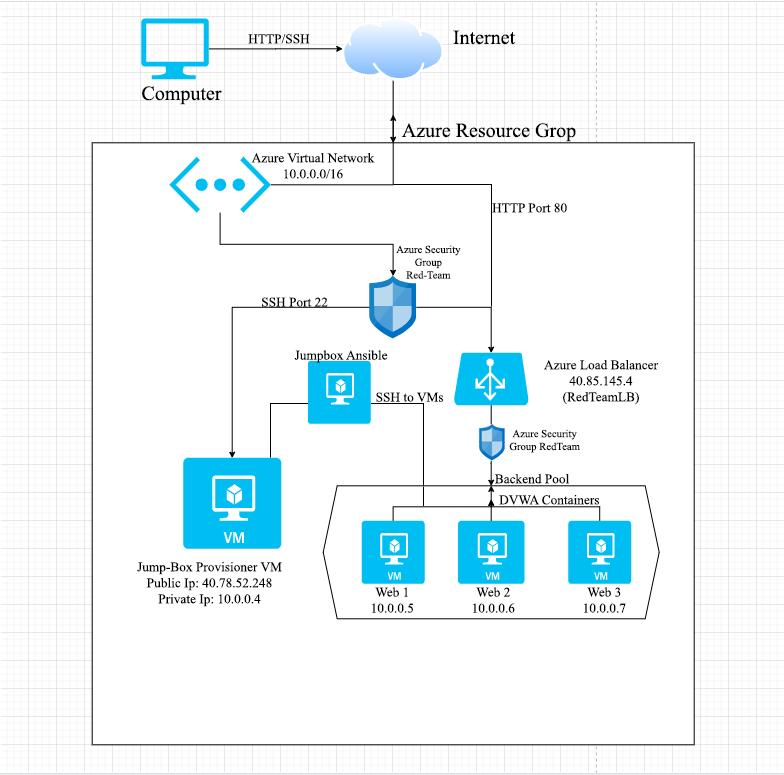
Part 3

OWASP

**What are we building?**

We are building a virtual network that is running on the Microsoft Azure cloud. In this cloud we have a total of four virtual machines that were created under a Virtual Network named “RedTeam”. Within this virtual network is the networks security group, with everything within the virtual network inside the network security group. One of the virtual machines is called the “Jump-box-provisioner”, this machine is setup with a Docker container that also has a Ansible Virtual Machine within it. From the Jumpbox I ssh into the Ansible virtual machine and from there I am able to connect to the other three virtual machines that have been configured with an Ansible virtual machine. The three virtual machines are called Web1/2/3 and are behind a Loadbalancer that has the three web virtual machines grouped into a backend pool. The three Web virtual machines are hosting the same webpage, and with the load balancer having them grouped into a backend pool, if one webserver goes down the other two are still running.



**Main Assets**

The main assets that we are going to try and protect is the data within the webservers, the website. The three webservers will be the main target since they will be hosting the website as well as the data for the website.

Website: This is one of the main assets we will focus on to try and secure from threat agents. The website will be what attracts traffic, and that traffic is a source of revenue. With the website being down, we will essentially be losing money.

Data: Aside from the actual website, the data within the webservers will also be especially important and must be protected and secured from threat agents as well. This data could be usernames/passwords, personal information, credit card information (if it were a website that sold items) and other various data that threats might exploit.

Possible Assets - Person Computer/Workstation: A possible asset that could be targeted is the computer that is connecting into the Azure website to run/manage the whole Virtual Network. This could also be a possible target of threat agents from the start, using the Azure virtual network as a way to recon and connect into the personal computer.

**Threat Agents/Potential Attacks**

Script Kiddies: Script kiddies can just randomly try and hack the website, the webservers or person just for fun or other various reasons. They don’t really have a motive other than to cause trouble/problems.

- DoS attack to temporarily shut down services

- Hack into a employee’s computer/work station, virtual machine or one of the webservers to cause trouble by destroying files and data.

Rival Websites: They have aim to either steal our data to get an edge over our website, or to compromise our virtual machines and network to ruin our brand. They could also sabotage our servers in order cause us damage by stopping the website or even destroying data and critical systems within the virtual machines.

-Sniffing data across the website in order to look into the data because the website is using http

-Hacking into a employee’s computer or the virtual machines in order to gain access to data that they can steal and use.

-Gaining access computers and virtual machines to cause trouble like deleting files.

