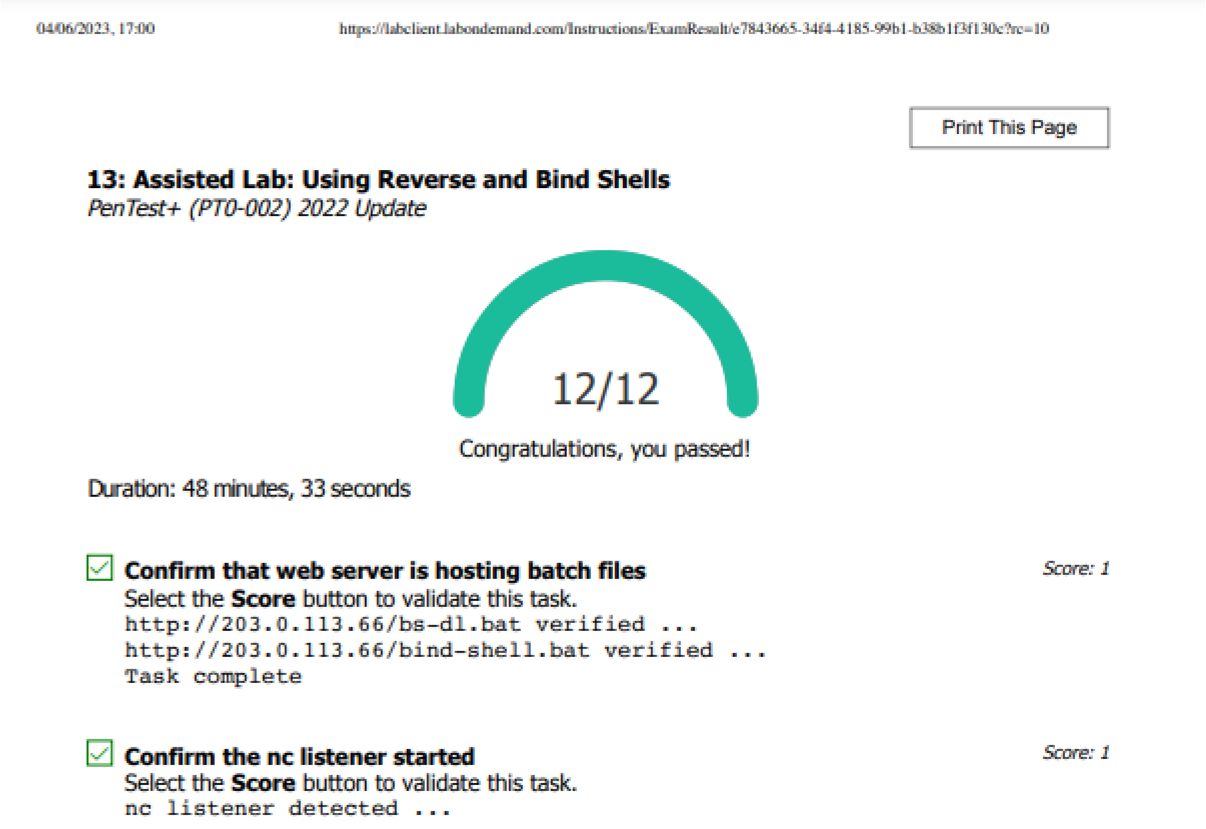
WEEK 7 ASSIGNMENT

The purpose of this paper is to describe reverse and bind shells, followed by post-exploit activities performed by a pentester. This paper also examines the reverse shells that are commonly used by pentesters and further steps that they can take in this scenario.



04/06/2023, 17:00 https://labclient.labondemand.com/Instructions/ExamResult/e7843665-34f4-4185-99b1-b38b1f3f130c?rc=10

13: Assisted Lab: Using Reverse and Bind Shells
PenTest+ (PT0-002) 2022 Update

12/12

Congratulations, you passed!

