Attacking a Virtual Private Network (3e)

Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 04

Student: Christian Barba	Email: christianbarba527@gmail.com

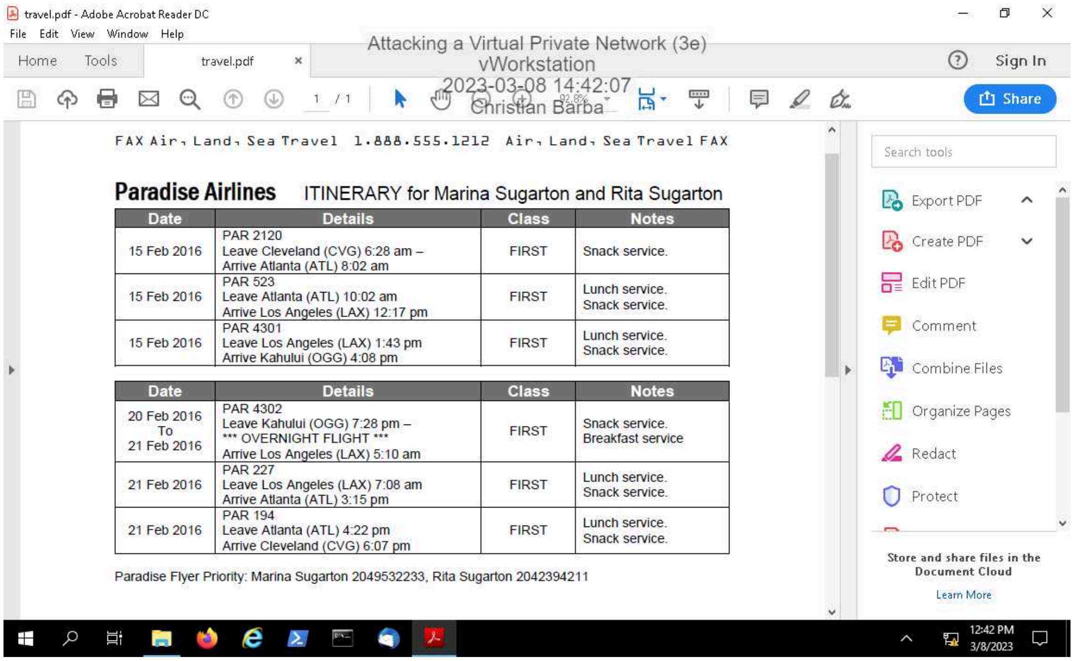
Time on Task: 8 hours, 12 minutes	Progress: 100%

Report Generated: Thursday, March 9, 2023 at 2:09 PM

Section 1: Hands-On Demonstration

Part 1: Observe a Social Engineering Attack

10. **Make a screen capture** showing the **entire travel itinerary for Marina and Rita**.



FAX Air, Land, Sea Travel 1.888.555.1212 Air, Land, Sea Travel FAX

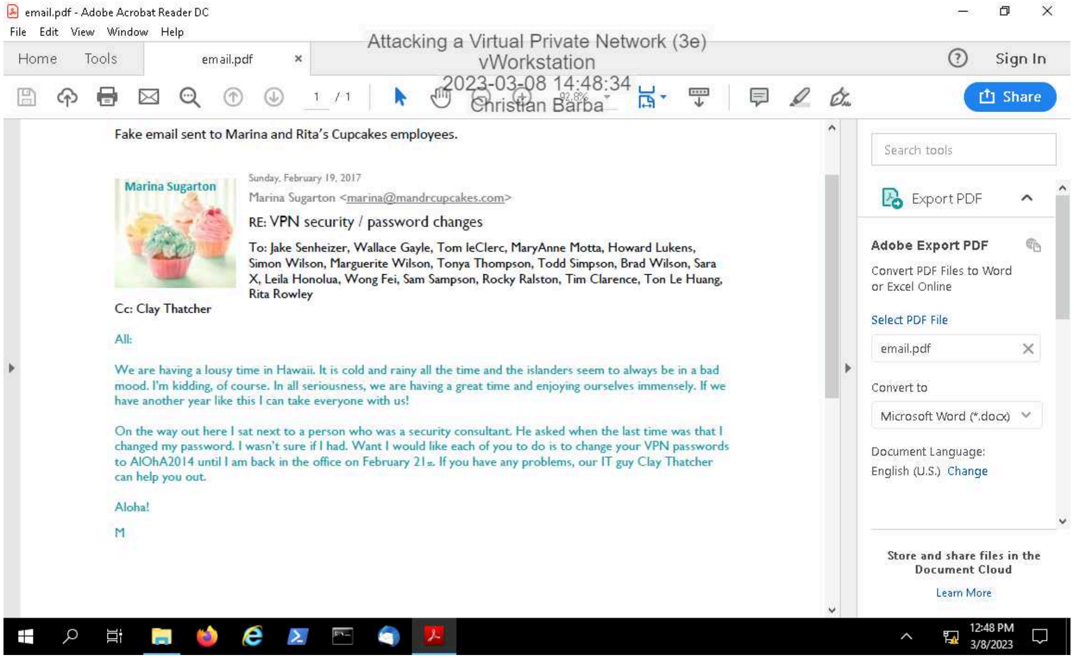
Paradise Airlines ITINERARY for Marina Sugarton and Rita Sugarton

