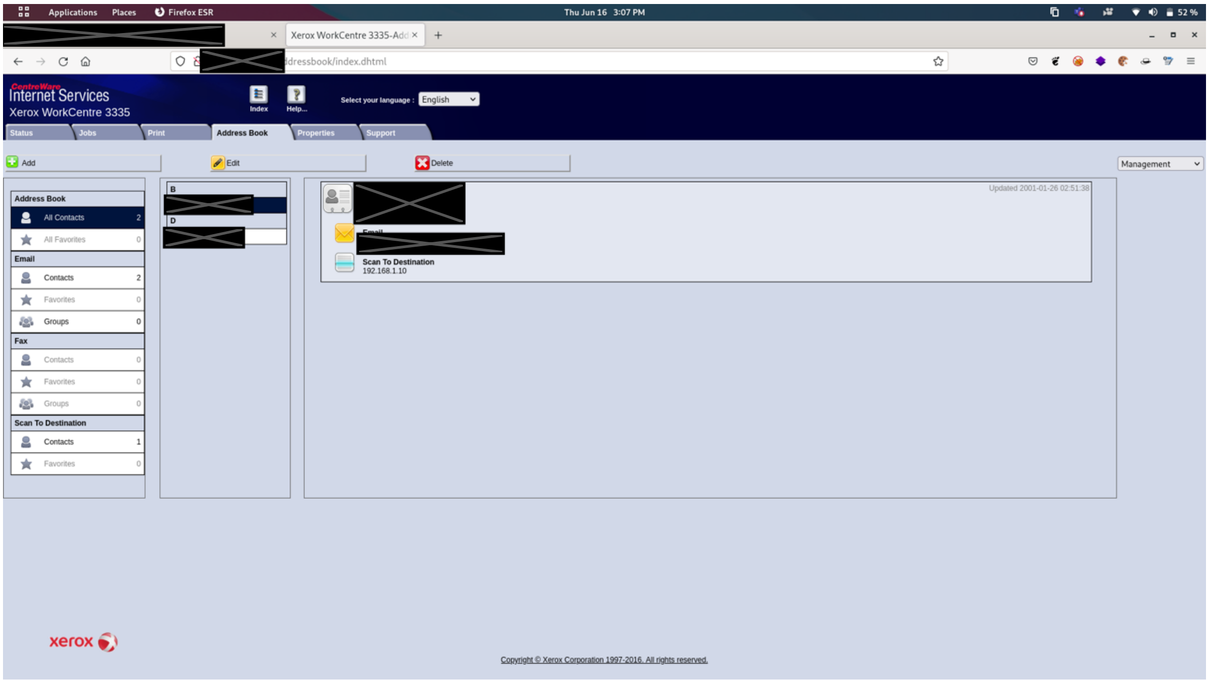
लगभग ३२,३०० नतिजाहरु (०.४५ सेकेन्ड)

admin and the default password is 1111. Enter or Return.

https://manualsbrain.com › ... › Administrator's Guide

Xerox WorkCentre 3335/3345 Administrator's Guide - Page 16 ...

Figure 16: Default Credentials



[redacted]

[redacted]dressbook/index.dhtml

Address Book	
All Contacts	2
All Favorites	0
Email	
Contacts	2
Favorites	0
Groups	0
Fax	
Contacts	0
Favorites	0
Groups	0
Scan To Destination	
Contacts	1
Favorites	0

B

[redacted]

D

[redacted]

[redacted]