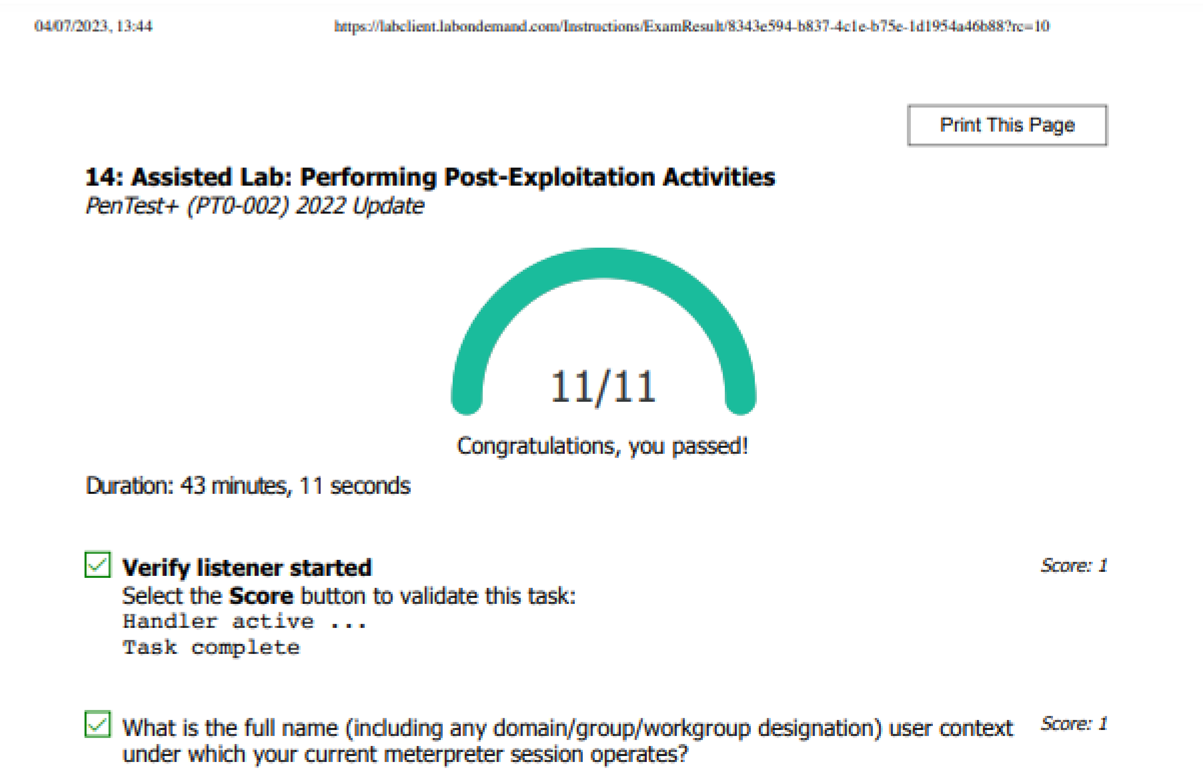
Duration: 48 minutes, 33 seconds

☑ **Confirm that web server is hosting batch files** *Score: 1*
Select the **Score** button to validate this task.

```
http://203.0.113.66/bs-dl.bat verified ...
http://203.0.113.66/bind-shell.bat verified ...
Task complete
```

☑ **Confirm the nc listener started** *Score: 1*
Select the **Score** button to validate this task.

```
nc listener detected ...
```



04/07/2023, 13:44 https://labclient.labondemand.com/Instructions/ExamResult/8343e594-b837-4c1e-b75e-1d1954a46b88?rc=10

14: Assisted Lab: Performing Post-Exploitation Activities
PenTest+ (PT0-002) 2022 Update

11/11

Congratulations, you passed!

Duration: 43 minutes, 11 seconds

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

```
Handler active ...
Task complete
```

☑ What is the full name (including any domain/group/workgroup designation) user context under which your current meterpreter session operates? *Score: 1*

Reverse Shells are commonly used by pen-testers to control a compromised host.

- **What type of information could they gather from a Reverse Shell?**
- **What type of situations would you use a Web Shell?**

the reverse shell, a technique wielded by the crafty pen-tester to attain remote access and gain full control over a compromised host. Oh, the possibilities! With a reverse shell, the attacker is given free rein to execute commands on the vulnerable machine from a distance, opening up a world of opportunities for the collection of sensitive data and the pursuit of malicious activities.

