CMPUT 333

Your Own Certificate Authority

Certificate Authority

Make a CA (Certificate Authority) and sign a server certificate with it.

- HTTP server (port 8080) on your virtual Windows host

- Add HTTPS service (port 443)
  - Add a certificate for the https server
  - Enable encrypted access
  - **Openssl: Use it to generate private keys, etc.**

Generate your own CA

Steps

1. First generate the Certificate Authority key
2. Use the Certificate Authority **key** to build the **certificate** itself

- **Be careful!**
  - The Common Name (CN) of the **CA certificate** and the **server certificate** must NOT match
  - The CA certificate's organization name should be **"GroupXX_F16"** where XX is your group ID
  - You are free to edit the remaining requested fields or you can leave them blank

Generate your own CA

1. Generate a server key and request for signing (.csr)

   - The certificate request's (.csr) organization name should be **"GroupXX_F16 Web Services"** where XX is your group ID
   - The Common Name (CN) as you generate the .csr file should match the **IP address** you specify in your Apache configuration (again this should **not match with the CA Common Name**)
   - Remember: the IP of your Windows VM: 10.229.XX.2, where XX is your group ID
   - You are free to edit the remaining requested fields or you can leave them blank

Generate your own CA

1. Sign the certificate signing request (csr) with your "CA" private key.
   - The policy should be set to **policy_anything.**

2. Create an " insecure " version of the server.key.
   - The insecure version will be used for when Apache starts
   - The server will not require a password with every restart of the web server

Generate your own CA

- Configure your web server to use the "GroupXX_F16 Web Services"
    - Include the appropriate keys and certificates that you produced
    - Load the appropriate modules
    - Pay attention to the ServerName
    - Remember to restart your server after your configuration
    - Remember to add an exception for port 443 in your Windows Firewall

Generate your own CA

- Use the web browser on the virtual Windows host to access your web server
  - Verify that it does not recognize the certificate authority that signed the certificate when you try:
    - **https:**//10.229.XX.2/
  - Take a screenshot!!!
  - Load your self-signed certificate into your browser
  - Try again to access your server's content and show that it is now successful
  - Take a screenshot!!!

