

- Filename: eccouncil-ceh31250-v10-6-1-5-password_attacks_pt5.md
- Show Name: CEHV10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Password Attacks Pt.5
- Description: In this episode, Daniel and Zach keep exploring common password attacks and tools. Here they round out hash gathering techniques such as LLMNR exploitation using Responder, stealing credentials using Man-in-the-Middle attacks, and performing a Pass-the-Hash attack for gaining access without actually needing to crack the password hash.

=====

Password Attacks Pt.5

- Malware/Spyware/keylogger
- LLMNR
 - Windows will look for Link-Local Multicast Name Resolution if DNS fails
 - Does this will multicast
 - Tool answers multicast
 - Tools include
 - responder
 - Metasploit
 - MITMf
 - Tells Windows to authenticate for access
 - Creds grabbed
 - User gets error
 - **DEMO: Responder cred grab**
 1. `responder -I eth0 -v`
 2. Victim requests resource through DNS and DNS fails to locate. Tries LLMNR
 - `net use \\server1\share1`
 3. Probably seeing username/pass-hash at this point
 - If user enter's username/password, you WILL see that get captured
 - **DEMO: Ettercap for DNS poisoning**
 1. Modify `etter.dns` file to have fake A records
 - Copy from Kali `/Tools/fakeArec.txt`
 - Change IP to match IP of bWAPP
 2. `ettercap -T -q -i eth0 -P dns_spoof -M arp /10.0.0.225//`
 - `-T` = Text Only
 - `-q` = Quiet. Do not display packet contents
 - `-i` = Set interface
 - `-P` = Choose plugin to use
 - `-M` = Perform MITM
 3. Browse to facebook from target
 4. Login to facebook/bWAPP and see user/pass info in Kali
- **Cool stuff. Any other things we need to be aware of when it comes to attacking passwords?**
- Pass the hash
 - Allows you to pass the hash value for a password instead of password

- Shell will PTH-WINEXE
 - View *pth-cheat-sheet.txt* in Documents folder of Kali.