Date	Details	Class	Notes
15 Feb 2016	PAR 2120 Leave Cleveland (CVG) 6:28 am – Arrive Atlanta (ATL) 8:02 am	FIRST	Snack service.
15 Feb 2016	PAR 523 Leave Atlanta (ATL) 10:02 am Arrive Los Angeles (LAX) 12:17 pm	FIRST	Lunch service. Snack service.
15 Feb 2016	PAR 4301 Leave Los Angeles (LAX) 1:43 pm Arrive Kahului (OGG) 4:08 pm	FIRST	Lunch service. Snack service.

Date	Details	Class	Notes
20 Feb 2016 To 21 Feb 2016	PAR 4302 Leave Kahului (OGG) 7:28 pm – *** OVERNIGHT FLIGHT *** Arrive Los Angeles (LAX) 5:10 am	FIRST	Snack service. Breakfast service
21 Feb 2016	PAR 227 Leave Los Angeles (LAX) 7:08 am Arrive Atlanta (ATL) 3:15 pm	FIRST	Lunch service. Snack service.
21 Feb 2016	PAR 194 Leave Atlanta (ATL) 4:22 pm Arrive Cleveland (CVG) 6:07 pm	FIRST	Lunch service. Snack service.

Paradise Flyer Priority: Marina Sugarton 2049532233, Rita Sugarton 2042394211

16. **Make a screen capture** showing **Marina's email**.



Attacking a Virtual Private Network (3e)
vWorkstation
2023-03-08 14:48:34
Christian Barba

Fake email sent to Marina and Rita's Cupcakes employees.

Marina Sugarton

Sunday, February 19, 2017
Marina Sugarton <marina@mandrcupcakes.com>
RE: VPN security / password changes
To: Jake Senheizer, Wallace Gayle, Tom leClerc, MaryAnne Motta, Howard Lukens, Simon Wilson, Marguerite Wilson, Tonya Thompson, Todd Simpson, Brad Wilson, Sara X, Leila Honolua, Wong Fei, Sam Sampson, Rocky Ralston, Tim Clarence, Ton Le Huang, Rita Rowley
Cc: Clay Thatcher

All:

We are having a lousy time in Hawaii. It is cold and rainy all the time and the islanders seem to always be in a bad mood. I'm kidding, of course. In all seriousness, we are having a great time and enjoying ourselves immensely. If we have another year like this I can take everyone with us!

On the way out here I sat next to a person who was a security consultant. He asked when the last time was that I changed my password. I wasn't sure if I had. Want I would like each of you to do is to change your VPN passwords to AlOhA2014 until I am back in the office on February 21st. If you have any problems, our IT guy Clay Thatcher can help you out.

Aloha!

