

Cyber Defense Organization

Spring 19' - Exploiting Windows with CDO's Founder



Agenda

- Meet Jared (Introduction)
- Live Demo
- Hands on Exploiting
- Bonus Challenge
- Q&A
- Final Remarks



What you do with this info

DISCLAIMER: This is purely for educational purposes, if you ever were to perform a Penetration Test you need **PERMISSION**.

“Although the procedure happens on the mutual consent of the customer and the **penetration testing** provider, a range of US state **laws** still consider it hacking. They all have a common ground: whoever makes illegal unauthorized use of computer systems commits a crime.”

Introduction

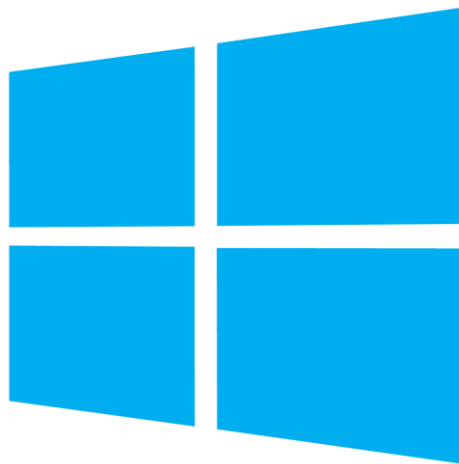
HELLO!

Live Demo

Hacking Windows 10 using Metasploit and Post-Exploitation with Meterpreter



VS



Hands on Exploiting

- Boot up the Windows 10 and Kali Linux Box!
- Follow these Steps!
- <https://bit.ly/2GoT3Ux>



What you should see at the end

```
root@kali: ~  
File Edit View Search Terminal Help  
[*] Running as SYSTEM extracting hashes from registry  
[*] Obtaining the boot key...  
[*] Calculating the hboot key using SYSKEY d3d3d79c9f3b64d502f357dfe2592e98...  
[*] Obtaining the user list and keys...  
[*] Decrypting user keys...  
[*] Dumping password hints...  
[*] No users with password hints on this system  
[*] Dumping password hashes...  
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[+] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[+] Martin:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[+] Shiela:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
[+] Jason:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
meterpreter > clearev  
[*] Wiping 363 records from Application...  
[*] Wiping 11703 records from System...  
[*] Wiping 3956 records from Security...  
meterpreter > clearev  
[*] Wiping 0 records from Application...  
[*] Wiping 14 records from System...  
[*] Wiping 1 records from Security...  
meterpreter > 
```

Bonus Challenge

- Boot up the Windows 7 Machine.
- Try Exploiting it!
- No instructions so....



Any Questions?

**About
CDO?**

**About
Jared?**

**About
what we
did?**



Announcements

Working on an interesting project? Have a specialty? Present!

If you are interested in a topic/want to present email us!

cyberdefenseorg@albany.edu

Cya Next week!

If you have any good memes send them to the email below.

wcsmith@albany.edu

Follow us on Twitter? Add on myInvolvement?



April 23rd, 7:15 BB007
WHAT ARE YOUR DREAM???!

Save the Data: May 4th.
CDO's First Competition!



<https://discord.gg/9Dh6R5R>