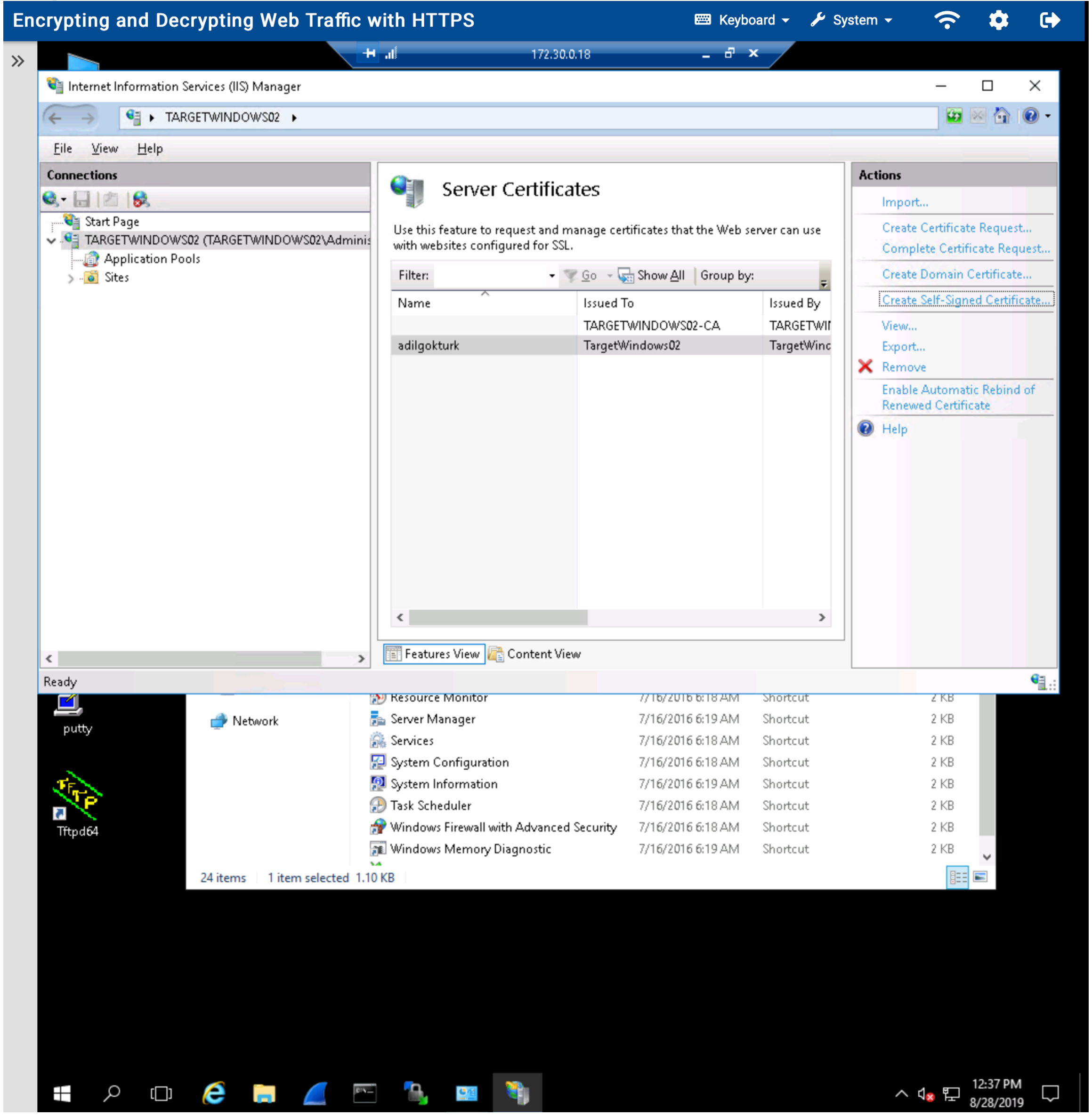
# Bonus Lab: Encrypting and Decrypting Web Traffic with HTTPS*