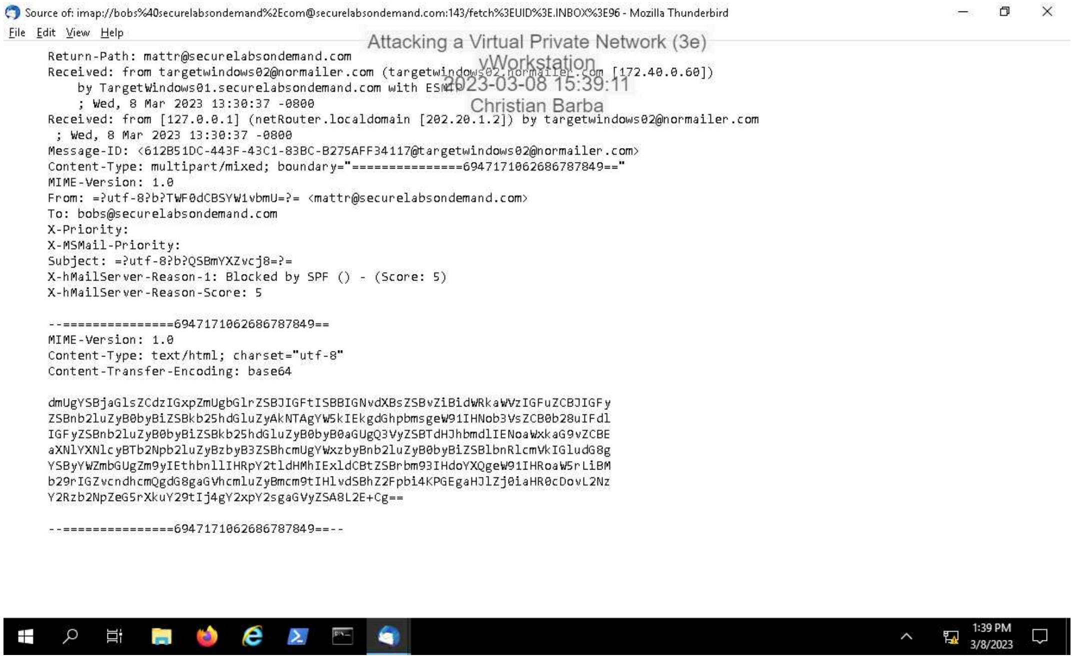
M

Part 2: Craft a Spear Phishing Email

4. **Describe** your favorite scam email or an example of a scam email that you have received in the past.

My favorite scam email is where the person trying to get access to my account claims that I need to verify all of my information or else my account will be deleted. This happened to my UTSA account once. I had received an email from a random person claiming to be a UTSA student stating that their records show I was trying to delete my school email account (I wasn't). They sent me a link that looked real, but I knew it wasn't since it didn't come from an official company. I ended up showing the email to my professor at the time, and he warned the rest of the class of this phishing scam that was starting to float arouind campus.

33. **Make a screen capture** showing the ***Blocked by SPF*** **message in the email headers**.



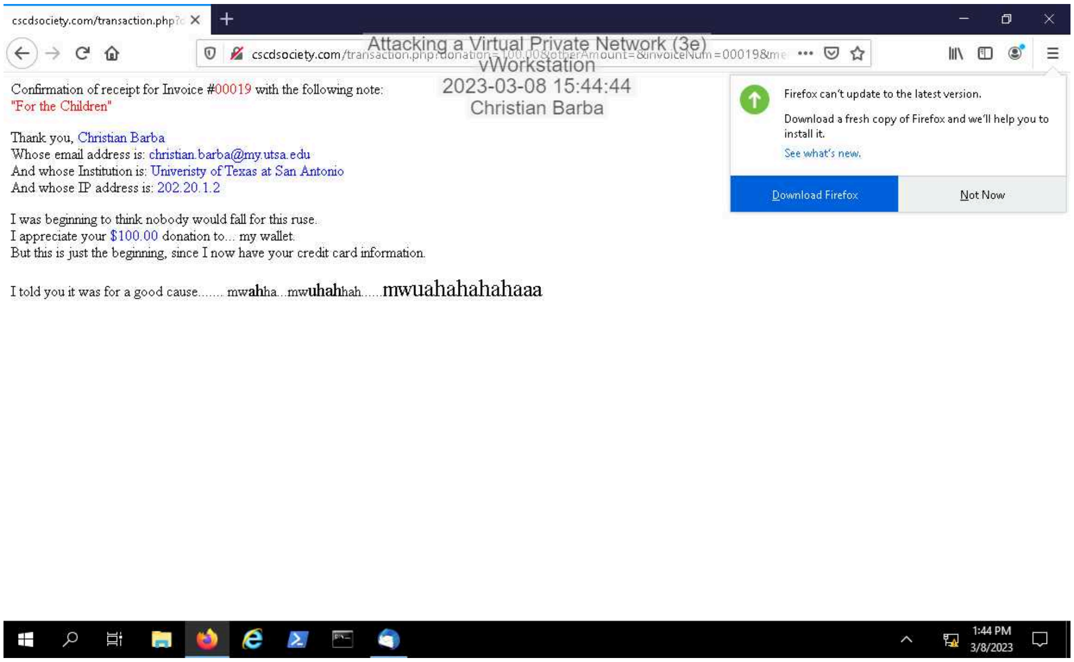
Source of: imap://bobs%40securelabsondemand%2Ecom@securelabsondemand.com:143/fetch%3EUID%3E.INBOX%3E96 - Mozilla Thunderbird
File Edit View Help
Attacking a Virtual Private Network (3e)
vWorkstation
2023-03-08 15:39:11
Christian Barba
1:39 PM
3/8/2023

```
Return-Path: mattr@securelabsondemand.com
Received: from targetwindows02@normailer.com (targetwindows02.normailer.com [172.40.0.60])
    by TargetWindows01.securelabsondemand.com with ESMTP
    ; Wed, 8 Mar 2023 13:30:37 -0800
Received: from [127.0.0.1] (netRouter.localdomain [202.20.1.2]) by targetwindows02@normailer.com
 ; Wed, 8 Mar 2023 13:30:37 -0800
Message-ID: <612B51DC-443F-43C1-83BC-B275AFF34117@targetwindows02@normailer.com>
Content-Type: multipart/mixed; boundary="===============6947171062686787849=="
MIME-Version: 1.0
From: =?utf-8?b?TWF0dCBSYW1vbmU=?= <mattr@securelabsondemand.com>
To: bobs@securelabsondemand.com
X-Priority:
X-MSMail-Priority:
Subject: =?utf-8?b?QSBmYXZvcj8=?=
X-hMailServer-Reason-1: Blocked by SPF () - (Score: 5)
X-hMailServer-Reason-Score: 5

--===============6947171062686787849==
MIME-Version: 1.0
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: base64
```

```
dmUgYSBjaGlsZCdzIGxpZmUgbGlrZSBJIGFtISBBIGNvdXBsZSBvZiBidWRkaWVzIGFuZCBJIGFy
ZSBnb2luZyB0byBiZSBkb25hdGluZyAkNTAgYW5kIEkgdGhpbmsgeW91IHNob3VsZCB0b28uIFdl
IGFyZSBnb2luZyB0byBiZSBkb25hdGluZyB0byB0aGUgQ3VyZSBTdHJhbmdlIENoaWxkaG9vZCBE
aXNlYXNlcyBTb2Npb2luZyBzbyB3ZSBhcmUgYWxzbyBnb2luZyB0byBiZSBlbnRlcmVkIGludG8g
YSByYWZmbGUgZm9yIEthbnllIHRpY2tldHMhIExldCBtZSBrbm93IHdoYXQgeW91IHRoaW5rLiBM
b29rIGZvcndhcmQgdG8gaGVhcmluZyBmcm9tIHlvdSBhZ2Fpbi4KPGEgaHJlZj0iaHR0cDovL2Nz
Y2Rzb2NpZXR5LmNvbS8+IGxpY2sgaGVyZSA8L2E+Cg==
```

```
--===============6947171062686787849==--
```

