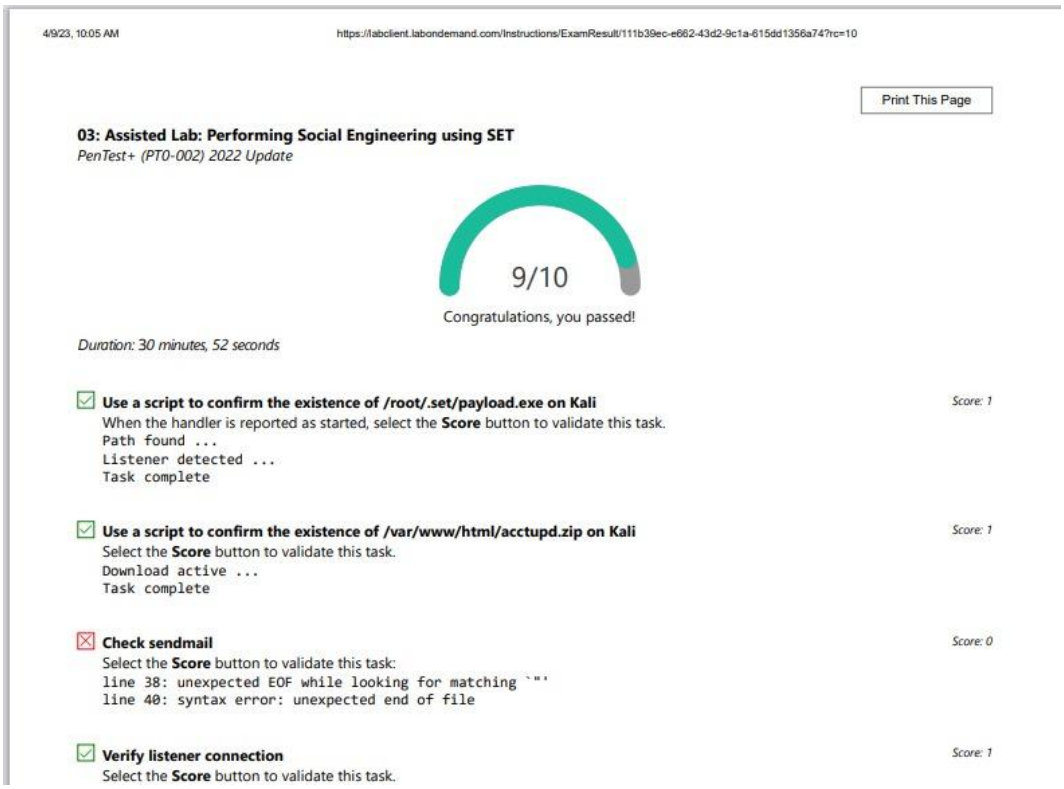

4/9/23, 10:05 AM https://labclient.labondemand.com/Instructions/ExamResult/111b39ec-e662-43d2-9c1a-615dd1356a74?rc=10

Print This Page

03: Assisted Lab: Performing Social Engineering using SET

PenTest+ (PT0-002) 2022 Update

9/10

Congratulations, you passed!

Duration: 30 minutes, 52 seconds

☑ **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: 0*
Select the **Score** button to validate this task:
```
line 38: unexpected EOF while looking for matching `"'
line 40: syntax error: unexpected end of file
```

☑ **Verify listener connection** *Score: 1*
Select the **Score** button to validate this task.

What are the benefits for a pen-tester to use the mass mailer feature in SET?

The employment of the mass mailer feature in the Social Engineering Toolkit (SET) can grant several advantages for pen-testers:

Efficient targeting: The mass mailer feature empowers pen-testers to reach out to a voluminous number of users, making it a highly efficient method to reach a broad audience.

Customization: Pen-testers can customize the email's subject line and content to fabricate a more convincing and targeted approach towards the audience.

Testing security effectiveness: The SET mass mailer feature provides the ability for pen-testers to scrutinize an organization's security measures against phishing attacks. Analyzing the attack's

success rate will grant pen-testers the opportunity to deliver recommendations for enhancing the security measures.

Time-saving: The automation of the mass mailer feature saves time for pen-testers, thereby releasing more time for other significant tasks in the penetration testing process.

Realistic testing: The ability to create realistic scenarios that simulate real-world phishing attacks provides a more accurate assessment of an organization's security posture.

All in all, the SET mass mailer feature is an effective tool that enables pen-testers to conduct phishing attacks and assess the organization's susceptibility to such attacks.

Do you think a pen-tester would have more success embedding malware into a document or providing a link to a phishing site asking for credentials to gain initial access to an end users computer?

Both embedding malware into a document and providing a link to a phishing site can be considered as efficacious methods for a pen-tester to infiltrate an end user's computer. Nevertheless, the efficacy of each approach can be contingent upon multiple factors such as the robustness of security measures, the level of awareness of the end user, and the attacker's level of acumen.

Embedding malware into a document can be a potent technique since it can circumvent certain security measures such as email filters, and the end user may be more prone to opening a document from a reputable source. Nevertheless, the attacker may require the usage of sophisticated social engineering techniques to entice the user to open the document, which may necessitate more effort and shrewdness.

On the other hand, providing a link to a phishing site can also be efficacious since it can dupe the end user into divulging their credentials, furnishing the attacker with initial access to the computer. However, the attacker may need to fabricate a credible and plausible phishing site and ensure that the link is conveyed in a manner that is not suspicious to the end user.

Generally speaking, a thriving attack can hinge on several factors such as the degree of security awareness of the end user and the sophistication of the attacker's modus operandi. It is vital for pen-testers to scrutinize and experiment with various attack vectors to ascertain potential chinks in an organization's security apparatus.

What type of tactics would you try to lure an end user to open your phishing email?

Phishing attackers frequently utilize social engineering tactics to entice end users into opening their phishing emails. These tactics can encompass:

Urgency or fear: The attacker might deploy scare tactics to instill a sense of urgency in the end user, such as a counterfeit security alert, a warning of a compromised account, or a threat of legal action. The objective is to create a sense of panic and impel the user to act swiftly without deliberation.

Curiosity or excitement: The attacker could attempt to provoke the end user's curiosity or excitement with a subject line that pledges exclusive or exhilarating information, such as an invitation to an extraordinary event, a celebrity scandal, or a leaked report.

Incentives or rewards: The attacker may propose an incentive or reward to the end user for accomplishing a specific action, such as a complimentary gift card, a discount coupon, or a prospect to win a prize. This tactic aims to allure the user into clicking on a link or opening an attachment.

Authority or trust: The attacker could pose as a trusted source, such as a bank, a government agency, or a reputable company, to win the end user's confidence and encourage them to reveal sensitive information.

Once again, it is important to note that these tactics are utilized by malicious actors to engage in illegal and unethical activities. It is crucial to remain vigilant and cautious when receiving unsolicited emails or messages and to report any suspicious activity to the relevant authorities.

Would you try scare tactics? If so what is an example?

Would you try offering a prize? If so what is an example?

As a malicious hacker I might try to employee this methods in performing certain unethical operations. As an example I would try to use scare tactics to send an email to the victim scaring him for a financial fraud, alerting the user of an hacked account.

As a nefarious attacker, I may indeed attempt to employ the strategy of enticing potential victims with the allure of prizes or incentives. To this end, I might craft an email that tantalizes the user with the promise of a free gift card or an opportunity to win an exciting prize. However, to claim the reward, the victim must surrender their personal information or follow a link embedded in the email.