## Part 1: Create an SSL Certificate
## Step #10

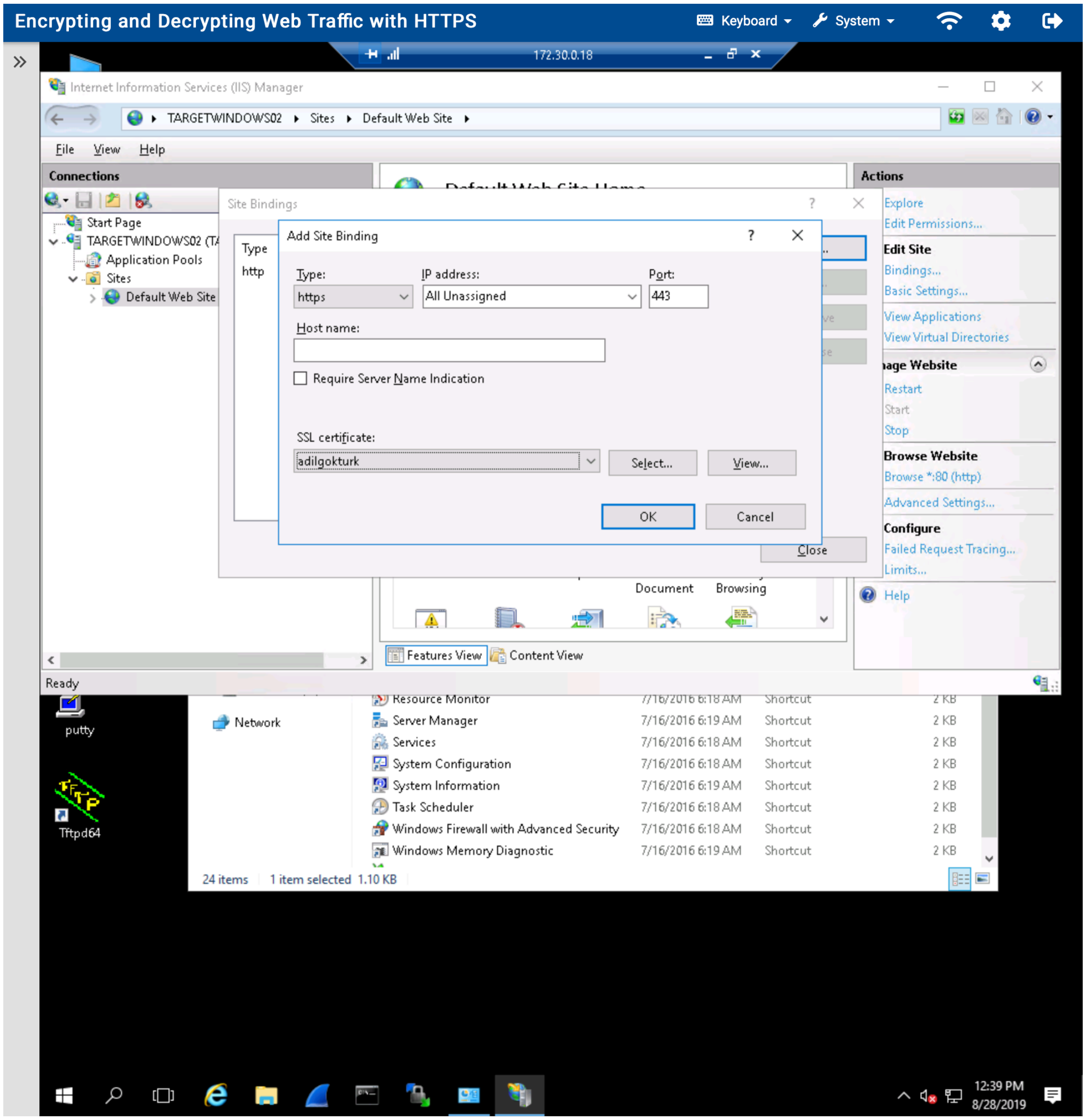

Encrypting and Decrypting Web Traffic with HTTPS
Keyboard
System
172.30.0.18
Internet Information Services (IIS) Manager
TARGETWINDOWS02
File View Help
Connections
Start Page
TARGETWINDOWS02 (TARGETWINDOWS02\Adminis
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
putty
Tftpd64
Network
24 items
1 item selected 1.10 KB
12:37 PM
8/28/2019