Generate your own CA

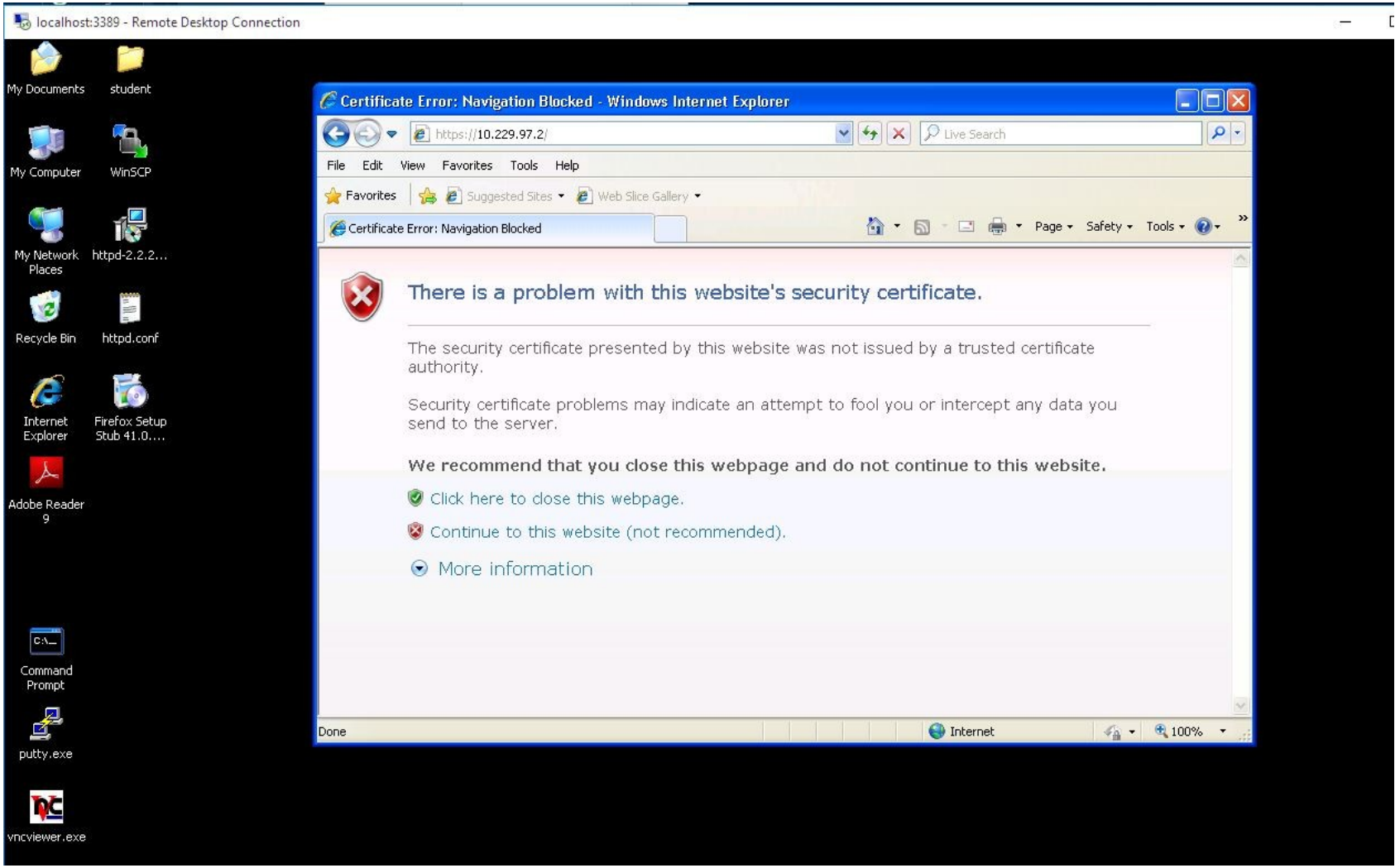

Figure 1. : Before loading the CA

Generate your own CA

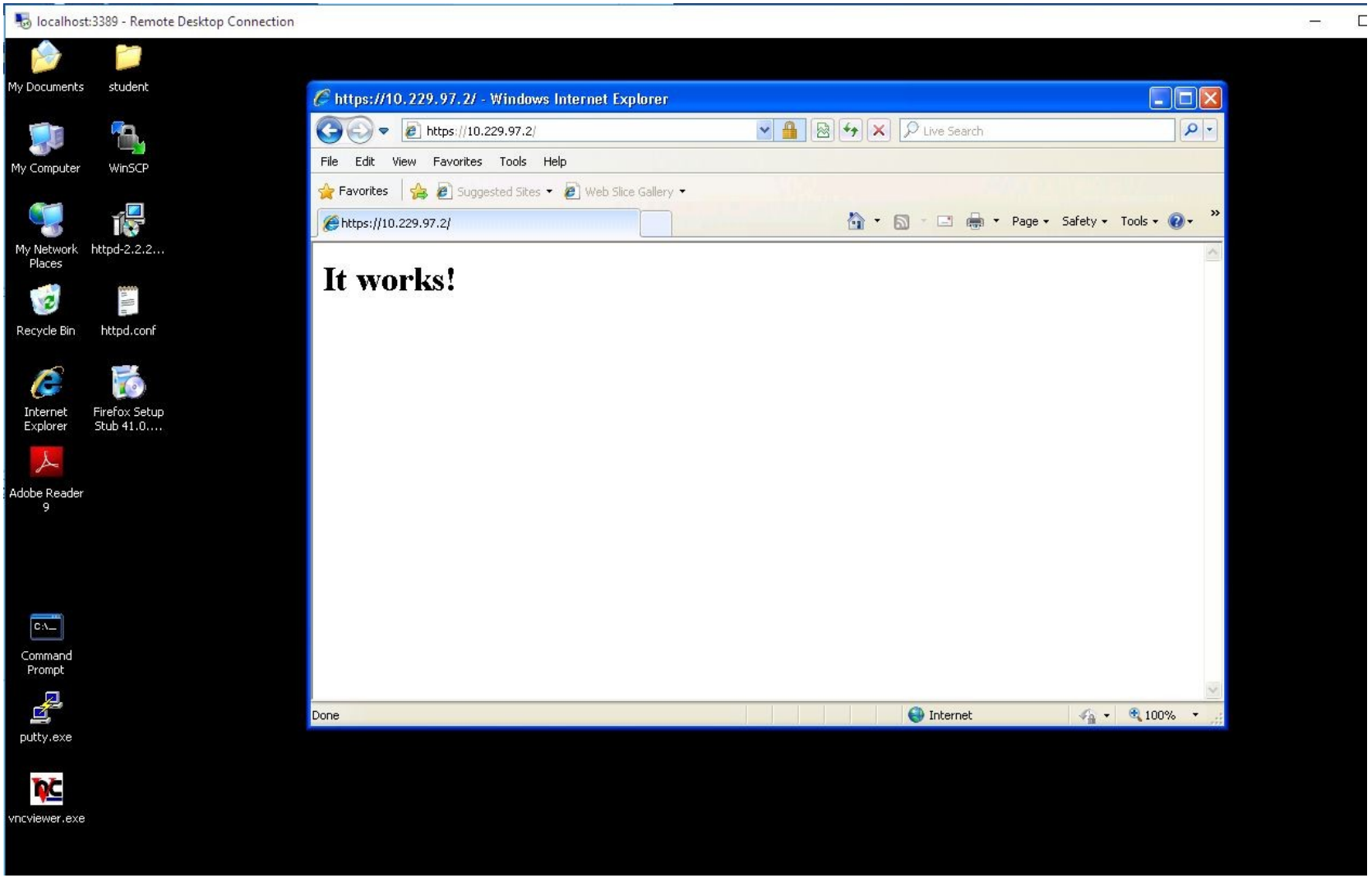

Figure 2. : After loading the CA

Generate your own CA

Tips:

A tutorial about openssl and certificates:

- http://web.archive.org/web/20110704035103/http://www.tc.umn.edu/~brams006/selfsign.html
- Make sure you follow the **Generate your own CA** option
- You can produce all keys and certificates in your Linux VM and transfer them in your Windows VM
- Make sure you submit all keys and certificates that you produce
- Make sure that you explain every step of the setup in your report
- Feel free to diverse from the tutorial and always include references in your report

Questions?