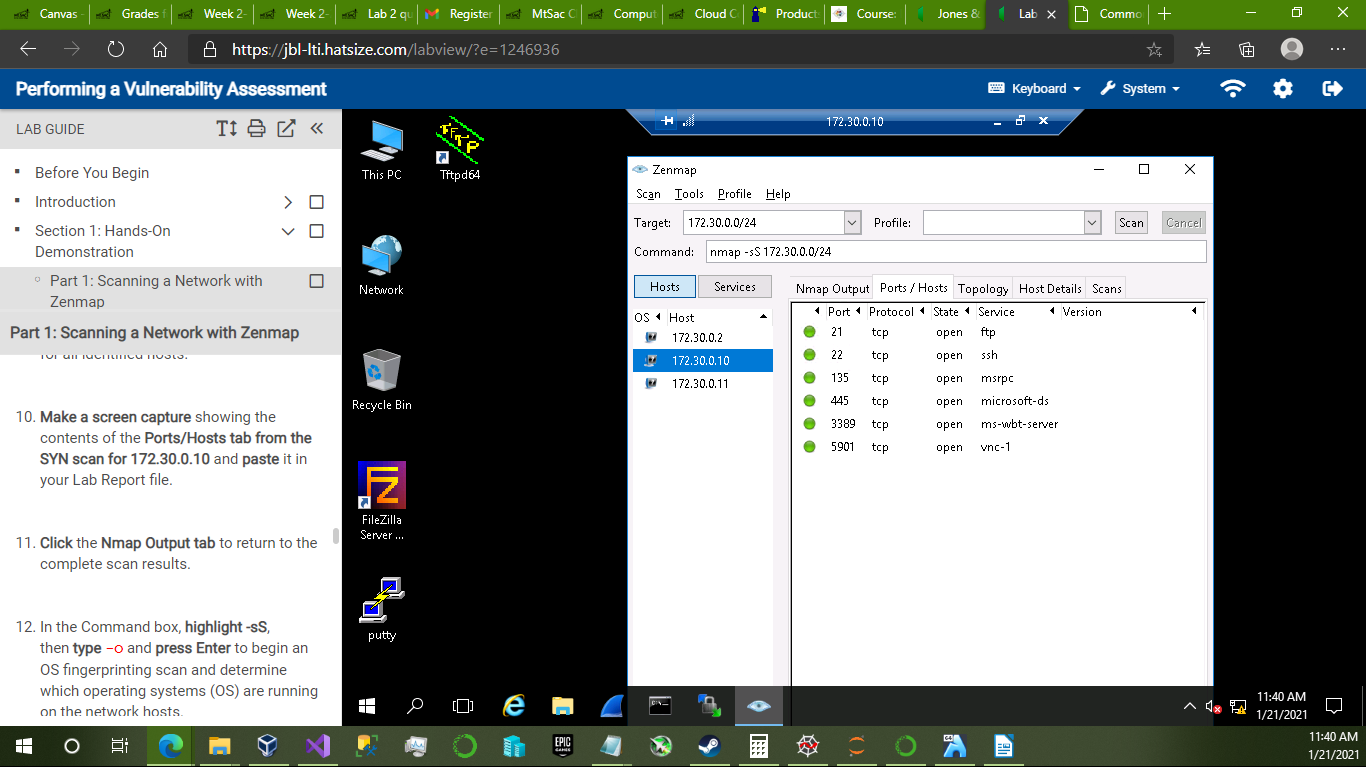
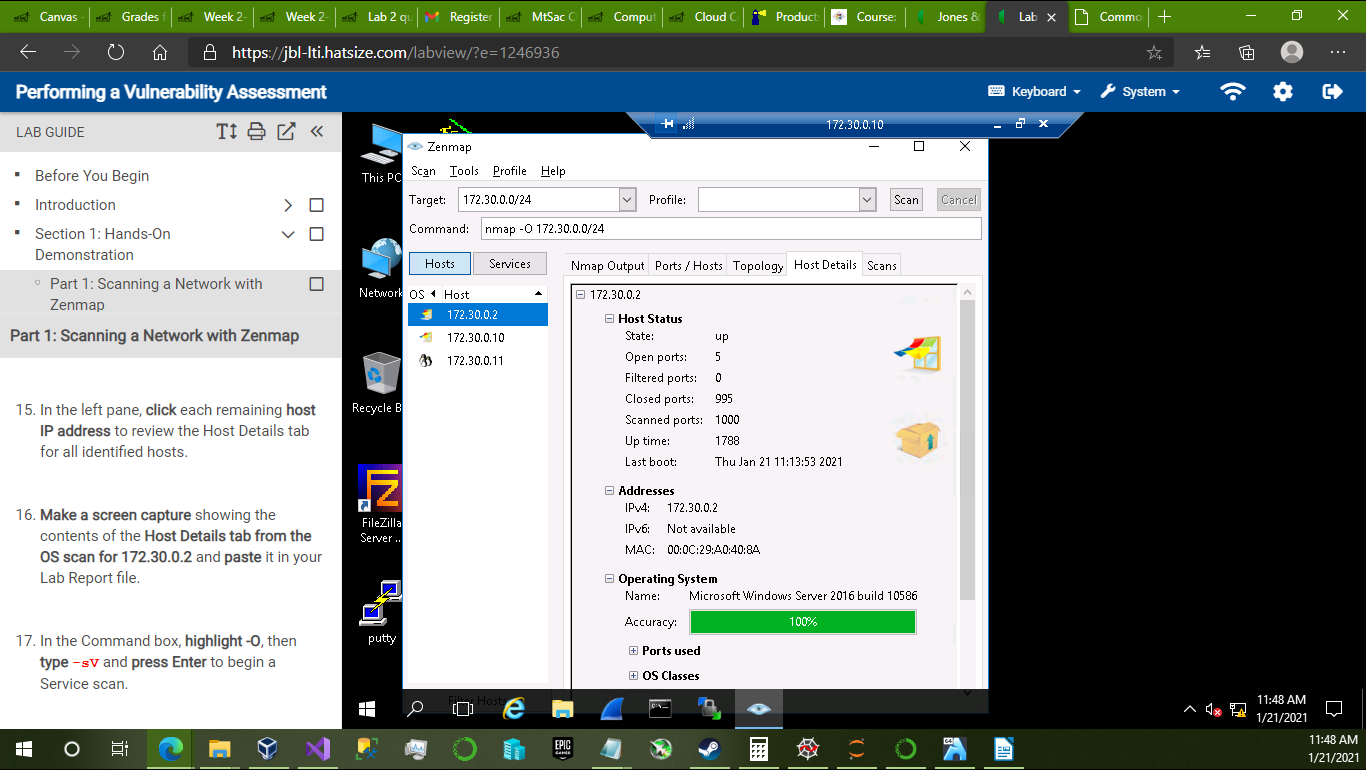
SECTION 1:

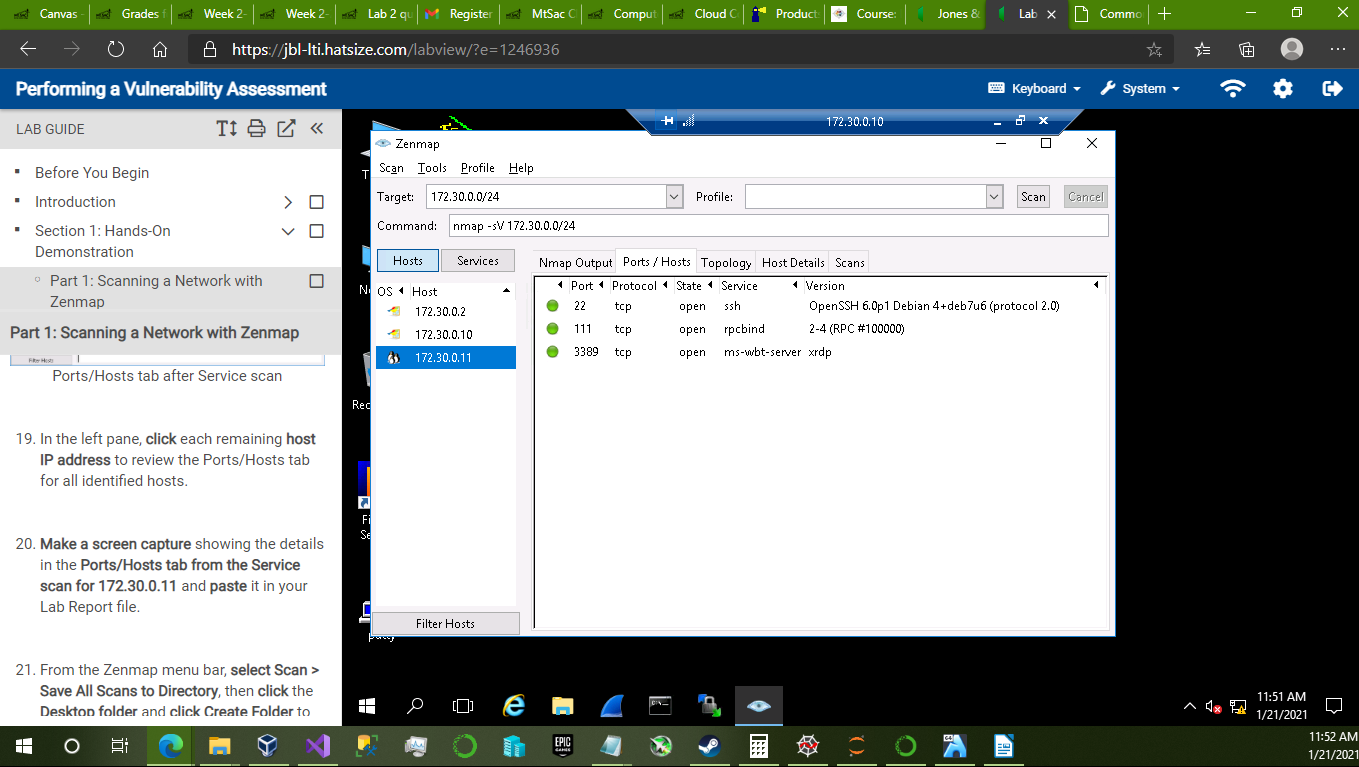
Ports hosts from the SYN scan for 172.30.0.10:



