XCorp Threat Model Report
for Red Team Virtual Network

Published on **12/09/2020**

Authors:

Eyal Ben Dror

Gaurav Varma

Lana McGee

Nell-e Medina

Table of Contents

EXECUTIVE SUMMARY

The importance of this report is to observe potential threats and prevent potential breaches of information of our Virtual Machines. Potential exploits attackers could use may be through the compromise of SSH public keys, IP spoofing and/or gaining elevated privileges. The potential of an attacker using these techniques are of medium to low probability. The Virtual Network had the proper safeguards in place to protect each Virtual Machine (VM).

Results High-Level Overview

GLEN Pentesters identified 1 High, 0 Moderate, and 0 Low severity findings. The top findings based on calculated severity ratings are as follows:

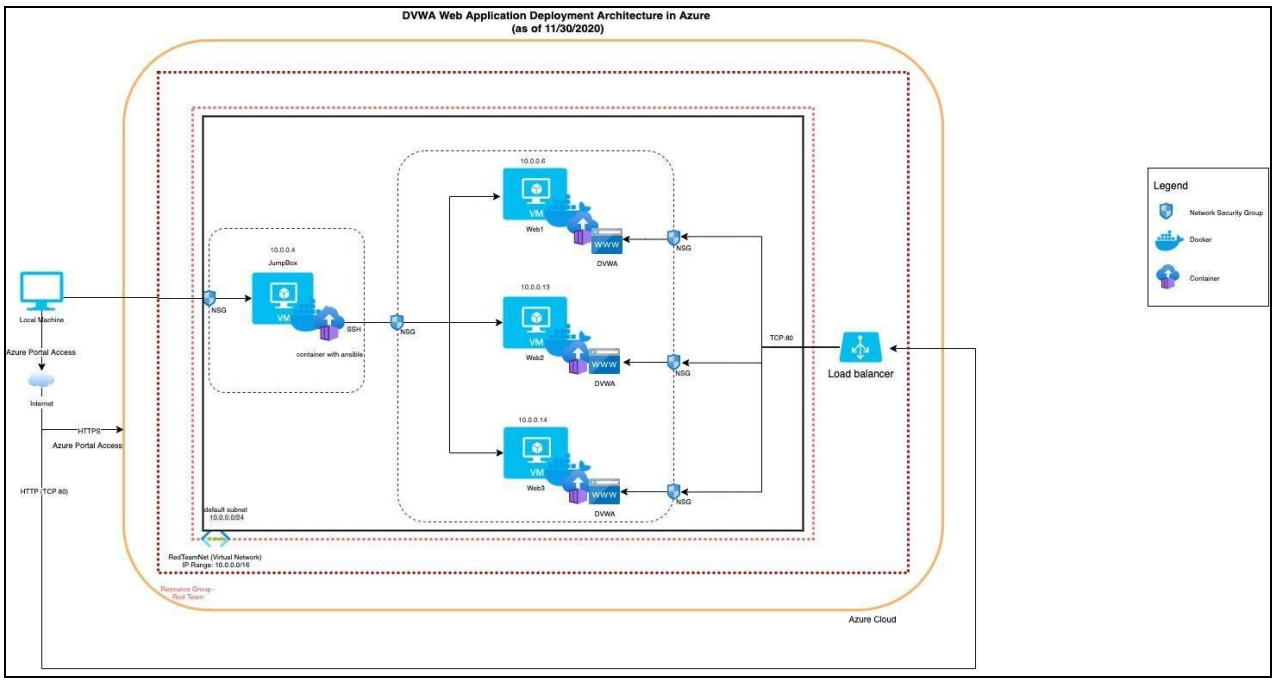
GPT-01: Sudo Accounts are not established, Root privilege is enabled.

SCOPE

The scope of this document is to build a Threat Model to assess weaknesses and threats to Red-Team Network Infrastructure in Azure Cloud. The applications that will be deployed in this network and related application security threats and data security threats are not in scope of this document.

At this time, we do not have details on the revenue generated by the Web application which is why this document will limit asset inventory to XCorp's cloud infrastructure. The asset value of cloud infrastructure is measured by time and cost it takes to build it from ground up.

Architecture Diagram



Scope of Target System Testing

The scope of the penetration test included external IP addresses of the Red Team Virtual Network. The scope was reviewed with the Administrators of the Red Team prior to the engagement and confirmed as accurate, complete and current at the time of the assessment.

Scope Considerations

GLEN Pentesters understands that no two penetration tests are the same and that methodologies are used as high-level guidance. Prior to testing, analysis was completed of which attack vectors applied to the Red Team Virtual Network and these in-scope vectors are identified in the table below. The diagram below illustrates all possible attack scenarios that could be in scope for a penetration test.

Attack Vectors in Scope for this Assessment

Based on the information provided during the planning phase of this assessment, the following attack vectors were determined to be in scope for this penetration test. Included are the expected results in the "Additional Information" column. If an attack vector is not in scope, justification is provided in the "Additional Information" column.