Criminals: These threat actors are trying to hack into the network to either get data or information that they can use to make a gain financially.

-Sniffing the http traffic to recon

-Gaining access through port 22

-Exploiting outdated applications or firmware that the webservers are using, like Apache.

-Exploiting horrible coding within applications, for example the website itself is poorly coded

-Phishing attack on the employees to gain control of their computer, or infect that computer to further infect the network

Employees: Employees can be threats to the network. Either knowingly wanting to cause harm or unknowingly.

-A disgruntled employee might use old credentials that might not have been changed/deleted in order to access the network from another location to cause harm and damage the company

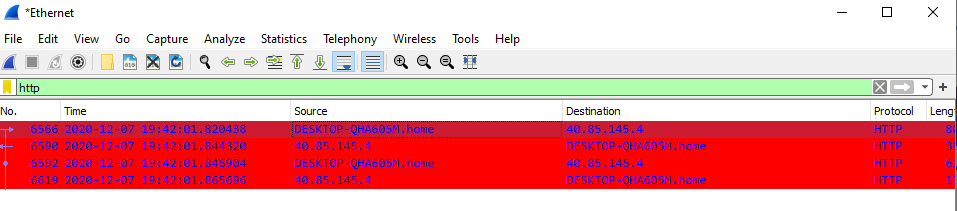
-Fall victim to a phishing attack or connecting to the network from an unsecure location

-Accessing unsecure websites

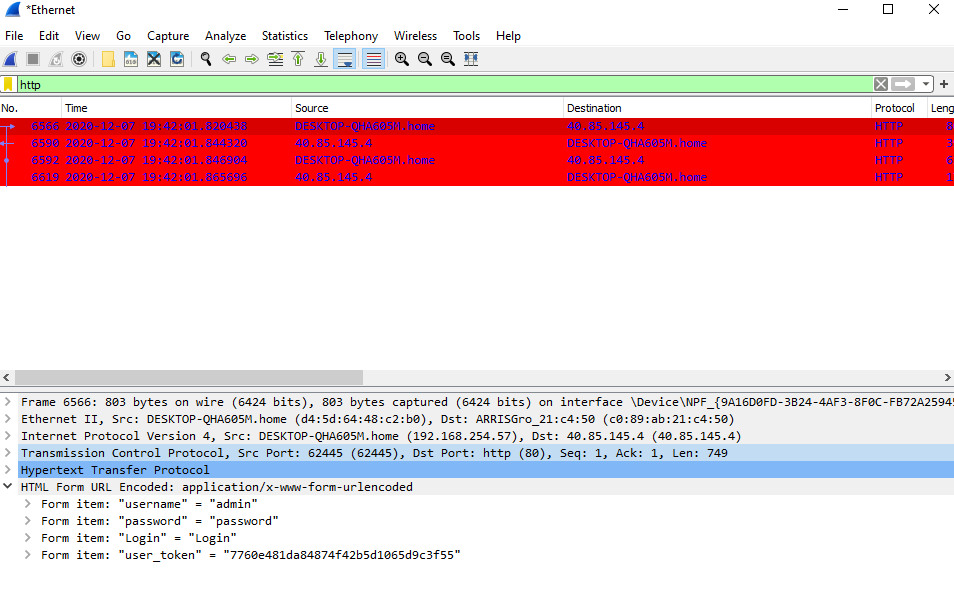
**Exploitable Vulnerabilities & Risk Analysis**

HTTP: Because http is not secure and unencrypted, it can easily be a subject of a Man-in-the-Middle attack. It can also be reconned by being monitored or use programs to sniff the traffic.

* Because http is unsecured, a MiTM attack can be used to record traffic within the network. A threat actor can use a program like “ettercap” listen in on the network traffic from the employee’s workstation. From there they can use “wireshark” to capture packets. Once they feel like they have enough packets, they can filter the packet by http (http)



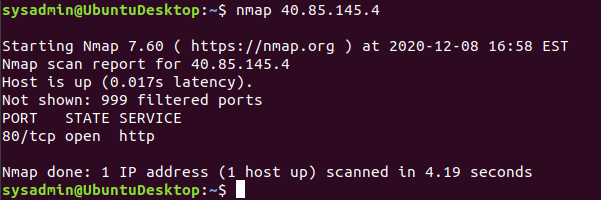
* Then they can look through the stolen packets for when the user input the username/password into the website.



