L’arte del PenTesting

Provare a superare le difese perimetrali prima che lo facciano altri

MEDIASECURE SRL
www.mediasecure.it

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

Mediasecure

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 Lucchese 68 – 50019 Sesto Fiorentino (FI)
P.I. 01687800472

Tel. 055.3424714
Mail. info@mediasecure.it
Sito. www.mediasecure.it

XXXXXXX SPA
VIA PIPPO 1
50100 FIRENZE

PROGETTO ASSESSMENT
TECHNICAL SUMMARY

Documento	Oggetto	Autore	Codice	Pagine
PROGETTO ASSESSMENT	TECHNICAL SUMMARY	LORENZO D'ORIANCO	OF2017.038	Pag. 1 a 37

- ✓ 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

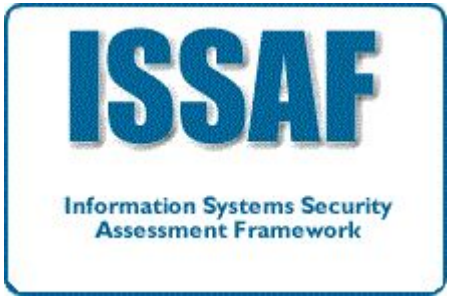
ESISTONO VARIE PENTEST LINUX DISTROS (https://hacktips.it/le-migliori-distro-pentesting-2016/)