Updated 2001-01-26 02:51:38

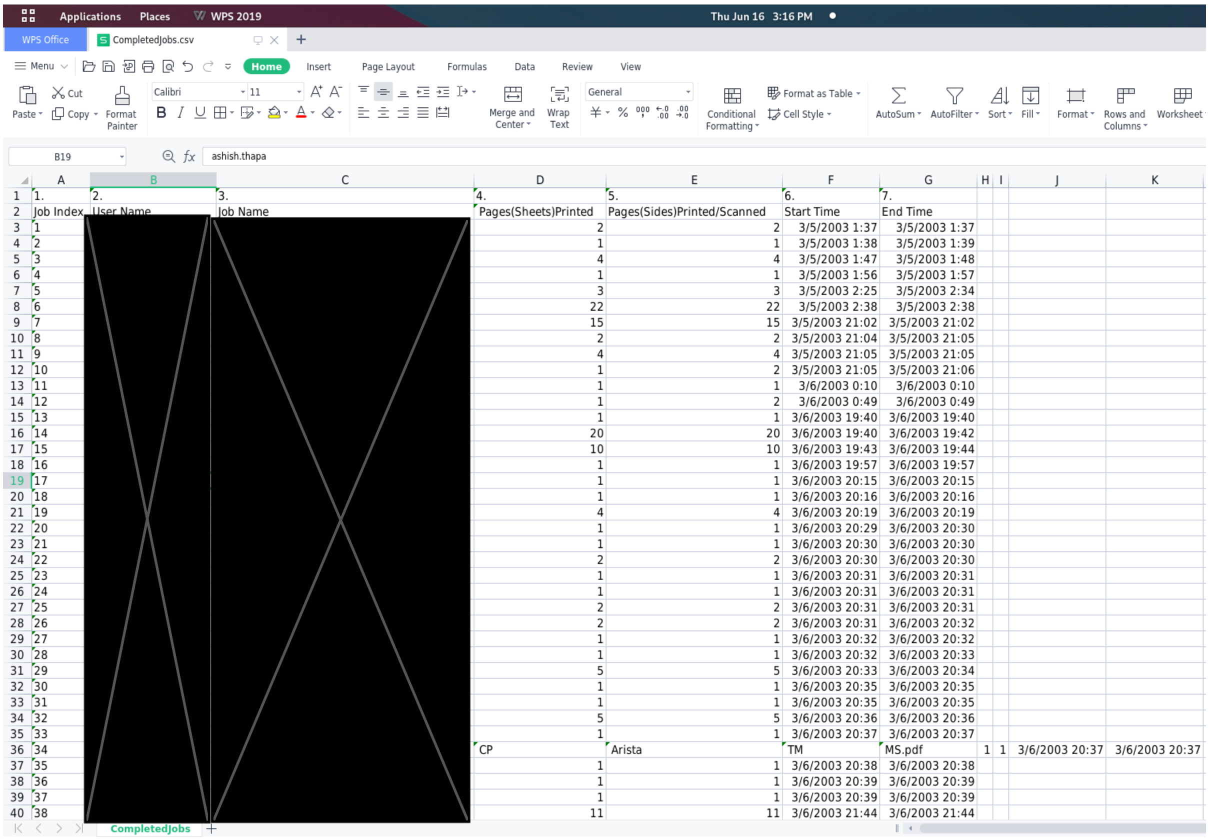
Email

[redacted]

Scan To Destination
192.168.1.10

Copyright © Xerox Corporation 1997-2016. All rights reserved.

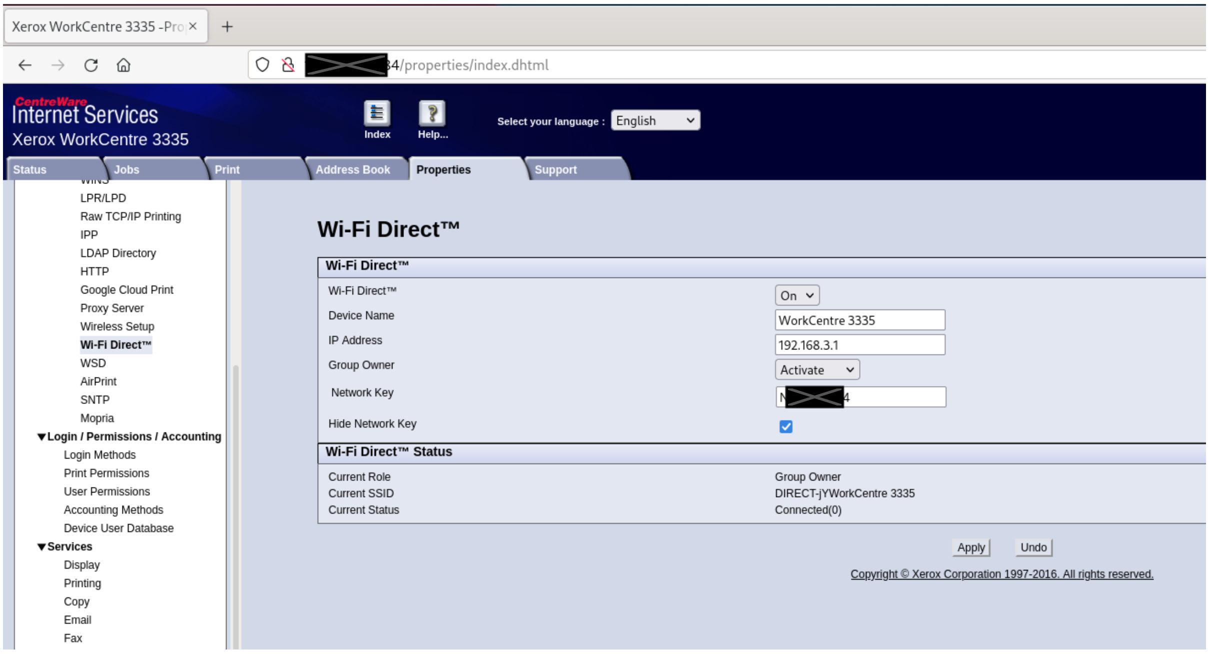
Figure 17: Accessing printer with the identified credentials