43. **Make a screen capture** showing the **transaction.php page in the browser**.



cscdsociety.com/transaction.php?c
cscdsociety.com/transaction.php?donation=100.00&otherAmount=&invoiceNum=00019&me
Attacking a Virtual Private Network (3e)
vWorkstation
2023-03-08 15:44:44
Christian Barba
1:44 PM
3/8/2023

Confirmation of receipt for Invoice #00019 with the following note:
"For the Children"

Thank you, Christian Barba
Whose email address is: christian.barba@my.utsa.edu
And whose Institution is: Univeristy of Texas at San Antonio
And whose IP address is: 202.20.1.2

I was beginning to think nobody would fall for this ruse.
I appreciate your $100.00 donation to... my wallet.
But this is just the beginning, since I now have your credit card information.

I told you it was for a good cause....... mw**ah**ha...mw**uhah**hah......mwuahahahahaaa

Firefox can't update to the latest version.

Download a fresh copy of Firefox and we'll help you to install it.

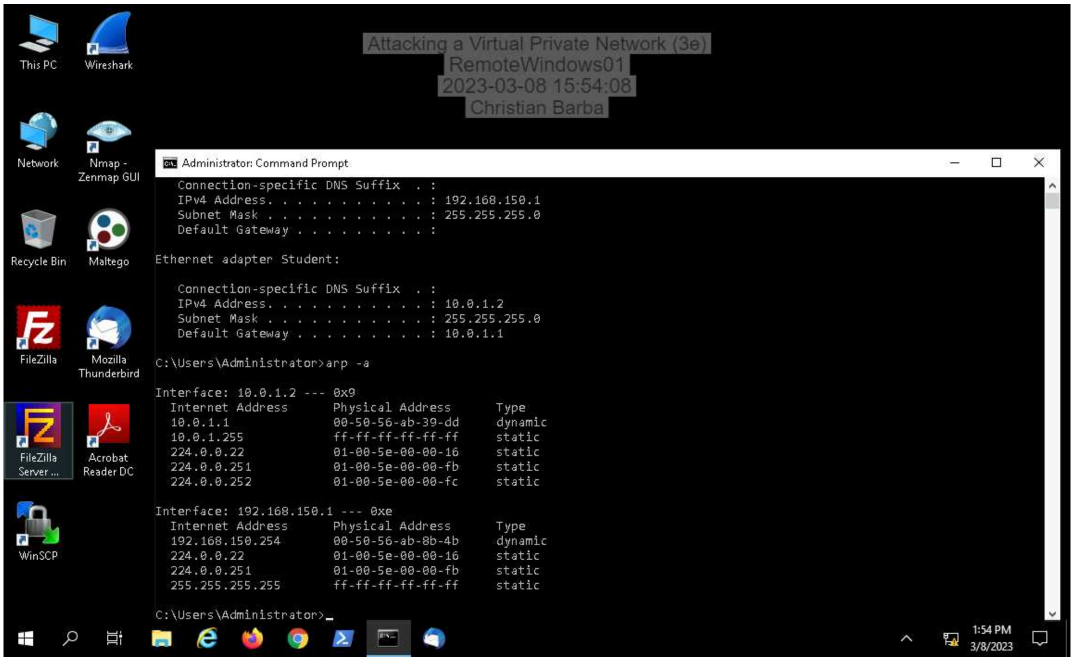
See what's new.