Hosts Details tab from the OS scan for 172.30.0.2:



Ports/Hosts tab from the Service scan for 172.30.0.11:



Mitigation Recommendations of Medium-risk vulnerabilities for 172.30.0.10:

1) SSL Certificate Cannot be Trusted:

– Plugin Id: 51192

– CVE ID: N/A

– Recommended Action(s): Purchase or generate an appropriate SSL certificate for this service. Follow the certificate chain to identify unrecognized certificates, self-signed certificates, or missing intermediary certificates and address them directly.

2) SSL Self-Signed Certificate:

– Plugin Id: 57582

– CVE ID: N/A

– Recommended Action(s): Purchase or generate an appropriate SSL certificate for this service. Be wary of Man-in-the-Middle Attacks, check endpoint certificates to see if any are signed by an unrecognized party.

3) Microsoft Windows Remote Desktop Protocol Server MitM Weakness:

– Plugin Id: 18405

– CVE ID: CVE-2005-1794

– Recommended Action(s): Force the use of SSL as a transport layer for this service if supported or/and

select the ‘Allow connections only from computers running Remote Desktop with Network Level Authentication’ setting if it is available. Secure the hard-coded RSA private key in a secure secrets vault or in a password protected folder.

4) SSL Certificate Expiry:

– Plugin Id: 15901

– CVE ID: N/A

– Recommended Action(s): Purchase or generate a new SSL certificate to replace the expired one.

