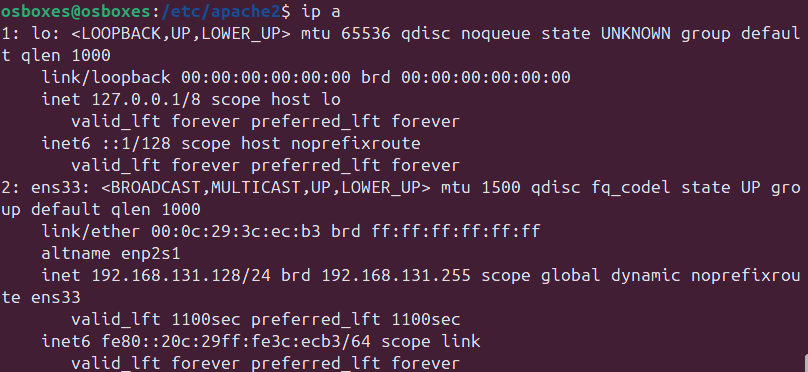
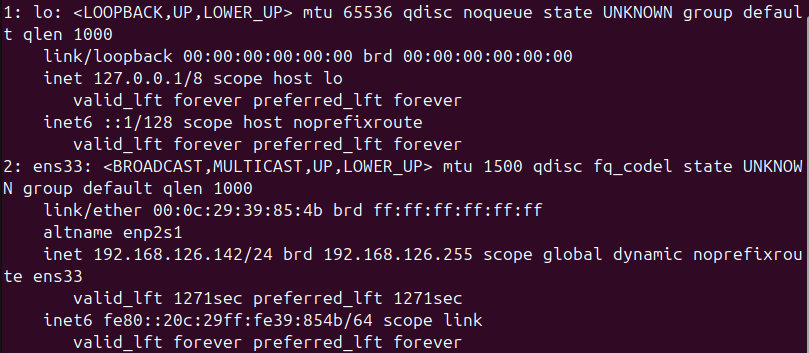
Assignment 1 – Discovery

ISEC2079

By Mohammad Al Jokhadar

Current IP Address configuration :

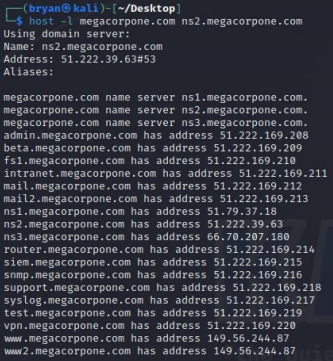




1. Who is the VP of legal and what is their Email address?

The **VP of Legal** is **Mike Carlow**. Their **Email Address** is [**mcarlow@megacorpone.com**](mailto:mcarlow@megacorpone.com). I have reached this information by browsing to the website, which I accessed from my Kali Linux at 192.168.126.142.

1. During class, we conducted a DNS zone transfer on MegaCorpOne’s name server. Given the list of subdomains we found, what subdomains look like good targets for an attack and why? Pickl 3 subdomains.



My choices would be (descending from most important down) :

1. **Admin.megacorpone.com**  
     
   Since the Administration Page would be usually holding administrator privileges on the website and beyond (if the ability to configure elements of the organization’s infrastructure is web-based, and added to the administrative page), it would prove invaluable for exploitation, as well as maintaining a foothold (by adding Reflected XSS code unto the page as an object etc.).
2. **Mail.megacorpone.com**

The human beings can easily be the weakest link in an organization’s security posture, and in accordance to the cybersecurity hacks of our modern times, it is extremely common as a gateway for attackers unto the organization’s network and assets. The mail server can be used for Phishing and Spear-Phishing campaigns, as we would obtain the organization’s email directory of employees ( and key targets for Spear-Phishing), as well as sending the Phishing emails by using the organization’s server to send them ( as it is a trusted mail domain), and potentially capture the templates used in emails by the organization for further Phishing attacks (if they do not change them). The use of the information found in that server could also pave the way for conducting a Social Engineering campagin as well ( as another entry point/lateral movement/privilege escalation, etc. )

1. **Vpn.megacorpone.com**  
     
   If the organization has multiple locations, such as branches, or offices in other countries for example, and they are all connected by this VPN server, compromising that server would provide the perfect means of lateral movement. Furthermore, if the organization’s employees work from home, then they can be excellent targets. since human beings are the weakest link, especially if they did not follow any procedures pertaining to protection against Phishing or Social Engineering campaigns , or there is a lack of training/guidelines pertaining to it. The attacks that would be done could involve Social Engineering and MFA Fatigue/Bypass Attack (especially dangerous if some sort of SIM Swapping attack is a part of it).