The gains from such a maneuver are manifold, for one can easily procure system information through the reverse shell's wiles, ranging from the operating system and CPU architecture to the memory that is available.

But wait, there's more! With the reverse shell, one can also claim network information, gleaning valuable insights into the network to which the vulnerable host is connected, including IP addresses, open ports, and active connections.

Ah, and we haven't even touched on the glorious treasure trove that is user information. Oh yes, dear reader, with the reverse shell, the attacker can unearth critical intel on the users of the compromised host, revealing juicy tidbits such as usernames, passwords, and home directories. Quite the bounty, wouldn't you say?

But lo, let us not forget the web shell, a delicious morsel of maliciousness that can be uploaded to a web server through a vulnerable application. The web shell is a veritable key to the kingdom, offering the attacker an opportunity to execute commands on the server and plunder all manner of sensitive data. It is often employed in situations where the attacker has previously secured access to the web server through a weakly protected PHP script or a vulnerable CMS. With the web shell in hand, the attacker can continue their marauding by executing commands on the server, manipulating files, and interfering with the database. Truly a fearsome weapon in the hands of the skilled hacker!

What might be the next steps a pen-tester would try to take after gaining access to a remote system?

Once a pen-tester has successfully infiltrated a remote system, the next steps they take will vary depending on the goals of the penetration test and the level of access they have achieved. Let's explore some common next steps that a pen-tester might take:

Firstly, they might attempt to escalate their privileges on the compromised system. This can involve a series of sophisticated maneuvers, such as exploiting zero-day vulnerabilities, abusing weak passwords, or tampering with system configurations. By doing so, the pen-tester aims to gain access to additional resources, such as sensitive data or other hosts on the network.

Next, if the compromised system is part of a larger network, the pen-tester might try to move laterally through the network to gain access to other systems or resources. This can involve compromising intermediate systems, using pass-the-hash attacks, or exploiting trust relationships between systems.

The pen-tester might also attempt to establish persistence on the compromised system, enabling them to maintain access and control over the system even after the penetration test is over. This can involve a range of techniques, such as installing rootkits, backdoors, or remote access Trojans.

If the goal of the penetration test is to assess the security of data assets, the pen-tester might attempt to exfiltrate sensitive data from the compromised system. This can involve techniques such as copying files to remote servers, using covert channels to transfer data, or extracting data using SQL injection attacks.

Finally, the pen-tester might perform various post-exploitation activities, such as installing backdoors, creating user accounts, or modifying system settings to maintain access and control over the compromised system. These activities must be performed within the scope of the penetration test and with the permission and knowledge of the system owner.

It's important to note that the ultimate goal of a pen-test is to identify and mitigate security vulnerabilities, not to cause harm to the target system or its users. The pen-tester must adhere to ethical standards and respect the privacy and security of the system owner.

What can a pen-tester do to cover their tracks?

During the process of performing a penetration test, the pen-tester should ensure that they maintain a low profile, so that they don't leave any traces that could alert the system owners or administrators. There are several steps that the pen-tester can take to cover their tracks, including deleting logs of their activities, spoofing their identity or IP address, hiding files they have uploaded or created, modifying timestamps of accessed or modified files, cleaning up residual files, and using encryption to protect their communication channels. It's important to note that pen-testers should always obtain proper authorization and follow legal and ethical guidelines when conducting a test, including obtaining written permission to test, staying within the scope of the test, and avoiding causing damage or disrupting system availability. It's imperative that the pen-tester should execute these steps carefully and with great caution to ensure that they don't get detected by the system owners or administrators.

References :

Jamil, M., Akhlaq, M. A., Shafique, K., & Saeed, S. (2021). A comprehensive review of penetration testing: A technical guide for cyber security professionals. Computers & Security, 102, 102219.

Gupta, S. (2019). Penetration testing: A comprehensive guide with advanced methods. Packt Publishing Ltd.

Blanchard, O. (2021). Practical security assessment: A hands-on guide to evaluating information security. O'Reilly Media, Inc.