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

→ DEMO ←

Kali Linux

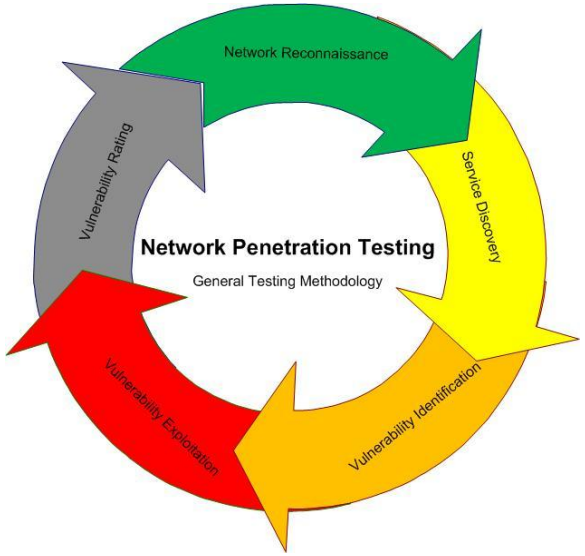
Metodo di lavoro



- ✓ 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

Mediasecure

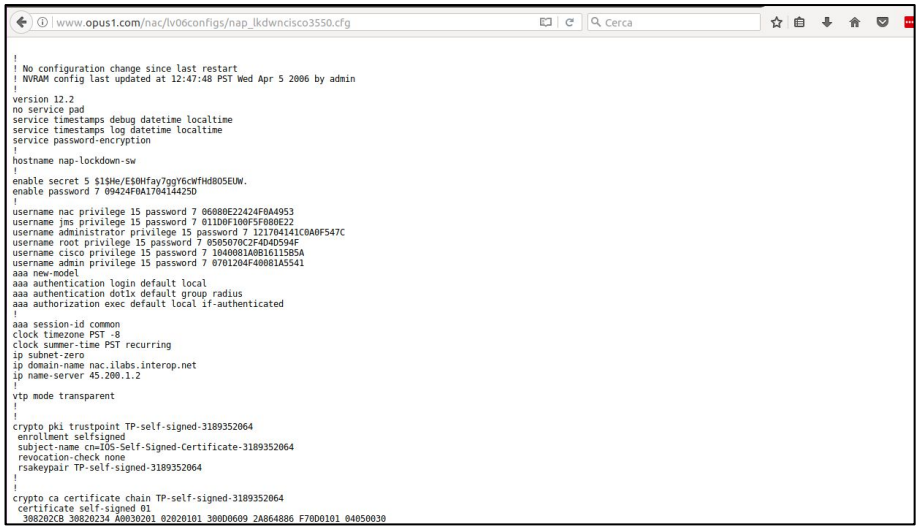
Fasi di un pentest



- ✓ 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



Fase 1: DISCOVERY TOOLS

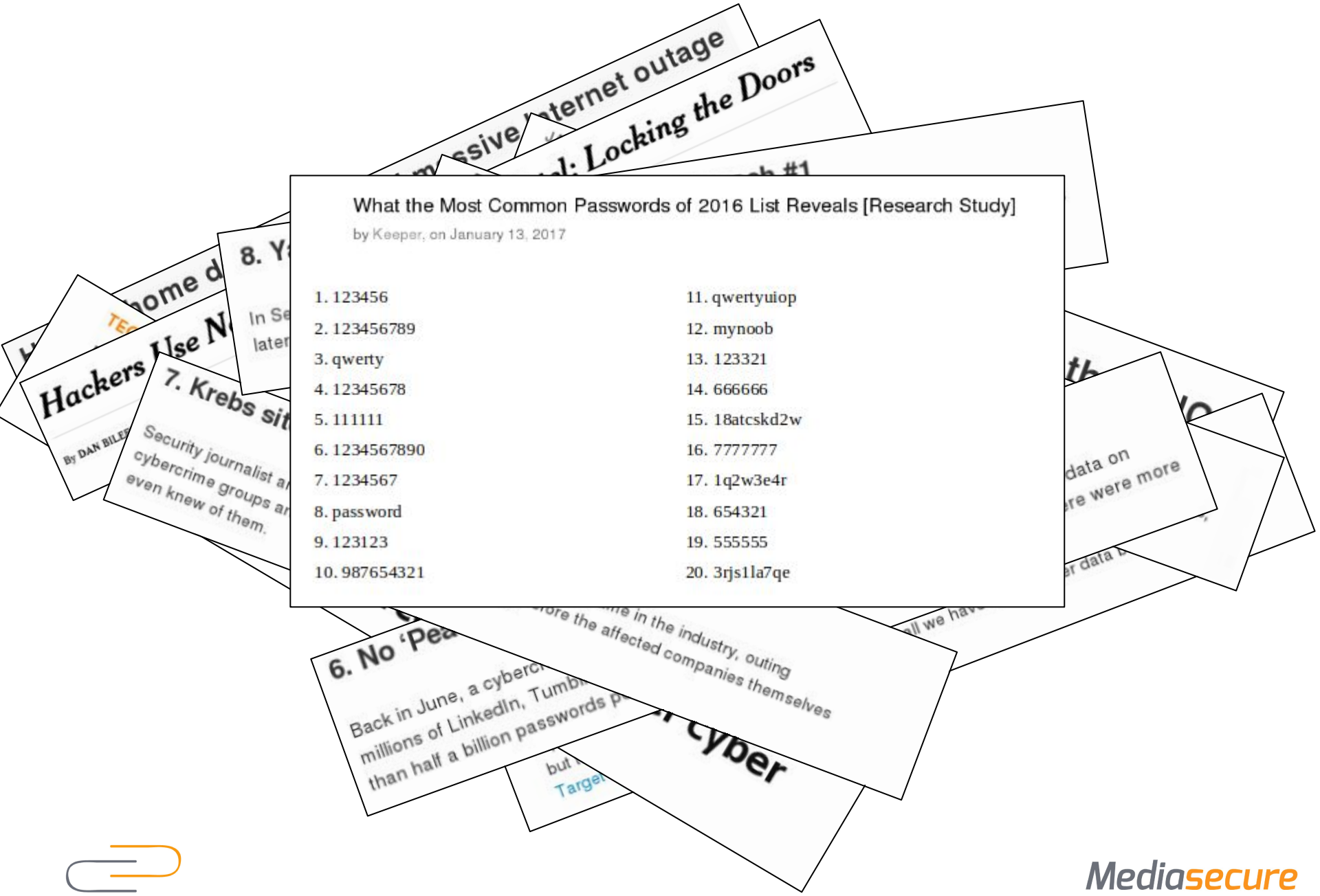
TOOL PER COLLEZIONARE INFORMAZIONI SU INTERNET

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

→ DEMO ←

Dnsmap - The Harvester - Recon-ng

```
root@test-kalbox:~# theharvester -b google -l 50 -d nathanheafner.com

*******************************************************************
*                                                                 *
*  _   _                                            _            *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Google:
        Searching 0 results...


[+] Emails found:
------------------
No emails found

[+] Hosts found in search engines:
-----------------------------------
[-] Resolving hostnames IPs...
173.201.141.128:www.nathanheafner.com
root@test-kalbox:~#
```



