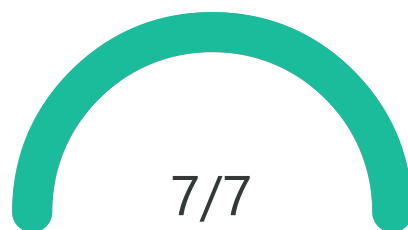


28: Assisted Lab: Understanding On-Path Attacks

Security+ (Exam SY0-701)



Congratulations, you passed!

Duration: 26 minutes, 18 seconds

- ☒ **use a script to confirm the existence of /var/www/html/newproxy.bat** Score: 1
Select the **Score** button to validate this task.
http://10.1.16.66/newproxy.bat verified ...
Task complete
- ☒ **Validate proxy configuration** Score: 1
Select the **Score** button to validate this task.
Proxy configuration confirmed ...

Task complete
- ☒ When the Burp Suite's Intercept function is turned off, what is the tool doing? Score: 1

☐ Session hijacking
☒ AitM sniffing
☐ Credential cracking
☐ Cookie theft
☐ Session ID abuse

Congratulations, you have answered the question correctly.
- ☒ What was the purpose of changing the proxy settings on the victim? Score: 1

☐ To prevent encryption negotiation
☒ To route traffic to the attacker's system
☐ To disable the firewall
☐ To enable DNS resolution

Congratulations, you have answered the question correctly.
- ☒ What would stop the victim's credentials from being stolen in the AitM attack? (select two) Score: 1

☐ SPAM filter
☒ Encrypted protocols
☐ Firewall
☒ Not trusting unsolicited instructions

☐ Intrusion detection system

Congratulations, you have answered the question correctly.

☒ What is the HTTP method of communication that contained the victim's credentials in the AitM attack? *Score: 1*

- ☐ GET
- ☐ HEAD
- ☐ PUT
- ☒ POST

Congratulations, you have answered the question correctly.

☒ Which of the following concepts should be added to the user training at the organization to avoid this type of scam in the future? *Score: 1*

- ☒ Do not execute scripts offered via email
- ☒ Do not use company credentials anywhere other than valid internal systems
- ☐ Log out of system when not in use
- ☐ Be cautious about instructions provided over the phone
- ☐ Do not share your credentials with others

Congratulations, you have answered the question correctly.