B19 fx ashish.thapa

	A	B	C	D	E	F	G	H	I	J	K
1	1.	2.	3.	4.	5.	6.	7.				
2	Job Index	User Name	Job Name	Pages(Sheets)Printed	Pages(Sides)Printed/Scanned	Start Time	End Time				
3	1	[redacted]	[redacted]	2	2	3/5/2003 1:37	3/5/2003 1:37				
4	2	[redacted]	[redacted]	1	1	3/5/2003 1:38	3/5/2003 1:39				
5	3	[redacted]	[redacted]	4	4	3/5/2003 1:47	3/5/2003 1:48				
6	4	[redacted]	[redacted]	1	1	3/5/2003 1:56	3/5/2003 1:57				
7	5	[redacted]	[redacted]	3	3	3/5/2003 2:25	3/5/2003 2:34				
8	6	[redacted]	[redacted]	22	22	3/5/2003 2:38	3/5/2003 2:38				
9	7	[redacted]	[redacted]	15	15	3/5/2003 21:02	3/5/2003 21:02				
10	8	[redacted]	[redacted]	2	2	3/5/2003 21:04	3/5/2003 21:05				
11	9	[redacted]	[redacted]	4	4	3/5/2003 21:05	3/5/2003 21:05				
12	10	[redacted]	[redacted]	1	2	3/5/2003 21:05	3/5/2003 21:06				
13	11	[redacted]	[redacted]	1	1	3/6/2003 0:10	3/6/2003 0:10				
14	12	[redacted]	[redacted]	1	2	3/6/2003 0:49	3/6/2003 0:49				
15	13	[redacted]	[redacted]	1	1	3/6/2003 19:40	3/6/2003 19:40				
16	14	[redacted]	[redacted]	20	20	3/6/2003 19:40	3/6/2003 19:42				
17	15	[redacted]	[redacted]	10	10	3/6/2003 19:43	3/6/2003 19:44				
18	16	[redacted]	[redacted]	1	1	3/6/2003 19:57	3/6/2003 19:57				
19	17	[redacted]	[redacted]	1	1	3/6/2003 20:15	3/6/2003 20:15				
20	18	[redacted]	[redacted]	1	1	3/6/2003 20:16	3/6/2003 20:16				
21	19	[redacted]	[redacted]	4	4	3/6/2003 20:19	3/6/2003 20:19				
22	20	[redacted]	[redacted]	1	1	3/6/2003 20:29	3/6/2003 20:30				
23	21	[redacted]	[redacted]	1	1	3/6/2003 20:30	3/6/2003 20:30				
24	22	[redacted]	[redacted]	2	2	3/6/2003 20:30	3/6/2003 20:30				
25	23	[redacted]	[redacted]	1	1	3/6/2003 20:31	3/6/2003 20:31				
26	24	[redacted]	[redacted]	1	1	3/6/2003 20:31	3/6/2003 20:31				
27	25	[redacted]	[redacted]	2	2	3/6/2003 20:31	3/6/2003 20:31				
28	26	[redacted]	[redacted]	2	2	3/6/2003 20:31	3/6/2003 20:32				
29	27	[redacted]	[redacted]	1	1	3/6/2003 20:32	3/6/2003 20:32				
30	28	[redacted]	[redacted]	1	1	3/6/2003 20:32	3/6/2003 20:33				
31	29	[redacted]	[redacted]	5	5	3/6/2003 20:33	3/6/2003 20:34				
32	30	[redacted]	[redacted]	1	1	3/6/2003 20:35	3/6/2003 20:35				
33	31	[redacted]	[redacted]	1	1	3/6/2003 20:35	3/6/2003 20:35				
34	32	[redacted]	[redacted]	5	5	3/6/2003 20:36	3/6/2003 20:36				
35	33	[redacted]	[redacted]	1	1	3/6/2003 20:37	3/6/2003 20:37				
36	34	[redacted]	[redacted]	CP	Arista	TM	MS.pdf	1	1	3/6/2003 20:37	3/6/2003 20:37
37	35	[redacted]	[redacted]	1	1	3/6/2003 20:38	3/6/2003 20:38				
38	36	[redacted]	[redacted]	1	1	3/6/2003 20:39	3/6/2003 20:39				
39	37	[redacted]	[redacted]	1	1	3/6/2003 20:39	3/6/2003 20:39				
40	38	[redacted]	[redacted]	11	11	3/6/2003 21:44	3/6/2003 21:44				