Y/N	ATTACK VECTOR	ADDITIONAL INFORMATION
☒	**#1a External to VLAN**	We should not be able to access any network or data outside of what is available for public dissemination through Red Team's virtual footprint.
☒	**#2 External to Target System**	We should not be able to access any network, application, or data outside of what is available for public dissemination.
☒	**#3 Target System to Web Applications**	We should not be able to access web applications accessed by Red Team.

Table 1: Attack Vectors in Scope

Threat Agents

The main threat agents to Red-Team's Network Infrastructure addressed in this document are:

- Identity Theft of DevSecOps employees
- Incompetent DevSecOps employee breaking cloud configurations
- APTs (Advanced Persistent Threats)
- Azure cloud outages
- Script kiddies
- Man-in-the-middle attack on Public Load Balancer Traffic

STRIDE Threat Model

STRIDE is a model of threats implemented to help consider and identify potential threats to a system. The below mentioned threats fall under Six categories of threats under STRIDE model:

Spoofing

It was found that DevSecOps employees use simple passwords without Multi-factor authentication to login to Azure Portal. This glaring vulnerability puts Red-Team's network infrastructure open to exploitation by attackers. An attacker can target this weak authentication mechanism and impersonate a DevSecOps employee to access Azure Portal and modify Red-Team's cloud network infrastructure.

Mitigation: *Implement multi-factor authentication on Azure Portal, preferably using Single-sign-on. XCorp can also look at restricted access to Azure Portal's XCorp account to internal network (or via corporate VPN)*

Tampering

A malicious hacker can infiltrate Red-Team's cloud network by remotely controlling an employee's machine. This hacker can then modify important security controls like security groups or VM images or ansible Playbooks that could violate integrity of the system.

Mitigation: *Save all security configurations and playbooks on a repository like Github with proper identity and access management. This will help verify and restore the system faster in case of tampering on the Jumpbox server container. If configurations are stored locally, it should be hashed and monitored in order to keep the integrity of the files.*

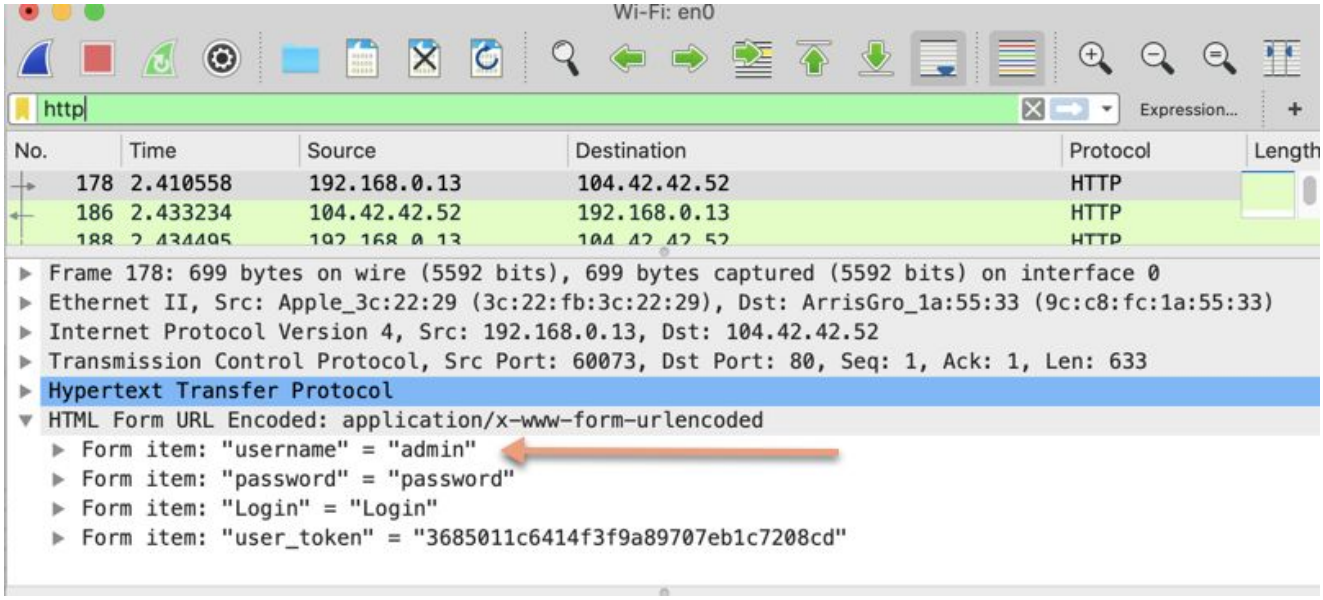
Repudiation

There is a lack of Identity and Access Management on Red-Team's cloud network. Since all DevSecOps employees have full access to the system, there are high chances of Repudiation where an employee can claim to not have made changes to the system.