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

Mediasecure

Fase 2: AUTOMATIZZAZIONE MAPPATURA

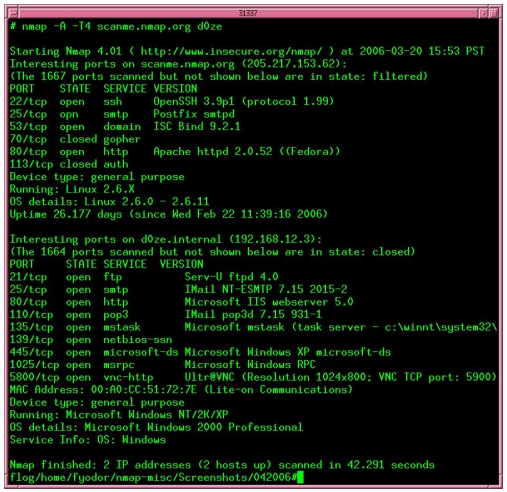
✓ ESEMPIO DI SCRIPT PER MAPPATURA CLIENTE

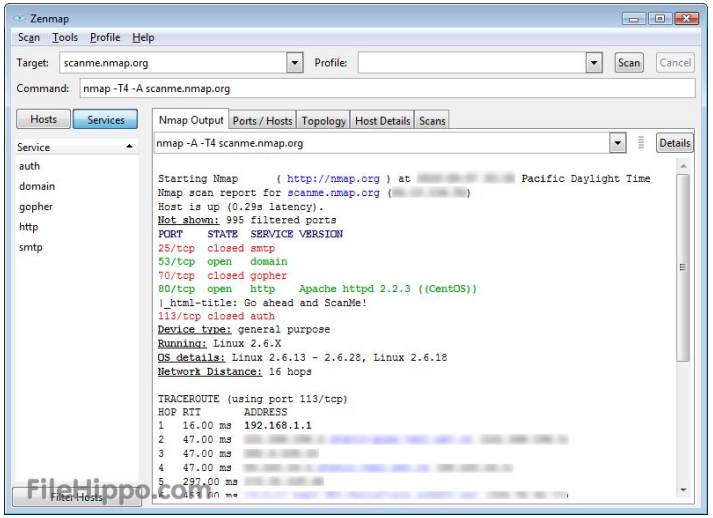
```
#/bin/bash
SCANDIR=/home/SCAN
DNSMAP=/usr/bin/dnsmap
DNSMAPLIST=$SCANDIR/scripts/MSdnslist.txt
HARVESTER=/usr/bin/theharvester
PIDFILE=/var/run/scan.sh
## variables for sendEmail
HOST=`hostname`
RELAY=smtpovpn.mediasecure.it
SENDER=lchiavacci@mediasecure.it
RECEIVER=mediacheck@mediasecure.it
SENDEMAIL=/usr/bin/sendemail