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

| Name | Issued To | Issued By |
|---|---|---|
| | TARGETWINDOWS02-CA | TARGETWI |
| adilgokturk | TargetWindows02 | TargetWinc |

| | | | |
|---|---|---|---|
| Resource Monitor | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Server Manager | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Services | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| System Configuration | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| System Information | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Task Scheduler | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Windows Firewall with Advanced Security | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Windows Memory Diagnostic | 7/16/2016 6:19 AM | Shortcut | 2 KB |

## Part 1: Create an SSL Certificate
## Step #17



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

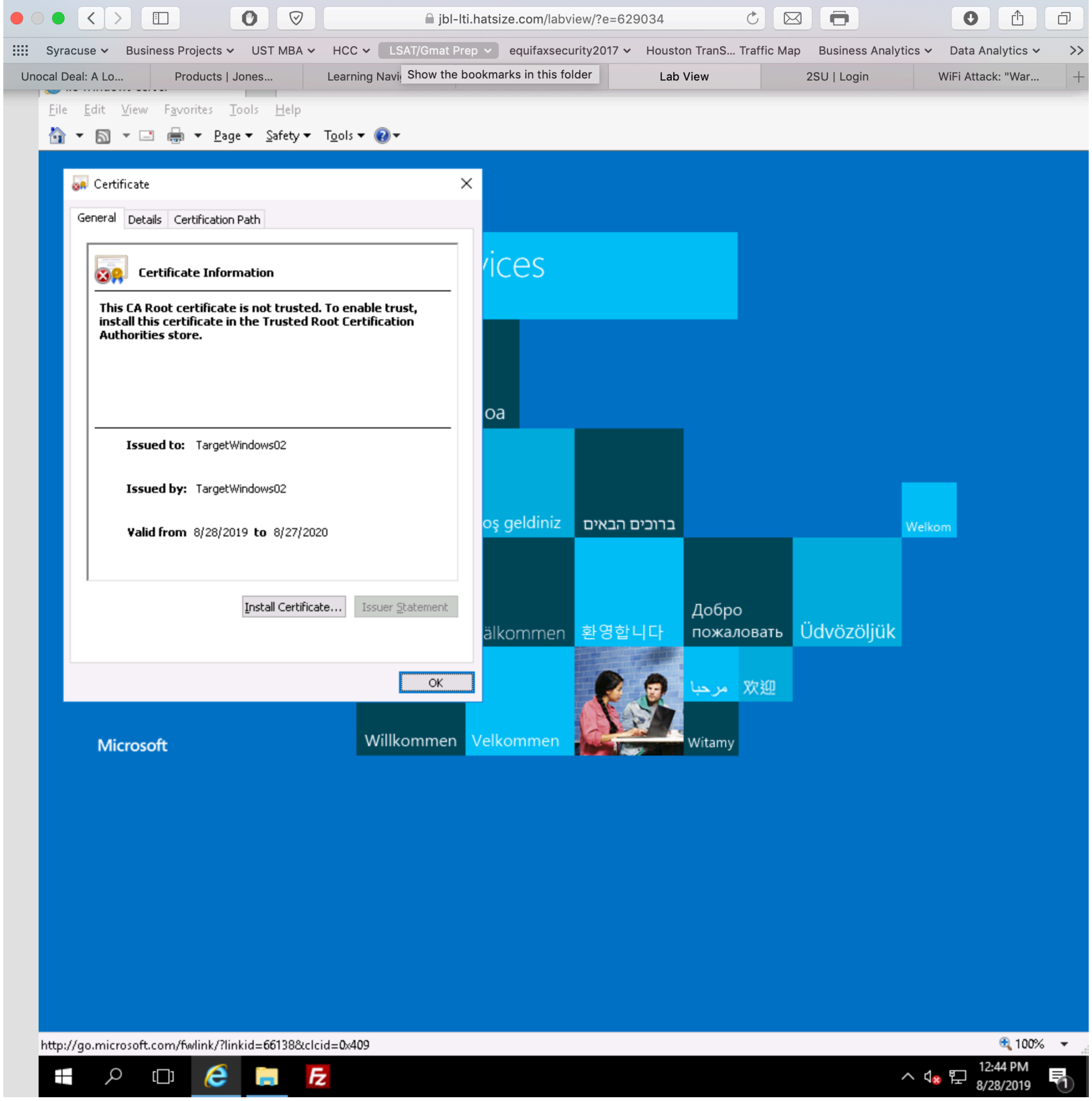
□ Require Server Name Indication

SSL certificate: adilgokturk

| | | | |
|---|---|---|---|
| Resource Monitor | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Server Manager | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Services | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| System Configuration | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| System Information | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Task Scheduler | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Windows Firewall with Advanced Security | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Windows Memory Diagnostic | 7/16/2016 6:19 AM | Shortcut | 2 KB |

