COURSE: SECURITY+ SY0-401

MODULE 1: NETWORK SECURITY

Part B
• Given a scenario, implement common protocols and services

• Given a scenario, troubleshoot security issues related to wireless networking
Common Protocols

- ICMP
- IPv4
- IPv6
- iSCSI
- Fibre Channel
- FCoE
- FTP
- SFTP
- TFTP
- TELNET
- HTTP
- NetBIOS
- IPSec
- SNMP
- SSH
- DNS
- TLS
- SSL
- TCP/IP
- FTPS
- HTTPS
- SCP
Standard Ports

- 21
- 22
- 25
- 53
- 80
- 110
- 139
- 143
- 443
- 3389
OSI Model – Ports & Protocols

Application
Presentation
Session
Transport
Network
Data Link
Physical
Secure Wireless Networking

Wireless Protocols and Features

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
Secure Wireless Networking

Wireless Protocols and Features

- TKIP
- CCMP
- Antenna Placement
- Power level controls
- Captive portals
- Antenna types
- Site surveys
- VPN (over open wireless)
Secure Wireless Networking

MAC Filter

Wireless MAC Filter

Enabled

Prevent PCs listed below from accessing the wireless network.

Permit PCs listed below to access the wireless network.

Wireless Client List

<table>
<thead>
<tr>
<th>MAC 01</th>
<th>MAC 02</th>
<th>MAC 03</th>
<th>MAC 04</th>
<th>MAC 05</th>
<th>MAC 06</th>
<th>MAC 07</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>MAC 26:</td>
<td>MAC 27:</td>
<td>MAC 28:</td>
<td>MAC 29:</td>
<td>MAC 30:</td>
<td>MAC 31:</td>
<td>MAC 32:</td>
</tr>
<tr>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>
Secure Wireless Networking

Disable SSID Broadcast
Secure Wireless Networking

Demonstration

NetStumbler
THANK YOU