**Notable mentions :**

* **snmp.megacorpone.com**  
    
  Since the snmp protocol is used for network device analysis ( as well as other devices), it could provide us with information on the nodes on the network for further exploitation.
* **siem.megacorpone.com**

Since it is the collective hub of logs for the organization, we can use the information to evade being noticed by the organization’s logging infrastructure, as well as erasing tracks.

* **Router.megacorpone.com**

It is a valid target, as the potential for weak credentials/default credentials being in use is quite high (as attested by Shodan’s platform). It could be very helpful in internal target enumeration and lateral movement.

3. What email address does the contact-us form go to?

The email address that the form on the “Contact Us” page is supposed to be the [customer\_inquiery@megacorpone.com](mailto:customer_inquiery@megacorpone.com) email address, due to this lovely memo that was in the page’s source code :



Screenshot of the comment mentioning the email address to direct emails to (on *http://192.168.126.142/contact.html*)

Alternatively , we could use **FoxyProxy/Wireshark** to submit some information in the Contact Us form, and then examine the contents of the packet.

4. When was the site last updated?

The site was last updated in 2023, with the exception of the About page being from 2017.

5. Can you find the secret message and what does it say? (4 points)

<!-- Timm: remember to direct the form to customer\_inquiery@megacorpone.com-->

6.Plan out a social engineering attack against a target of your choosing. You may use any number of attacks (email phishing, vishing, etc.) in an attempt to gain initial access into MegaCorpOne’s environment (credentials, workstation access, M365, VPN, etc.). You must explain each step of the attack including what you would say to the target, who you are pretending to be (if applicable), why you chose the target, and list potential replies to your social engineering. (12 points)

My attack strategy would involve a number of different strategies:

## Email Phishing Strategy

1. Since I would need a trusted domain to send Phishing emails from, I would utilize the Contact Us form. The following note on the Contact Us page’s source code tells us :   
     
   Timm: remember to direct the form to [customer\_inquiery@megacorpone.com](mailto:customer_inquiery@megacorpone.com)
2. I would fake create LinkedIn profiles for the following three positions (with lots of fake experience):

**Citrix Administrator**

Maintain, secure, and expand the MegaCorp One Citrix installation. Applicant must be well versed with remote work conditions and understand endpoint security solutions.   
( a clue for an oncoming attack)

**Firewall Administrator**

Position is responsible for the administration of the Firepass firewall. Applicant must have at least 3 years experience with firewall administration and 5 years networking experience.

(This tells us the type of Firewall being utilized. This would be helpful)

**Sales Representative**

MegaCorp One is involved in selling various substances. Representatives must have demonstrable experience in all manner of sales situations. Contact us for details.

(Another clue)

1. I would open an avenue of communication on LinkedIn Chat with an HR representative for MegaCorpOne ( to establish an ongoing rapport with the HR department).   
     
   At the same time,   
     
   I would use the Contact Us section of the page to send AI-generated emails pertaining to each of the three employment positions.   
      
   The contents of the starting chat on LinkedIn :  
      
   “Hello,  
      
   My name is Bob, and I am really interested in pursuing a career with MegaCorpOne. I believe my qualifications speak for themselves …” list fake accomplishments, and then ask questions about the position.   
     
   When the gracious HR department responds via LinkedIn or email :   
     
   “Thank you for your interest in MegaCorpone! Please send me your resume and portfolio!”   
     
   I would also start a conversation from three different fake LinkedIn profiles created for each position ( Citrix , Firepass Firewall, and Sales). The goal is to establish a line of communications and built rapport and trust!