24 items 1 item selected 1.10 KB

## Part 2: View SSL Certificate
## Step #8



Certificate

General | Details | Certification Path

**Certificate Information**

**This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.**

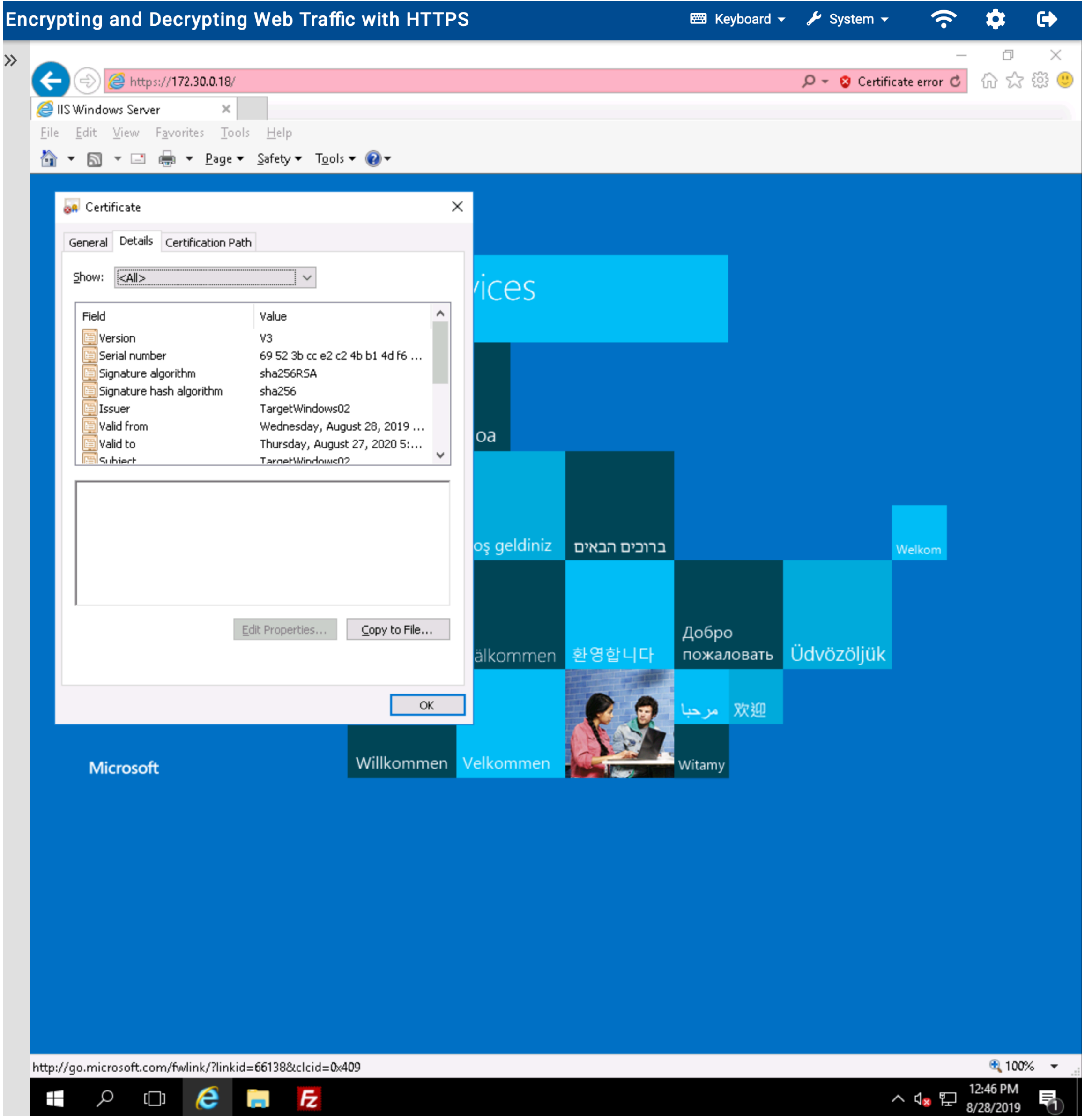
**Issued to:** TargetWindows02

**Issued by:** TargetWindows02

**Valid from** 8/28/2019 **to** 8/27/2020

jbl-lti.hatsize.com/labview/?e=629034
Install Certificate...
Issuer Statement
OK
Microsoft
http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409
12:44 PM
8/28/2019

## Part 2: View SSL Certificate
### Step #10


Encrypting and Decrypting Web Traffic with HTTPS
Keyboard
System
https://172.30.0.18/