Download Firefox | Not Now

Section 2: Applied Learning

Part 1: Perform a Man-in-the-Middle Attack

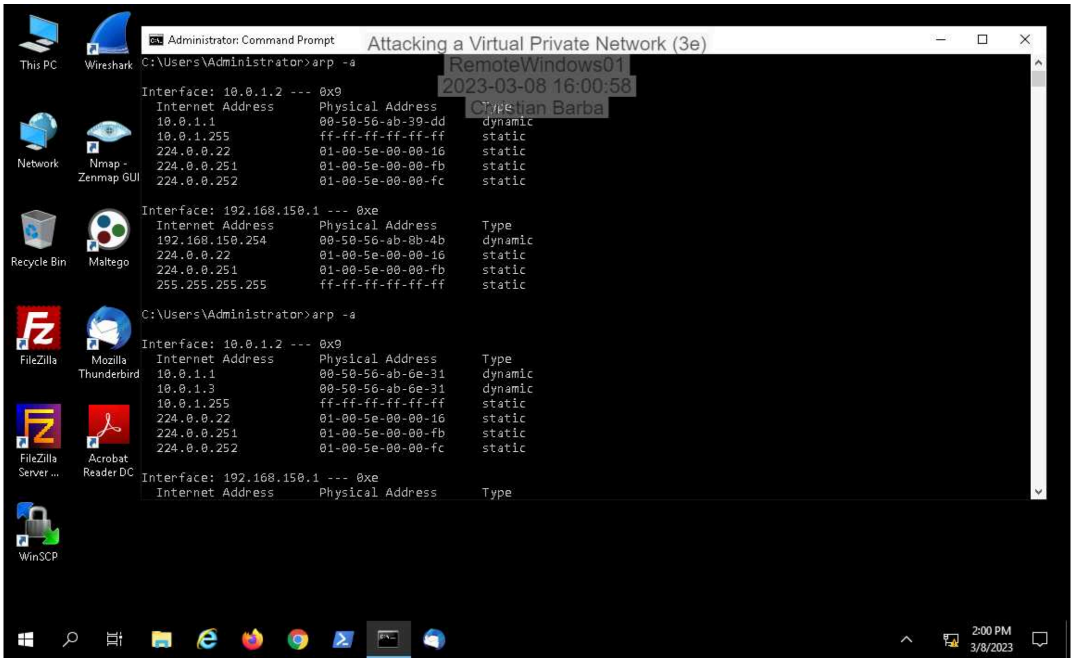
5. **Make a screen capture** showing the **RemoteWindows01 ARP table**.



Attacking a Virtual Private Network (3e)
RemoteWindows01
2023-03-08 15:54:08
Christian Barba

```
   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.150.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Student:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- 0x9
  Internet Address      Physical Address      Type
  10.0.1.1              00-50-56-ab-39-dd     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.150.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.150.254       00-50-56-ab-8b-4b     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>_
```

17. **Make a screen capture** showing the **RemoteWindows01 ARP table after the ARP poisoning**.

