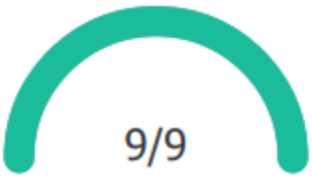
Print This Page

15: Assisted Lab: Establishing Persistence

PenTest+ (PT0-002) 2022 Update



Congratulations, you passed!

Duration: 29 minutes, 14 seconds

☑ **Verify listener started** *Score: 1*

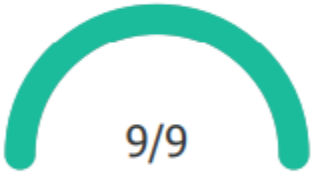
Select the **Score** button to validate this task:

```
Listener detected ...
Task complete
```


Print This Page

16: Assisted Lab: Performing Lateral Movement

PenTest+ (PT0-002) 2022 Update



Congratulations, you passed!

Duration: 24 minutes, 44 seconds

☑ **Verify listener started** *Score: 1*

Select the **Score** button to validate this task:

```
Listener detected ...
Task complete
```

Thesis Statement :

The purpose of this paper is to describe the persistence, lateral movement and elevated permissions which are critical for an effective penetration testing. This paper also provides details on assessing an environment's security, identifying it's vulnerabilities and simulating the tactics of the real world attackers to prevent dangerous activities.

What is the purpose of pen-testers wanting to establishing persistence on a system?

Penetration testers, or "pen-testers," are motivated to establish persistence on a targeted system to maintain access to it and extend their reconnaissance and exploitation activities well beyond the initial point of entry. The attainment of persistence is a crucial objective for pen-testers as it enables them to remain firmly entrenched within the system even if it is rebooted or if their initial access route is detected and blocked. The establishment of persistence empowers them to persist in their testing and uncover additional vulnerabilities or confidential information that may be available on the system. Moreover, persistence aids pen-testers in simulating the tactics of real-world attackers who strive to maintain a backdoor entry to a system to carry out nefarious activities over a protracted period of time. In essence, the ability to establish persistence is a hallmark of skilled pen-testing and a crucial component of an effective penetration testing strategy.

What are 3 ways to accomplish establishing persistence on a targeted system?

Penetration testers wield a vast array of sophisticated techniques to secure persistence on a targeted system. Behold, here are three exemplary illustrations of such tactics:

Firstly, the installation of backdoors constitutes a conventional, yet ubiquitous stratagem. In essence, backdoors are surreptitious programs or scripts that endow the pen-tester with the ability to retain their access to the system, even if their initial entry point is discovered and purged. These backdoors can be utilized to spawn additional user accounts, modify system configurations, or install auxiliary software, among sundry other feats of sorcery and skullduggery.

Secondly, rootkits represent another potent weapon in the pen-tester's armory. Rootkits are software programs that are explicitly crafted to obfuscate the existence of other software or processes on the system. In fact, these kits of iniquity may be deployed to cloak the pen-tester's backdoors or other noxious software from detection by security tools or system administrators, thereby rendering their nefarious activities indiscernible to the unsuspecting targets.

Finally, pen-testers may devise scheduled tasks that execute on the system at predetermined intervals, such as every time the system is rebooted or at specific times of the day. These tasks can be leveraged to execute code or scripts that perpetuate the pen-tester's access to the system, whilst simultaneously engaging in reconnaissance or exploitation activities, thereby facilitating the tester to establish an enduring foothold on the system.

What is the purpose and end goal for pen-testers to performing lateral movement?

Penetration testers, those cunning cyber warriors, engage in the art of lateral movement, a crafty method to escalate their privileges within a targeted network and infiltrate critical assets or

sensitive data. The end goal of such a strategy is to obtain a position of significant influence within the network, a lofty perch from which the pen-tester can launch even more sophisticated attacks or carry out malicious activities with a higher degree of success. By nimbly moving laterally across the network, these crafty testers can artfully evade or bypass security measures such as firewalls and intrusion detection systems, effortlessly slinking through the virtual shadows without raising any alarms. This allows them to gain access to an array of valuable resources, such as user credentials, database servers, or administrative privileges, all of which can be exploited with ruthless precision to further their nefarious objectives. In the grand scheme of things, lateral movement is an indispensable technique for pen-testers, a means to evaluate the security posture of a network and identify any potential vulnerabilities that attackers could exploit with ruthless efficiency.

Would a penetration tester need elevated permissions to access critical servers in an environment?

Explain why or why not.

Penetration testing, an integral technique for assessing the security posture of an environment, necessitates elevated permissions to access critical servers, as it allows the tester to mimic the actions of a genuine attacker who has already breached the network and obtained privileged access. This type of access is crucial for the tester to comprehensively assess the environment and pinpoint potential vulnerabilities that an attacker could exploit, since restrictions on permissions could hinder their ability to gauge the security level of a critical server. Nonetheless, it is vital to exercise prudence in granting such permissions and ensure that the tester adheres to rigorous guidelines and obtains explicit authorization from the organization to avoid any

inadvertent or deliberate harm to the environment. In the end, the control and monitoring of the permissions given to a penetration tester is indispensable in ensuring that the testing is carried out in a secure and regulated manner.

References :

Miller, M. (2021, March 22). *Why is the scope of a penetration test so important? " triaxiom security*. Triaxiom Security. https://www.triaxiomsecurity.com/why-is-the-scope-of-a-penetration-test-so-important/#:~:text=Scope%20Can%20Impact%20Risk&text=As%20an%20example%2C%20an%20external,not%20fully%20evaluating%20the%20risk.

What is lateral movement in cyber security? | cloudflare. (n.d.). https://www.cloudflare.com/learning/security/glossary/what-is-lateral-movement/

staff, I. T. (2023, March 2). *Improving security by protecting elevated-privilege accounts at Microsoft*. Inside Track Blog. https://www.microsoft.com/insidetrack/blog/improving-security-by-protecting-elevated-privilege-accounts-at-microsoft/