5) SMB Signing Disabled:

– Plugin: Id 57608

– CVE ID: N/A

– Recommended Action(s): Enforce message signing in the host’s configuration for authentication. On Windows, this is found in the policy setting ‘Microsoft network server: Digitally sign communications (always)’. On Samba, the setting is called ‘server signing’.

6) SSL Medium Strength Cipher Suites Supported

– Plugin Id: 42873

– CVE ID: CVE-2016-2183

– Recommended Action(s): Reconfigure the affected application if possible to avoid use of medium strength ciphers. Review network security in order to mitigate against the threat of a local attacker on the same network.

7) Terminal Services Encryption Level is Medium or Low

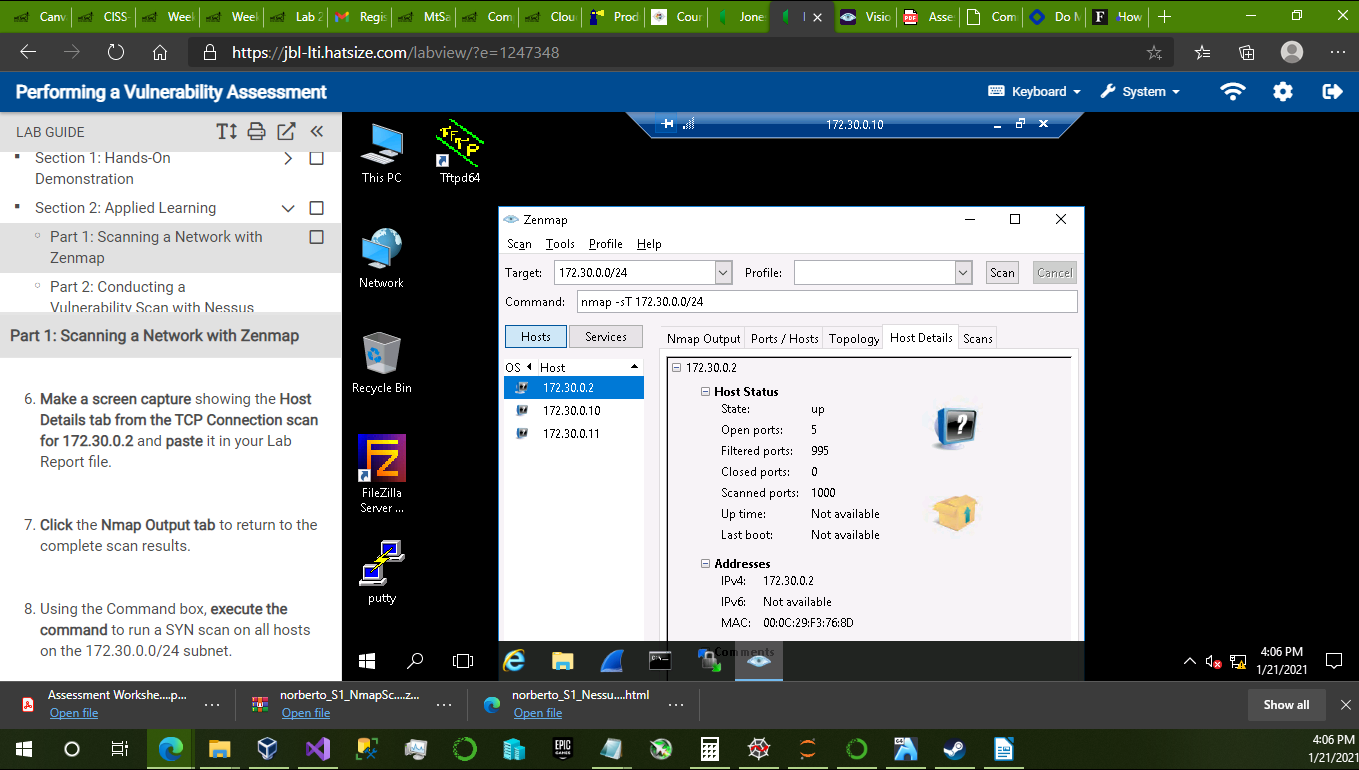
– Plugin Id: 57690

– CVE ID: N/A

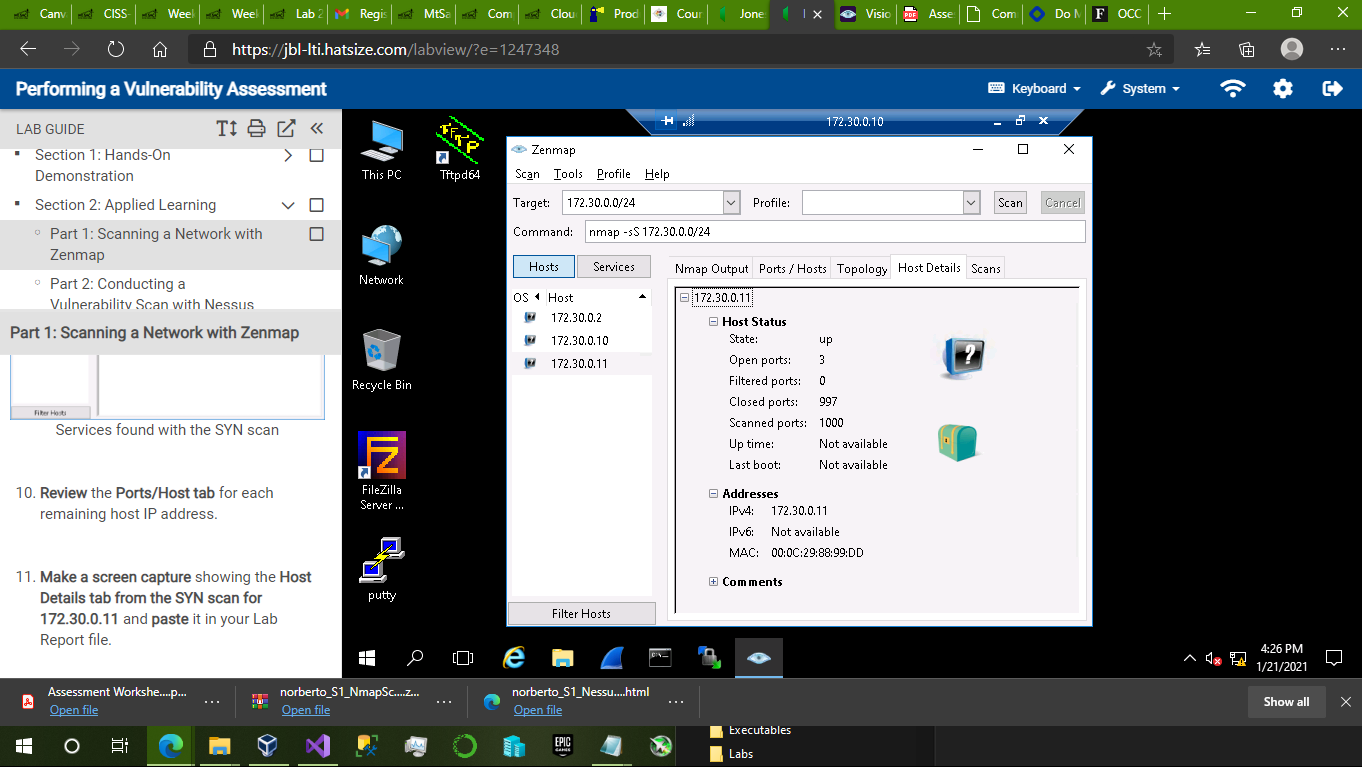
– Recommended Action(s): Change RDP encryption level to either ‘High’ or ‘FIPS Compliant’ in order to improve cryptography strength on the remote host.

