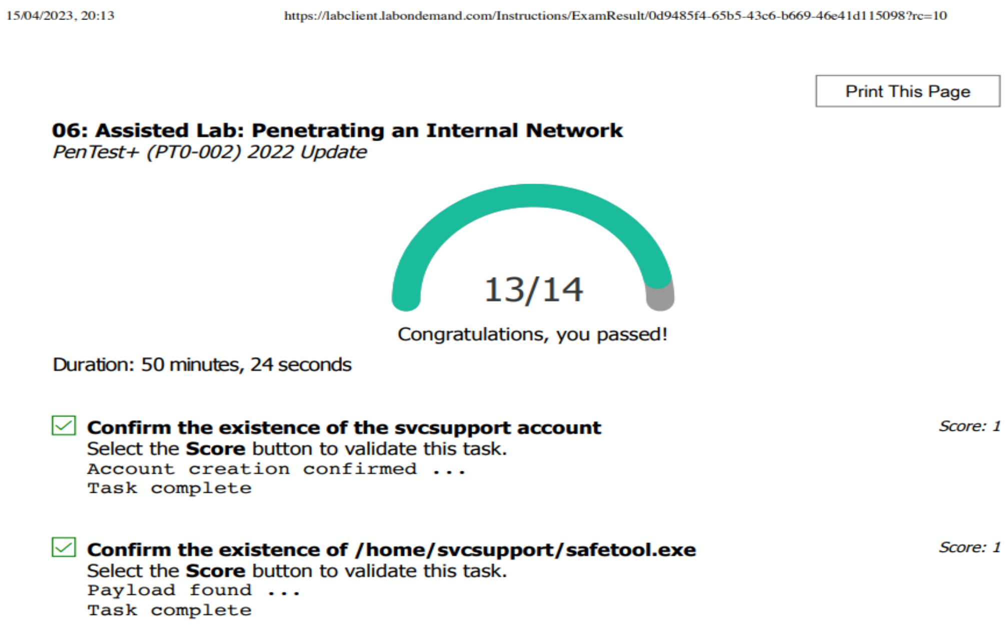
ASSIGNMENT WEEK 4



15/04/2023, 20:13 https://labclient.labondemand.com/Instructions/ExamResult/0d9485f4-65b5-43c6-b669-46e41d115098?rc=10

06: Assisted Lab: Penetrating an Internal Network

PenTest+ (PT0-002) 2022 Update

13/14

Congratulations, you passed!

Duration: 50 minutes, 24 seconds

☑ **Confirm the existence of the svcsupport account** *Score: 1*

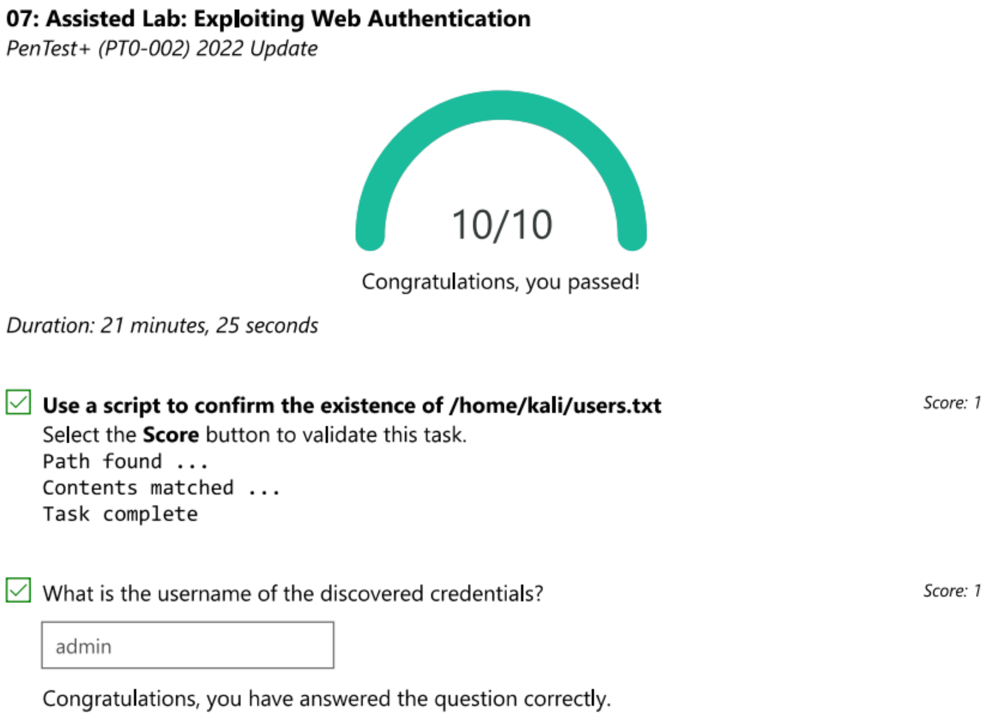
Select the **Score** button to validate this task.

```
Account creation confirmed ...
Task complete
```

☑ **Confirm the existence of /home/svcsupport/safetool.exe** *Score: 1*

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

```
Payload found ...
Task complete
```



07: Assisted Lab: Exploiting Web Authentication

PenTest+ (PT0-002) 2022 Update

10/10

Congratulations, you passed!