Figure 18: Viewing printer jobs



[redacted]4/properties/index.dhtml

Select your language : English

Wi-Fi Direct™

Wi-Fi Direct™

Wi-Fi Direct™	On
Device Name	WorkCentre 3335
IP Address	192.168.3.1
Group Owner	Activate
Network Key	N[redacted]4
Hide Network Key	☑

Wi-Fi Direct™ Status

Current Role	Group Owner
Current SSID	DIRECT-jYWorkCentre 3335
Current Status	Connected(0)

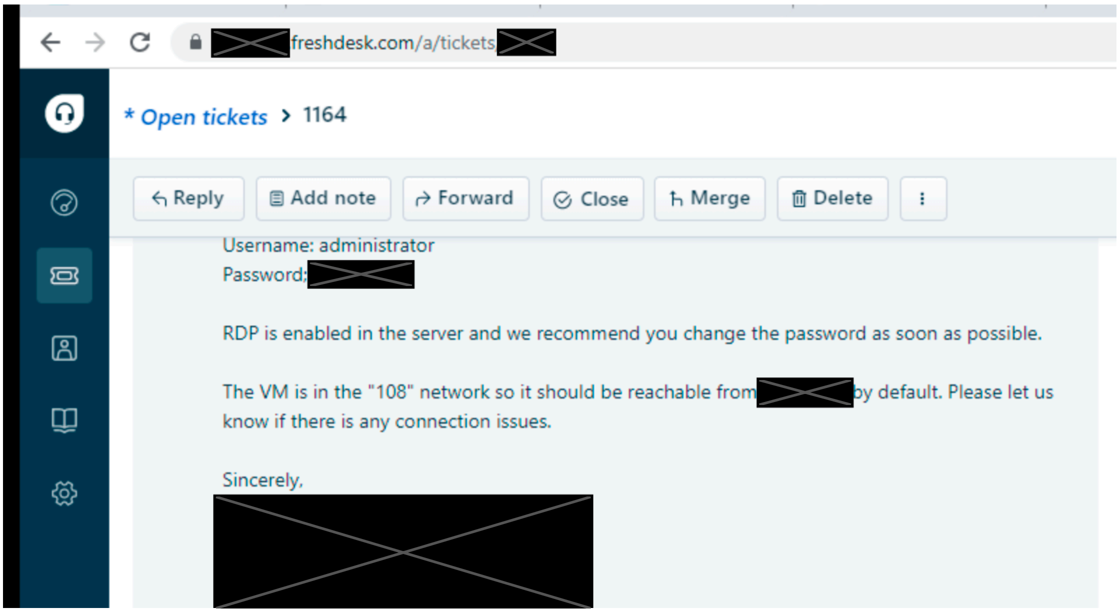
Copyright © Xerox Corporation 1997-2016. All rights reserved.

Figure 19: Viewing credentials for SSID broadcasted by the printer

Accessing Instances

Looking at the message from S[redacted]'s workstation, we were able to identify the IP address, username, and password of one of the instances at 1[redacted]19.