SECTION 2:

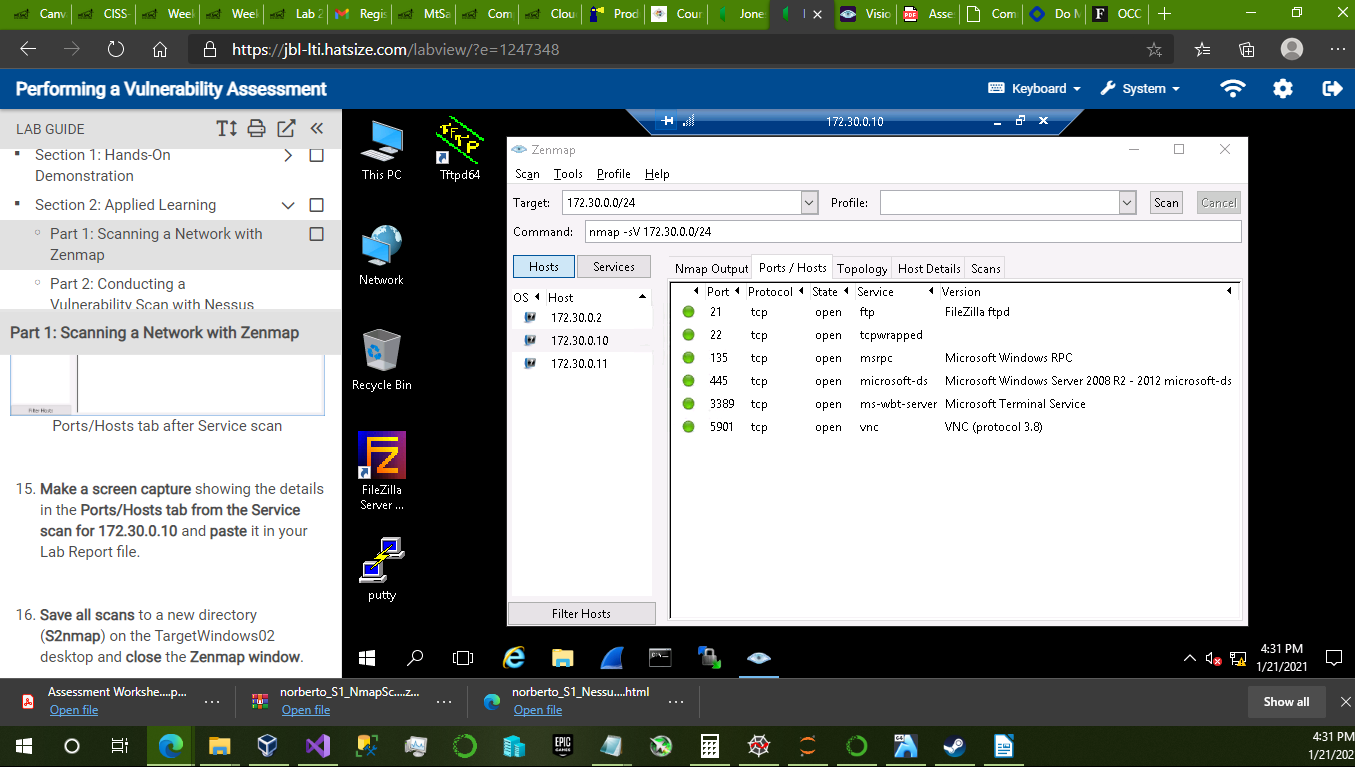
Host Details from TCP Connection scan for 172.30.0.2:



Host Details tab from the SYN scan for 172.30.0.11:



Ports/Hosts tab details from Service scan for 172.30.0.10:



Mitigation Recommendations of Medium-risk vulnerabilities for 172.30.0.11:

1) Terminal Services Doesn’t Use Network Level Authentication (NLA) Only

– Plugin Id: 58453

– CVE ID: N/A

– Recommended Actions: Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the ‘Remote’ tab of the ‘System’ settings on Windows.

2) SSH Weak Algorithms Supported:

– Pugin Id: 90317

– CVE ID: N/A

– Recommended Actions: Contact vendor, documentation or professional consultant in order to take the appropriate steps needed to remove the weak ciphers and replace them with stronger alternatives.