HTTP Risk Analysis: The risk of this vulnerability being exploited is extremely high. This sort of vulnerability is also amazingly easy to exploit because the threat agent is just recording traffic that is going through the network. The threat actor simply needs to look through that data and can easily find the unencrypted data, the username and password. The impact of this exploited vulnerability is very severe, adding harmful links or even stealing information like other user data/logins. Because the exploitation of this risk is extremely high, while the execution of the attack is simple and easy, this vulnerability is a top priority to fix.

Bad Coding: The coding in which the DVWA website was written in is faulty and can be exploited to recon and gain information on the webserver that could be used to infiltrate the network.

* A threat actor can scan the ip to recon and look for vulnerabilities, like ports. Port 80 is a very common port that is known to be very common for unsecured http and sql injections.

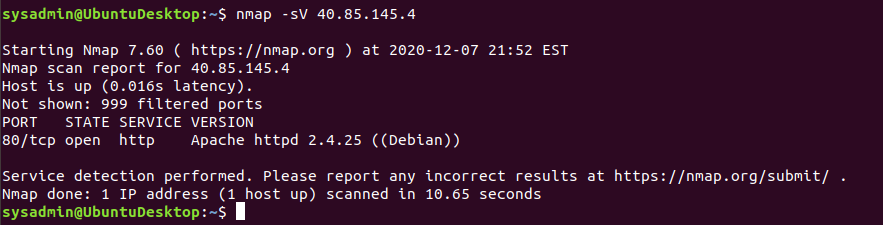


* Once confirming the open port (80), they test to see if he can use SQL injection attacks by first trying to confirm if its possible. Using a command on the url of the webpage like this (page=or 1=1–) and not getting a “Error” from the website shows that there are SQL vulnerabilities.

Bad Coding Risk Analysis: The risk for this vulnerability is also extremely high. Checking to see port 80 is open and being used along with a site that is http can show threat actors that this site is poorly planned and could be done by beginners, leading to them looking for basic vulnerabilities like sql injections within bad coding. The impact of this is very severe, threats can add their own malicious codes and even do recon to open look for more exploitable vulnerabilities.

Outdated services, modules, programs: Hackers can try and look for different vulnerabilities associated with outdated systems, services like Apache.

The risk of this code is very

* A simple nmap -sV 40.85.145.4 would show that Apache is being used along with its version. With this information a hacker can check to see if there is a vulnerability with the current version of Apache. 

Outdated Services Risk Analysis: This vulnerability is low because threat actors will need to hope that the systems they are aiming for should be outdated and sometimes be outdated in a certain version that is known to have a bug or exploit.

Employee Computer: The computers in which an employee is using can be the subject of attacks from hackers to gain access to the network. This can range from phishing attacks on the employee to trying to sniff the user’s traffic to gain control of the system.

* A threat actor can start a series of phishing attacks to get control of the employees’ computer. Being able to get control of the employee’s computer will enable the threat agent can get full access to the network.
* Another scenario could also be an employee also who isn’t being cautious or safe by signing into either the website through his admin account or by connecting to the network from an unsecure location or from home.
* A disgruntled employee can also want to cause harm by using his username/password for the website and logging onto it and causing trouble for various reasons like being fired. If the administrators aren’t doing their jobs right, the old workers admin account or user credentials for logging into the work computer is still active and not deleted/terminated.

**Risk Mitigation**

HTTP: The easiest way to fix this is to switch the website to HTTPS. Although there will be some cost switching it over, this will ensure that the traffic from the website is encrypted and cannot easily be read. This is by far the best step, even though there will be cost getting a SSL Certificate it will be worth is.

Bad Coding: This risk will likely require the hiring a professional that knows how to properly code a website. Also with the hiring of a professional to properly code the website, another cost might be to buy software that can help with locating missed vulnerabilities within the code.

Outdated Services: This risk can be mitigated by simply ensuring that all programs are up to date and running properly.

Employees: This risk will require different ways to tackle the multiple scenarios that could happen. First there needs to be a company mandatory training that covers multiple security related topics.

* How to identify malicious and fake emails.
* Not logging into the networks from unsecure locations
* To not access unsecure websites that might contain malicious programs.

The other scenario that needs to be addressed is with employees who’ve been terminated, administrators will need to make sure accounts of old employees are properly deleted and that their accounts are no longer useable within the system/network.