Duration: 21 minutes, 25 seconds

☑ **Use a script to confirm the existence of /home/kali/users.txt** *Score: 1*

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

```
Path found ...
Contents matched ...
Task complete
```

☑ What is the username of the discovered credentials? *Score: 1*

admin

Congratulations, you have answered the question correctly.

What is Metasploit used for?

Metasploit, a highly popular penetration testing framework among security experts and ethical hackers, is utilized for simulating real-world attacks on computer systems and networks, enabling the evaluation of the effectiveness of existing security measures. It comprises a vast array of resources and tools, such as exploit modules, payloads, and auxiliary modules, allowing users to both identify and exploit vulnerabilities in computer systems while also creating customized exploit modules, making it an exceptionally potent tool for offensive and defensive security operations.

The Metasploit framework finds extensive applications in testing network security, evaluating web applications' security, and assessing the security posture of an organization's IT infrastructure. Additionally, it can be used to assess the effectiveness of existing security controls and train security personnel in recognizing and responding to potential cyber threats, providing immense value for an organization's security apparatus.

Overall, due to its versatility and power, Metasploit is widely used by security professionals and researchers worldwide and continues to be a vital tool for security testing and assessment in the cybersecurity industry.

What is the default port number for Metasploit?

The Default port number for the Metasploit is 4444. However certain changes can be embedded to clarify the desired port number for the specific operations.

What two tools make up MSF Venom?

MSF Venom, an essential tool within the Metasploit framework, is a singular utility that is employed for producing customized payloads for exploiting vulnerabilities in computer systems and networks. Contrary to the misconception that it comprises two separate tools, MSF Venom is a versatile tool that offers numerous features for generating and customizing payloads that cater to various architectures, platforms, and languages. Besides, MSF Venom supports multiple output formats and encoding options to bypass the detection mechanisms of antivirus software and intrusion detection systems, thereby making it an indispensable tool for penetration testing and security testing. All in all, MSF Venom's impressive capabilities make it a potent tool for creating tailored payloads that can be used for probing and assessing the security posture of computer systems and networks.

When creating a payload with MSF Venom, what is the difference between LHOST and RHOST?

MSF Venom is a tool of immense value that boasts sophisticated capabilities for generating custom payloads to exploit vulnerabilities within the Metasploit framework. One of the key aspects that necessitate meticulous configuration is the LHOST and RHOST parameters. LHOST, commonly referred to as "Local Host," is a critical parameter that specifies the IP address or hostname of the machine to which the payload connects once it executes on the target machine. The connection typically ensues on the attacker's machine, where the Metasploit listener impatiently anticipates the target's connection. Conversely, RHOST, which stands for "Remote Host," plays a crucial role in determining the IP address or hostname of the target machine, on which the payload executes. This is the machine that the attacker endeavors to exploit and access. By configuring these parameters with precision, the attacker can ensure that the payload's performance is optimal, connecting back to the attacker's machine, and effectively exploiting the target machine.

Additionally, MSF Venom offers a diverse array of advanced features that empower users to create bespoke payloads customized for different architectures, platforms, and languages. The tool also supports several output formats and encoding options that serve as an effective countermeasure to evade detection by antivirus software and intrusion detection systems. These capabilities render MSF Venom a mighty tool for security and penetration testing, allowing users to craft bespoke payloads that bypass security measures and effectively exploit vulnerabilities.

What type of password attacks does Hydra support?

When it comes to cracking passwords, Hydra is a remarkably versatile tool that offers a range of attack types. Some of the most notable attacks that Hydra supports include brute force, dictionary, hybrid, rainbow table, pass the hash, and LDAP injection.

With a brute force attack, Hydra tries every possible combination of characters until it discovers the correct password. Meanwhile, with a dictionary attack, Hydra uses a pre-defined list of words and tries each word as a potential password. A hybrid attack combines both brute force and dictionary attacks to improve the chances of success.

Hydra can also perform rainbow table attacks, which involve using precomputed tables of passwords to find the correct password, as well as pass the hash attacks, which use previously obtained hash values to authenticate to a target system. Finally, Hydra is capable of executing LDAP injection attacks, exploiting vulnerabilities in an LDAP server to extract password information.

Due to its vast capabilities and effectiveness, Hydra is a popular choice among security professionals and penetration testers for performing password attacks.

List 3 of the 50 different protocols Hydra can be used against.

Hydra, the remarkably versatile password cracking tool, boasts the capability to launch password attacks against an extensive variety of protocols. Whether it's HTTP, FTP, Telnet, or many others, Hydra has the potential to infiltrate several different systems and applications that utilize these protocols, granting hackers the opportunity to crack open the security of the system by attempting to guess the login credentials. For instance, with HTTP authentication, Hydra can be employed to execute password attacks against web applications, where attackers can manipulate the security weaknesses to gain access to confidential information. Similarly, when it comes to FTP servers, Hydra can be utilized to conduct password attacks, where it attempts to obtain entry to sensitive files and data that may contain valuable information. Additionally, when it comes to

Telnet servers, Hydra can be deployed to conduct attacks on passwords, where hackers can try to uncover confidential login information and system vulnerabilities. In conclusion, with Hydra's ability to crack passwords across a wide range of protocols, it stands as a desirable tool for security professionals and penetration testers alike.