Certificate error
IIS Windows Server
File Edit View Favorites Tools Help
Page Safety Tools
Certificate
General Details Certification Path
Show: <All>
Edit Properties...
Copy to File...
OK
Microsoft
Welkom
Willkommen Velkommen Witamy
http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409
100%
12:46 PM
8/28/2019

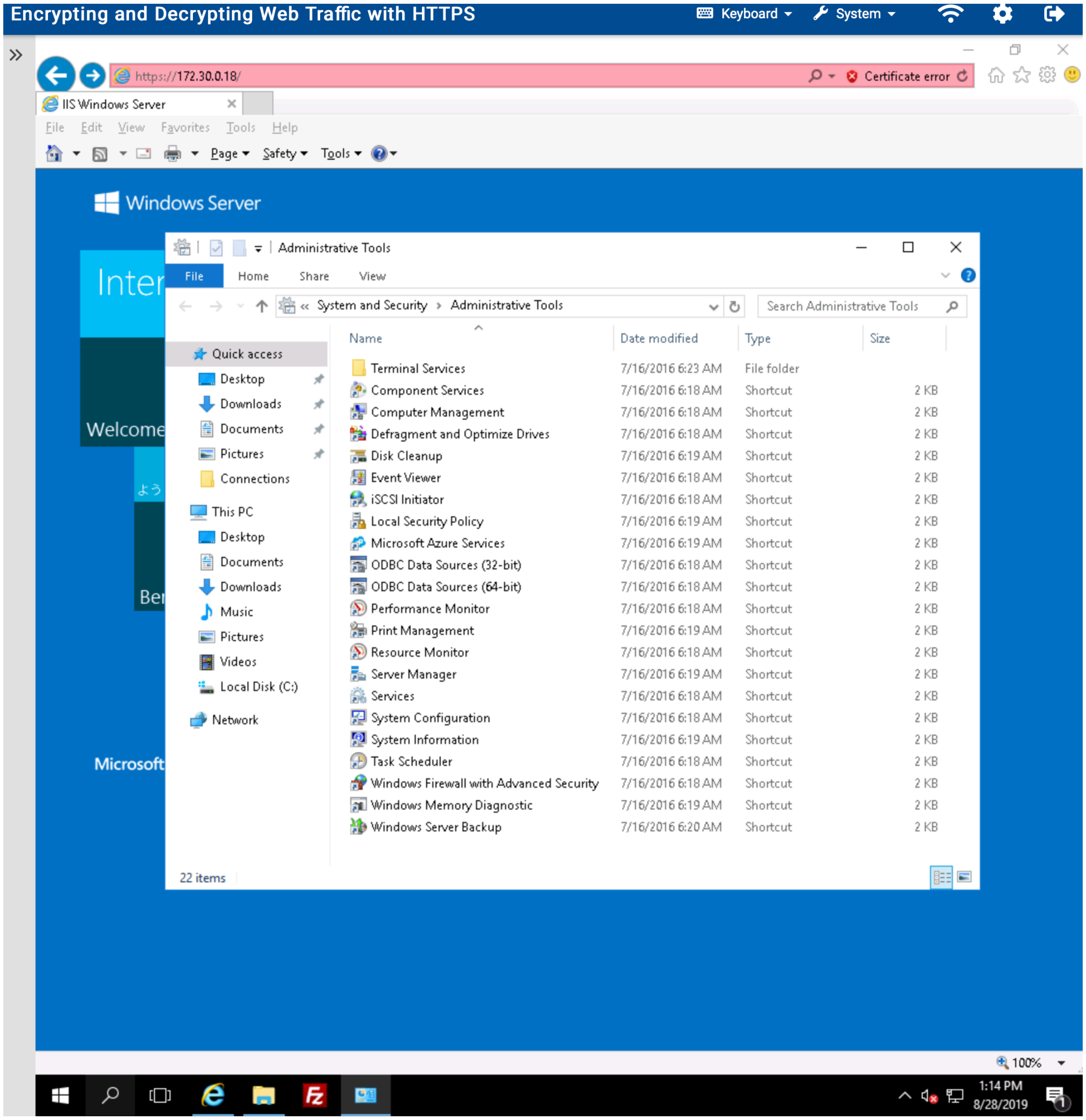
| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 69 52 3b cc e2 c2 4b b1 4d f6 ... |
| Signature algorithm | sha256RSA |
| Signature hash algorithm | sha256 |
| Issuer | TargetWindows02 |
| Valid from | Wednesday, August 28, 2019 ... |
| Valid to | Thursday, August 27, 2020 5:... |
| Subject | TargetWindows02 |