Mitigation: *Implement the Principle of Least Privilege by establishing role-based access and assign sudo privileges to those with business need. Implement proper audit logging for critical system changes and review of the logs in order to verify validity of the changes made.*

Information Disclosure

It was found that all traffic to load balancer happens on unsecure http port 80. This can lead to information disclosure where an attacker on the network can sniff packets and extract critical data leading to data breaches. This violates confidentiality of data. (below is a Wireshark packet capture for load balancer destination)



Mitigation: *Implement encryption in transit through SSL on the load balancer (HTTPS).*

Denial of Service

It was found that there is no DDoS protection on the public load balancer of Red-Team's cloud network. This can be exploited by an attacker to slow the system or impact the backend server adversely.

Mitigation: *Enable DDoS, implement monitoring and alerting when server resource (like RAM, CPU, Diskspace) consumption is high*

Elevation of Privilege

It was found that login to Jumpbox and Web Servers let the user assume *sudo* privilege. This violates authorization and can be used by an attacker to create a hidden account that can be later used to spoof a user.

Mitigation: *Implement Proper authorization like role-based access; practice least privilege principle*

Threat Assessment and Mitigation with CVSS Score

Threat	Description	Severity (cvss score)	Mitigation
Unauthorized access to the Azure Account	If someone gains access to the Azure account then the outside actor gains full control of the Networks we've created.	**Critical**	2-factor authentication; Unique ssh keys for every user; Limited root access.

Stolen SSH key on Jump Box Admin's laptop	If an outside actor gains access to the account and changes the SSH key, it will disrupt communication between the Jump box and the host Azure connection; preventing access to any VM.	**Critical**	Enable identity and Access Management (IAM) and establish Principle of Least Privilege. Cycle SSH Keys frequently.
IP Spoofing on Port 22	An outside actor can spoof the IP address indicated on the Network Security Group and access the jumpbox using SSH	**Critical**	SSH keys
Stolen SSH key on Jump Box	If an outside actor gains access to Jump Box, they can copy SSH Keys from this VM to any other VM, modify the security group and gain access to all Web VMs.	**Medium**	Enable identity and Access Management (IAM) and establish Principle of Least Privilege. Cycle SSH Keys frequently.
DDos (Distributed Denial of Service) Attack	An outside actor can send overwhelming http requests to the server. Since load balancers do not have DDoS protection, this can create a burden on Web servers and likely to become unavailable.	**Low**	Rate limitation on the Load Balancer Firewall.
IP Spoofing on Port 80	An outside actor can disguise his origin IP. This is typically used in DoS assaults.	**Low**	Establish deep packet inspection (DPI) which uses granula analysis of all packet headers rather than just source IP address. This is a very resource intensive process that could lead to unavailability of service.
Man-In-The-Middle Attack (using unencrypted HTTP traffic from Port 80)	Enables outside actors to eavesdrop or break further into the servers once the single layer protection is compromised.	**Medium**	Establish VPN tunnel
Zero-day Vulnerability	If an outside actor identified a vulnerability on the VM Operating System, it may become vulnerable to exploitation through phishing, malware.	**Medium**	Create a plan on how Zero-day vulnerability will be addressed.

Web Application vulnerabilities based on the OWASP model.	If the application does not address OWASP top 10 Web application security risks, it will make the complete system vulnerable to attack and exploitation.	**High**	Validate and address OWASP top 10 Web application security risks on DVWA
Azure Cloud unavailability	Since we are relying on Azure cloud to host our application, any downtime for Azure will lead to the system being impacted	**Low**	Develop a written Third Party Risk Management Policy including quarterly and annual monitoring and reporting. The policy considerations must include the ability of the third party to maintain availability of services and Disaster Recovery objectives.
Known exploits and attacks on systems used in the cloud	All the key components in the architecture like Network Security Group, Resource Group, Virtual Network are software systems and susceptible to exploitation and attacks	**Low**	Work with Azure to understand Service Level Agreements on addressing patching and vulnerabilities of all software components in Azure cloud. Support ticket processes for Azure Cloud should also be documented.
Known exploits and attacks on Operating Systems, Docker, Container and DVWA code dependencies.	Emerging threats on software components like VM Operating System, Docker, Container and DVWA application code dependencies	High	Security patches on all software components like VM, Docker and Container should be performed on a regular basis. The schedule should address continuous redeployment of software components with latest security patches and related downtimes if any.
Outage	System unavailability - There can be multiple reasons why the web application could have an outage	High	Create alerts on system availability (like health probe fail) and make sure Operations support team is alerted if the application becomes unavailable or the CPU, RAM, Diskspace, IO operations reach a certain threshold

CONCLUSION/RECOMMENDATION

Maintaining the basic security controls that were implemented upon the initiation of the network infrastructure will ensure a good level of resiliency against attacks to gain entrance to the Virtual Network. However, there are still potential weaknesses of the Virtual Network. These include a disruption of communication between VM's or access to the Azure website; which is the key to the castle. It is important to understand the few avenues of gaining these privileges. Some security controls that may help protect the CIA Triad would be both technical and administrative to cross examine and maintain a secure Virtual Network. After implementing and/or discussing the mitigation steps mentioned in this document, the Red-Team should revisit the threats identified in STRIDE to check quality, feasibility, progress, and/or planning.