After three emails or so, when the moment arrives to provide my credentials, portfolio and resumes, I would generate a QR code for a shortened link to my fake portfolio or to a short video I recorded (due to my social anxiety) on a malicious yet innocent-looking domain. The link would pull a Rubber Ducky script to edit the C:\Windows\System32\drivers\etc\hosts file, and add the Kali Linux VM’s IP address and the domain information for another camouflaged Office365 fake domain to use with Evilginx 2.0. When the HR department asks for a resume, I would mention that they can reach it via the following Mircosoft Office 365 link. The HR personnel would be duped into logging in to their Office365 account from the fake mircosoft domain, with me waiting for Evilginx 2.0 to provide the session cookie! I would then use the session cookie to login to the Sales department’s email account, and send emails to the delivery department pertaining to a new client that requires a shipment, with a malicious link containing a realistic-looking shipping label (photoshopped and adapted to a new fake client). The malicious link would pull a TCP reverse shell, and would attempt to pull the Rubber Ducky script from before ( to edit etc\hosts file to another fake Office365 domain) as well as a TCP reverse shell. The email would be pertaining to an Excel spreadsheet for all the products that need to be shipped to the fake new client. I would use Artificial Intelligence to mimic the organization’s email template and the writing style of the personnel who work in the department to send further internal malicious emails

If the person that follows the Customer-Enquiry email address decides to go for either of the three emails, we would get a foothold unto that employee’s account privileges to send further phishing emails throughout the organization.

If they ignore the emails :

## Phone-based Social Engineering

1. I would call the MegaCorpOne’s office phone number, and pretend to be an interested Sales representative from an organization based in the US, specializing in the manufacturing of FIPS-certificed Nanotech-activated secure flash drives.
2. Since the MegaCorpOne organization is fine with selling a variety of items, they could potentially accept a sample ( which would contain the Ducky Script). If they do, a malicious-yet-innocent looking USB drive in a shiny exterior shell would arrive via mail, laden with malware!  
      
     
   Another phone call …  
      
     
   1. I would use AI to conduct a Vishing campaign , after doing OSINT work on the information found on LinkedIn, leading through lateral movement to the individual’s social media account. If they have plenty of videos, that would provide a sample to replicate their speech patterns for AI.

2. I would then launch a Denial of Service against the vpn.megacorpone.com domain. I would call the organization, pretending to be that employee, and mention on the phone call that I am having issues connecting to the VPN server.

3. If I am directed to contact IT or Citrix Support, I would attempt to copy the voice of the CEO (if they post videos on social media), and mention an issue with the Citrix VPN login.

Another phone call …

(Immediately before third the phone call, another Denial of Service attack is launched against vpn.megacorpone.com … )

I would wait a few minutes, and then call the organization’s phone number. I would declare myself as an IT specialist from Citrix , and ask to speak to the organization’s IT specialist.

When speaking to the IT specialist, I would mention that we are aware of the issues happening with the organization’s VPN connections. I would pretend to type really fast on the keyboard, and then mention that there is a need to reset the VPN credentials for the IT specialist, and every employee of the organization who works-from-home.

I will mention that it is arriving via email.

I would call again, reporting an issue with emails not being delivered. I would ask then to check the Junk mail folder (since I would send it from a suspicious domain), and include the link as a QR code in the email, as well as a link ( and mention QR codes makes your life easier). I would then ask for an alternative method to send it, just in case. I would ask them for their own mobile phone number to send it as a text message, as I have a lot of work to do to resolve this from my end …

The link in the email and SMS message would lead to a malicious camoflagued domain (with some replaced letters) resembling the reset password link used by Citrix. The link would keep failing, and I would let the individual on the phone know that we are still working on the issue, and to pass the link in an internal email to every work-from-home employee’s email inbox. The link would keep reloading the page, the person would complain it is not working, and then we would ask them for their credentials. Then I would ask them to login with their Office365 credentials. I would at the same time conduct a MFA Fatigue attack repeatedly when detecting a successful credential gain in Evilginx 2.0.

If I do obtain credentials successfully for the IT manager, I would gain privileges to their email account, and spread the fake password reset link ( as well as comforting them that MFA may be a bit glitchy, and that we appreciate their patience).

If the Citrix Jumpbox is misconfigured to allow access to the organization’s file servers, I would maintain persistence with In-Memory Meterpreter-based malware on as many nodes as possible, as well as exfiltrating the employees’ internal email addresses for further social engineering.

If the reverse shell runs on any of the organization’s systems, I would utilize the organization’s internal messaging services ( such as Microsoft Teams or Slack ) and further spread malware by matching the employee’s writing patterns and personality with AI. The IT specialist’s computer would be ideal for this, as I would inform employees of the Citrix-related issues, and ask them to reset their credentials, and install an important security update!