- Username: administrator
- Password: [redacted]
- IP Address: 1[redacted]19



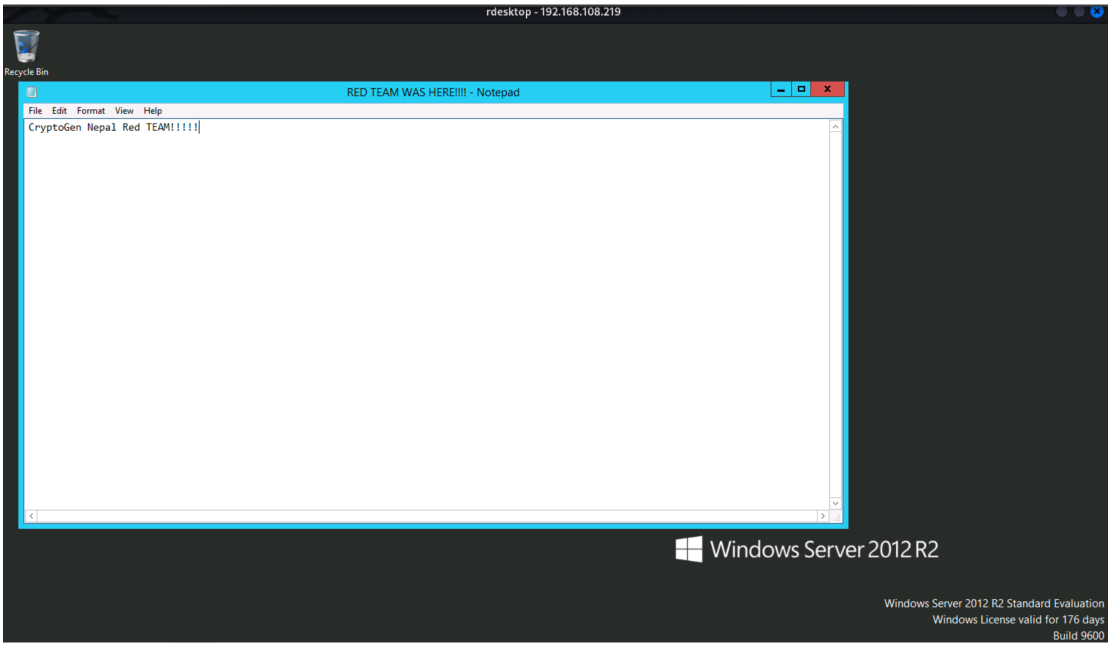
Username: administrator
Password:[redacted]

RDP is enabled in the server and we recommend you change the password as soon as possible.

The VM is in the "108" network so it should be reachable from[redacted]by default. Please let us know if there is any connection issues.

Sincerely,
[redacted]

Figure 20: Identifying credentials in support message


rdesktop - 192.168.108.219
Recycle Bin
RED TEAM WAS HERE!!!! - Notepad
File Edit Format View Help
Windows Server 2012 R2

```
CryptoGen Nepal Red TEAM!!!!!
```

Windows Server 2012 R2 Standard Evaluation
Windows License valid for 176 days
Build 9600

Figure 21: Accessing the machine and placing the message

Conclusion

CryptoGen Nepal performed a Red Team engagement to determine the full impact of a realistic threat. We identified several exploitable vulnerabilities and weak spots that were leveraged to establish a foothold, escalate privileges, expand access across the domain, and move proprietary information out of the network. CryptoGen Nepal assesses that an external threat can successfully compromise [redacted] based on the path demonstrated during the assessment.

No highly specialized exploits or tools were used or required to perform any of the actions described within this report. We used a publicly available attack framework for nearly all exploitation activities. The technical skill level required to conduct individual actions ranges from low to intermediate. The required technical capability and level of access that was achieved by chaining these vulnerabilities is a cause for concern. Critical exposures and observations include weak credentials. Overall, the Red Team was able to accomplish threat objectives, and it is our hope that the security posture of [redacted] systems will be improved as a result of the efforts.

OUR SERVICES

Our Services As Information Security Company Includes:

- SECURITY OPERATIONS CENTER
- INFORMATION SECURITY AUDIT
- SWIFT CSP ASSESSMENT
- DARKWEB MONITORING & BRAND PROTECTION
- VULNERABILITY MANAGEMENT
- PENETRATION TESTING
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER CONFIGURATION ASSESSMENT
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING

CryptoGen Nepal

/cryptogennepal
www.cryptogennepal.com
+977-1-4528928
whois@cryptogennepal.com