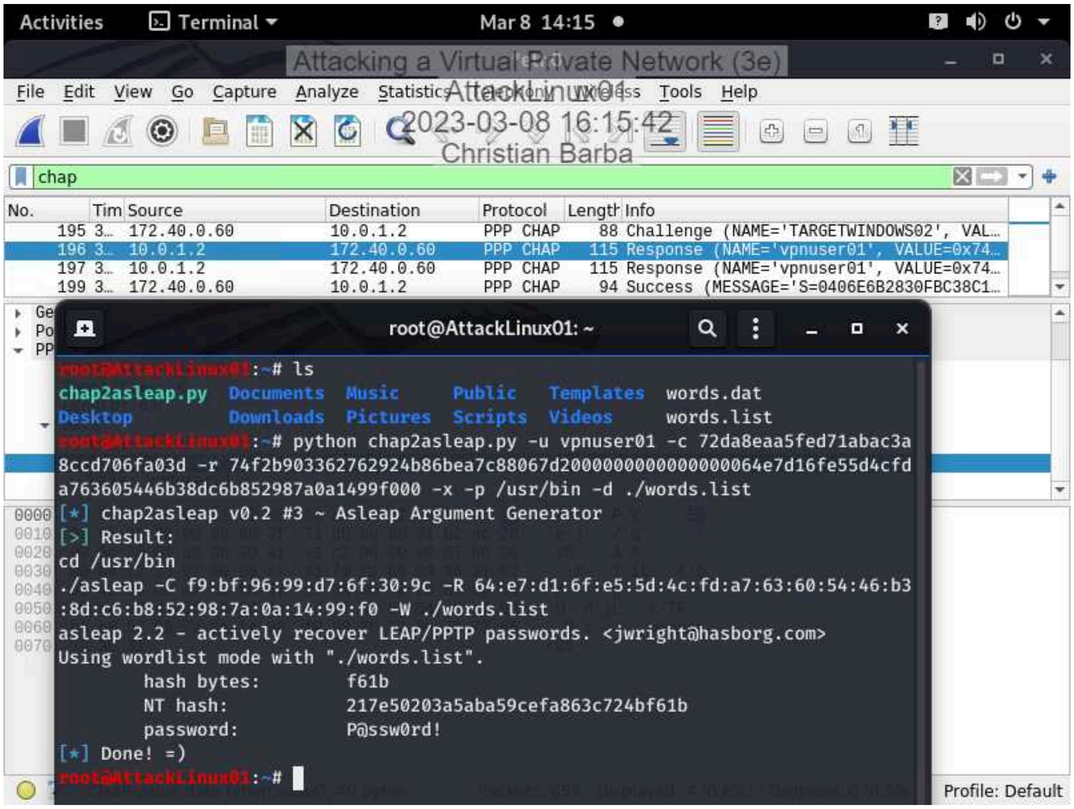


Attacking a Virtual Private Network (3e)
RemoteWindows01
2023-03-08 16:00:58
Christian Barba

```
C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- 0x9
  Internet Address      Physical Address      Type
  10.0.1.1              00-50-56-ab-39-dd     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.150.1 --- 0xe
  Internet Address      Physical Address      Type
  192.168.150.254       00-50-56-ab-8b-4b     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Administrator>arp -a

Interface: 10.0.1.2 --- 0x9
  Internet Address      Physical Address      Type
  10.0.1.1              00-50-56-ab-6e-31     dynamic
  10.0.1.3              00-50-56-ab-6e-31     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.150.1 --- 0xe
  Internet Address      Physical Address      Type
```

Part 2: Crack a VPN Password using Captured Packets

12. **Make a screen capture** showing the **cracked VPN password**.



```
No.   Tim Source        Destination   Protocol  Length Info
  195 3…  172.40.0.60   10.0.1.2      PPP CHAP    88 Challenge (NAME='TARGETWINDOWS02', VAL…
  196 3…  10.0.1.2      172.40.0.60   PPP CHAP   115 Response (NAME='vpnuser01', VALUE=0x74…
  197 3…  10.0.1.2      172.40.0.60   PPP CHAP   115 Response (NAME='vpnuser01', VALUE=0x74…
  199 3…  172.40.0.60   10.0.1.2      PPP CHAP    94 Success (MESSAGE='S=0406E6B2830FBC38C1…
```

```
root@AttackLinux01:~# ls
chap2asleap.py  Documents  Music     Public   Templates  words.dat
Desktop         Downloads  Pictures  Scripts  Videos     words.list
root@AttackLinux01:~# python chap2asleap.py -u vpnuser01 -c 72da8eaa5fed71abac3a
8ccd706fa03d -r 74f2b903362762924b86bea7c88067d2000000000000000064e7d16fe55d4cfd
a763605446b38dc6b852987a0a1499f000 -x -p /usr/bin -d ./words.list
[*] chap2asleap v0.2 #3 ~ Asleap Argument Generator
[>] Result:
cd /usr/bin
./asleap -C f9:bf:96:99:d7:6f:30:9c -R 64:e7:d1:6f:e5:5d:4c:fd:a7:63:60:54:46:b3
:8d:c6:b8:52:98:7a:0a:14:99:f0 -W ./words.list
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "./words.list".
        hash bytes:        f61b
        NT hash:           217e50203a5aba59cefa863c724bf61b
        password:          P@ssw0rd!
[*] Done! =)
root@AttackLinux01:~#
```

