

## 04: Assisted - Using SET to perform social engineering

Security+ (Exam SY0-701)



Congratulations, you passed!

Duration: 19 minutes, 34 seconds

- Which of the following attack types is NOT supported by SET? Score: 1
- Arduino-based
  - Wireless
  - Spear phishing
  - SQL Injection
  - Powershell
- Congratulations, you have answered the question correctly.
- Use a script to confirm the existence of /root/.set/payload.exe on Kali** Score: 1
- When the handler is reported as started, select the **Score** button to validate this task.  
Path found ...  
Listener detected ...  
Task complete
- Use a script to confirm the existence of /var/www/html/acctupd.zip on Kali** Score: 1
- Select the **Score** button to validate this task:  
Download active ...  
Task complete
- Check sendmail** Score: 1
- Select the **Score** button to validate this task:  
Recipient confirmed as jaime@structureality.com ...  
Sender confirmed as support@structureality.com ...  
Task complete
- Verify listener connection** Score: 1
- Select the **Score** button to validate this task:  
Handler active ...  
Task complete

- What is the Computer name displayed by this meterpreter command in the box below? Score: 1

MS10

Congratulations, you have answered the question correctly.

- What is the primary defense against the attack that you performed in this lab? Score: 1

- Do not execute files from email
- Updating malware scanners
- Implement biometrics
- Update the SPAM filter

Congratulations, you have answered the question correctly.

- Which security framework does SET use to set up listeners? Score: 1

- Arachni
- Metasploit
- SMTP binder
- Maltego

Congratulations, you have answered the question correctly.

- The most commonly used features of SET are spear phishing, website spoofing, payload delivery, and mass mailer attacks. True or False? Score: 1

- True
- False

Congratulations, you have answered the question correctly.

- What is the primary limitation or restriction in compromising a victim through a SET-crafted email and related exploit script/payload? Score: 1

- Client-side security blocking execution
- Server keyword filtering
- Firewall blocking email messages with attachments
- NAT traversal

Congratulations, you have answered the question correctly.

- Which of the following are true in regard to using SET? (Select all that apply) Score: 1

- SET emails can use spoofed source addresses
- SET emails must be from a trusted email domain
- SET payloads are allow-listed in most security filters
- SET can send messages to a single address or a large group of addresses
- SET can send attachments or hyperlinks to malicious scripts or payloads
- SET demonstrates the power of combining technology with social engineering

Congratulations, you have answered the question correctly.