

Forum:[Hack Forums](#)

Thread: [\[TuT\] Maintaining access with Web Backdoors - Kali Linux \[Weeveily\]](#)

rootsh3ll - July 8, 2015, 9:00 am

Hello, Today we will learn about maintaining access with Web backdoors using Web shell. Example, Weeveily (Pre-installed in Kali Linux).

Once a web server and its services have been compromised, it is important to ensure that secure access can be maintained. This is usually accomplished with the help of a Web Shell - a small program that provides stealth backdoor access and allows the use of system commands to facilitate post-exploitation activities.

Kali comes with several web shells, here we will use a popular PHP web shell called Weeveily.

Weeveily simulates a Telnet session and allows the tester or attacker to take advantage of more than 30 modules for post exploitation tasks, including the following:

1. Browsing the target filesystem.
2. File transfer to and from the compromised system.
3. Performing audits for common server misconfigurations.
4. Brute-forcing SQL accounts through the target system.
5. Spawning reverse TCP shells.
6. Executing commands on remote systems that have been compromised, even if PHP security restrictions have been applied.

Finally, Weeveily endeavors to hide communications in HTTP cookies to avoid detection. To create Weeveily, issue the following command from the Terminal.

```
root@rs :~ # weeveily generate <Password> <Path>
```

This will create the file weeveily.php in the root directory. Executing commands on remote systems that have been compromised, even if PHP security have been applied.

Using a file upload vulnerability or any other compromise , including ones that give access to the meterpreter file upload functions, upload weeveily.php onto the compromised website.

To communicate with the web shell, issue the following command from the command prompt, ensuring that the target IP address, directory, and password variables are changed to reflect those of the compromised system:

```
root@rs :~# weeveily http://<target IP address> <directory><password>
```

In the example shown in the following screenshot, we have verified that we are connected to the web shell using the whoami command (which identifies the correct directory) and the ls command in order to obtain a file list (which again confirms the source of the connection as weeveily.php). The cat /etc/passwd command was used to view passwords.

The web shell can also be used to establish a reverse shell connection back to the

tester, using either Netcat or the Metasploit Framework as the local listener.

Summary

In this tutorial, we examined websites and the services that they provide to authorized users from the perspective of an attacker. We applied the kill chain perspective to web services in order to understand the correct application of reconnaissance and vulnerability scanning.

Several different vulnerability scanners were presented; we focused on making and using modifications to existing scanners to support the assessment of websites and web services, the use of browser-based vulnerability scanners, and vulnerability scanners that are specifically designed to assess websites and their services. Only a select few exploits were reviewed, and we completed the chapter with an examination of a web shell that is specific for web services.

Credits - Mastering Kali Linux.

For more tutorials : www.rootsh3ll.com

Th3PonyWizard - July 8, 2015, 11:55 am

Seeing Weevely mentioned in HF always stings my heart. [Techie, one of the youngest and most talented people I've met here wrote his one over it.](#) Cheers.

rootsh3ll - July 8, 2015, 12:24 pm

(Jul 8, 2015 11:55 AM)Makise Kurisu Wrote: [\[CITE\]](#) Seeing Weevely mentioned in HF always stings my heart. [Techie, one of the youngest and most talented people I've met here wrote his one over it.](#) Cheers.

Thanks 'Makise Kurisu' for the feedback!

and thanks also for providing the Link.

This Weevely tutorial is written very deeply and in an easy to understand manner. Such a great post! Really helpful.

Thanks a lot dear! :)