## Part 3: Challenge Question

Discuss at least three security vulnerabilities/limitations in the current SSL protocol
(Discuss them in 70 words each.)

1. To see security vulnerabilities, first let's check the Certificate Information:
   - It says, "This CA root certificate is not trusted. To enable to trust, we need to install this certificate in the Trusted Root Certification Authorities Store." So we need to provide/buy a certificate from the Trusted Root Certification Authorities Store and than we need to install it.

2. Windows server operating System could be earlier version such as Windows NT, 2003 or 2008. Early versions, such as Windows Server NT, had poor security. Later versions of Windows Server, such as Windows Server 2008, are much more secure. They intelligently minimize the number of running applications and utilities by asking the installer questions about how the server will be used. They also make the installation of vulnerability patches very simple and usually automatic. They include server software firewalls, the ability to encrypt data, and many other security enhancements.
3. Windows server user interface: All recent versions of Windows Server have user interfaces that look like the interfaces in client versions of Windows. This makes learning Windows Server relatively easy. It would be helpful to try to download current internet option.



| Name | Date modified | Type | Size |
|---|---|---|---|
| Terminal Services | 7/16/2016 6:23 AM | File folder | |
| Component Services | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Computer Management | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Defragment and Optimize Drives | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Disk Cleanup | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Event Viewer | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| iSCSI Initiator | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Local Security Policy | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Microsoft Azure Services | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| ODBC Data Sources (32-bit) | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| ODBC Data Sources (64-bit) | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Performance Monitor | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Print Management | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Resource Monitor | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Server Manager | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Services | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| System Configuration | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| System Information | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Task Scheduler | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Windows Firewall with Advanced Security | 7/16/2016 6:18 AM | Shortcut | 2 KB |
| Windows Memory Diagnostic | 7/16/2016 6:19 AM | Shortcut | 2 KB |
| Windows Server Backup | 7/16/2016 6:20 AM | Shortcut | 2 KB |