Section 3: Challenge and Analysis

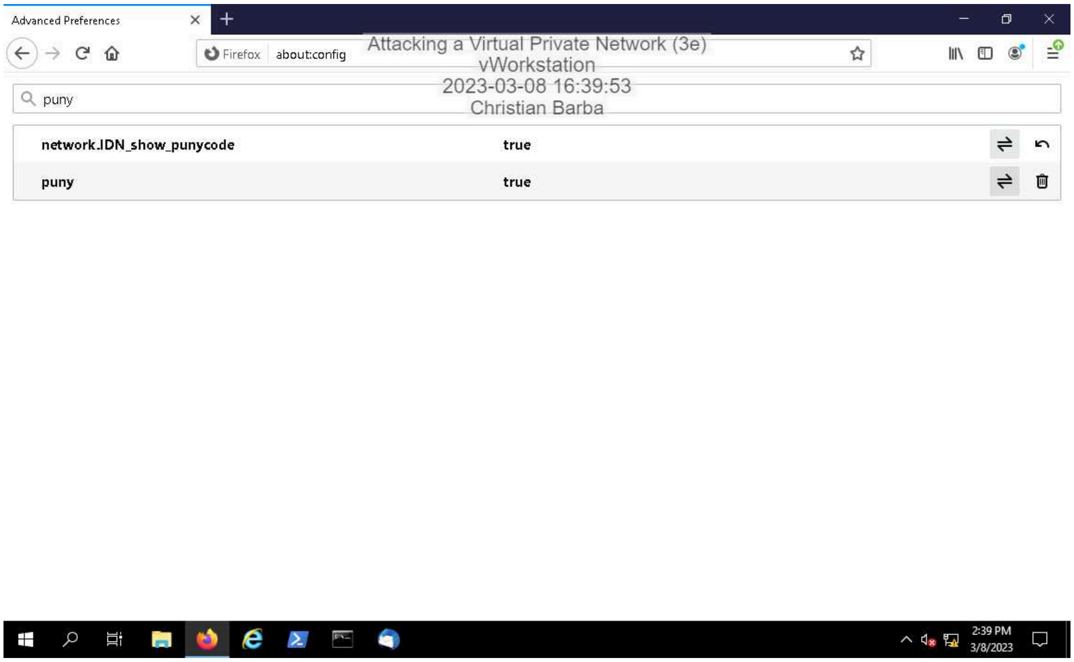
Part 1: Recommend Additional Spam Filtering Mechanisms

Describe the role of the DKIM and DMARC in a mailing infrastructure, and how these implementations help to prevent email forgery. Use the Internet to perform your research on these mechanisms.

Both DKIM and DMARC are in a trio of mail authentication according to Microsoft. DKIM is used as a way to ensure that the domain name is legitimate by adding a digital signature in the message header. The way DKIM works is that there is a private key associated with the outgoing email that the receiving participants are able to decrypt. They are able to decrypt it because the public key is uploaded to the DNS records for that specific domain, so people that obtain access to said email will be able to view it. This is all used to ensure that the person is who they say they are and the email address from the sender cannot be spoofed.
DMARC acts as a verifier behind the scenes. There are two different addresses that a person can mail an email from, the "Mail from address" and the "From address". The mail from address is used to show who really sent the email and the from address is used to show the author of the message. The way DMARC works is that it checks the domain that the from address came from is legitimate or not. In other words, it is used to validate that the servers the emails are coming from are linked to the user that is sending the email. There could malicious actors trying to pose as someone else, but the DMARC will be able to spot any suspicious activity.

Part 2: Enable Punycode Translation in Firefox

Make a screen capture showing the **enabled Display Punycode setting in Firefox**.

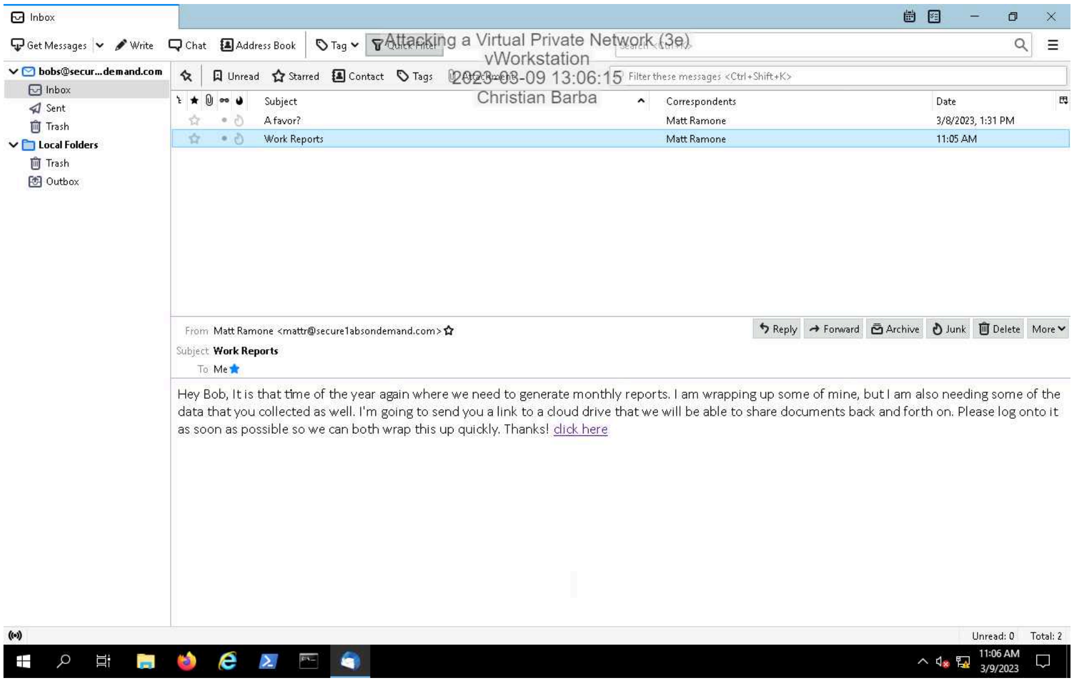


puny

network.IDN_show_punycode	true
puny	true

Part 3: Perform a Phishing Attempt to Test User Security Awareness

Make a screen capture showing the **email message headers** in Thunderbird.

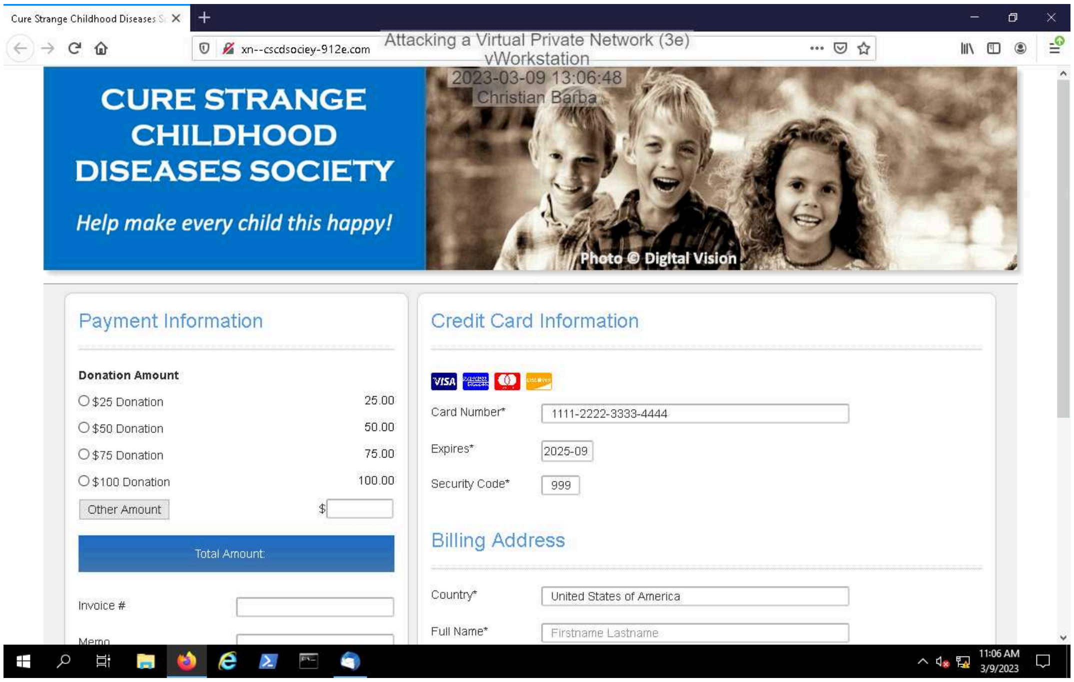


Subject	Correspondents	Date
A favor?	Matt Ramone	3/8/2023, 1:31 PM
Work Reports	Matt Ramone	11:05 AM

From Matt Ramone <mattr@secure1absondemand.com>
Subject **Work Reports**
To Me

Hey Bob, It is that time of the year again where we need to generate monthly reports. I am wrapping up some of mine, but I am also needing some of the data that you collected as well. I'm going to send you a link to a cloud drive that we will be able to share documents back and forth on. Please log onto it as soon as possible so we can both wrap this up quickly. Thanks! click here

Make a screen capture showing the **Punycode displayed** in the Firefox web browser.



Cure Strange Childhood Diseases S
xn--cscdsociey-912e.com
CURE STRANGE CHILDHOOD DISEASES SOCIETY
Help make every child this happy!
Photo © Digital Vision
11:06 AM
3/9/2023

Payment Information

Donation Amount

○ $25 Donation	25.00
○ $50 Donation	50.00
○ $75 Donation	75.00
○ $100 Donation	100.00
Other Amount	$

Total Amount:

Invoice #

Memo

Credit Card Information

Card Number* 1111-2222-3333-4444

Expires* 2025-09

Security Code* 999

Billing Address

Country* United States of America

Full Name* Firstname Lastname