DAY=$(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
}

printent()
{
 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 -- \npid : $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 '-' ',' | awk -F "," '{printf "%s.%s.%s.%s-%s\n", $1,$2,$3,$4,$8}'> $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 -d $DOMINIO -b all >> $TOTALIPS

done
## move list file into DONE directory

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

## send email if results are available
if [ -s $TOTALIP ] ; then
 echo "invio mail risultati"
 $SENDEMAIL -o tls=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



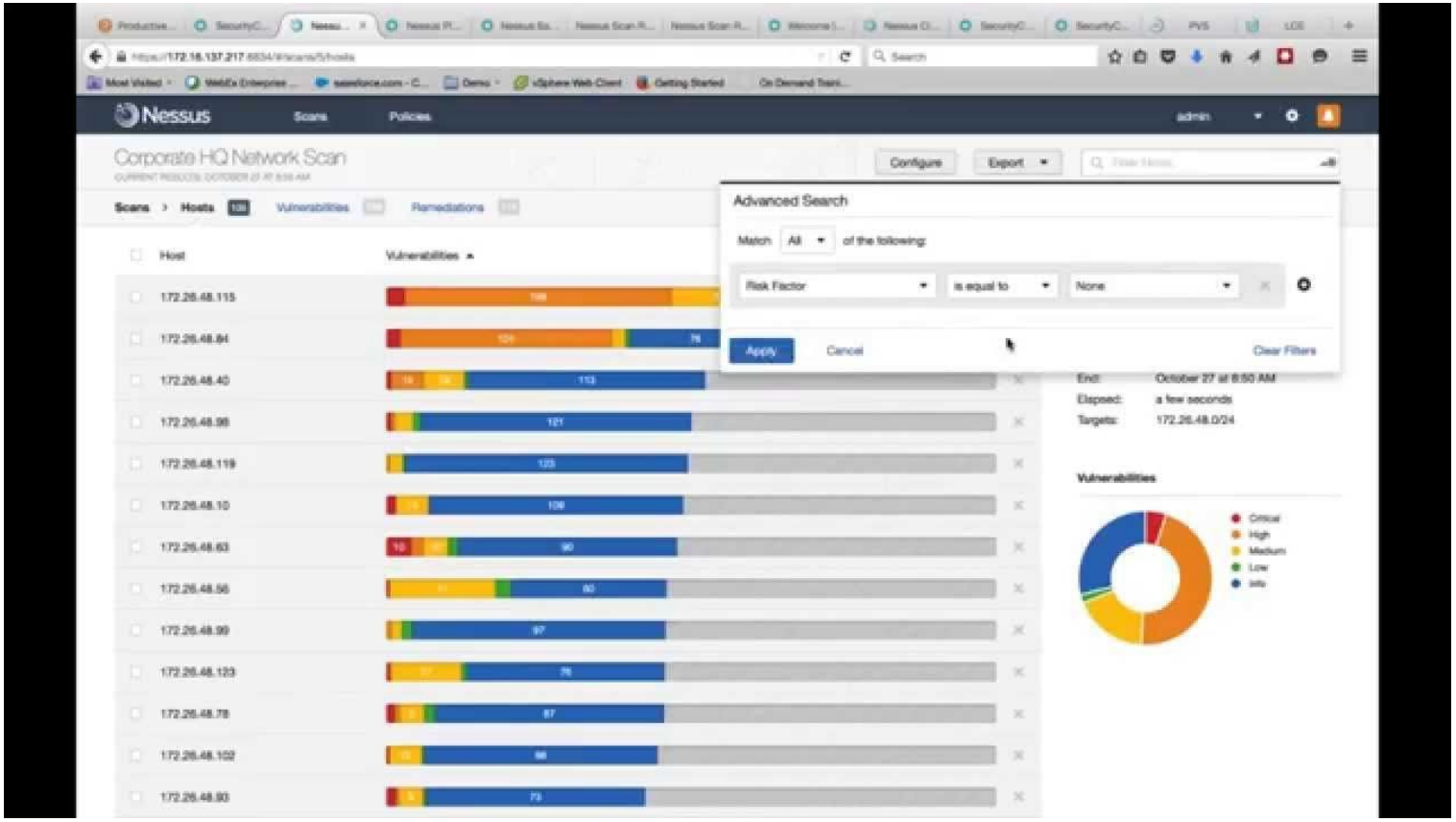


- ✓ NMAP – NON SOLO PORT MAPPING
- ✓ NMAP SCRIPTING ENGINE (https://nmap.org/book/nse.html)
- ✓ REFERENCE : https://nmap.org/nsedoc/ PER ELENCO CATEGORIE SCRIPT
- ✓ MAPPATURA VELOCE SU SUBSET DI PORTE
  - ✓ *#nmap -sS -p 22,23,1433,3306,5900,3389*
- ✓ PROVATE SU RANGE INTERNET DI PROVIDER E TROVERETE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

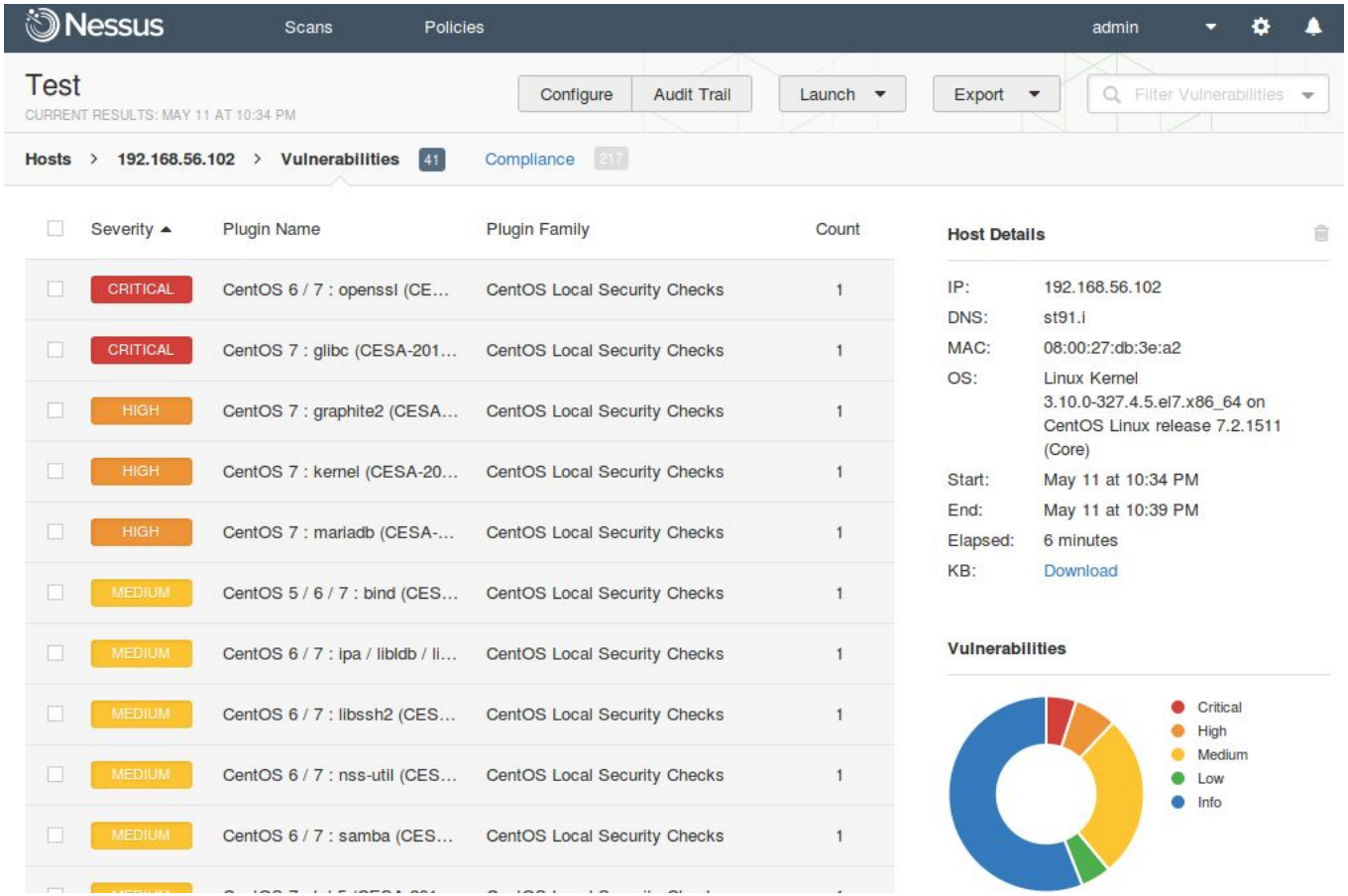
✓

→ DEMO ←
Nmap

Fase 2: ANALISI NESSUS RESULT



Fase 2: ANALISI REPORT

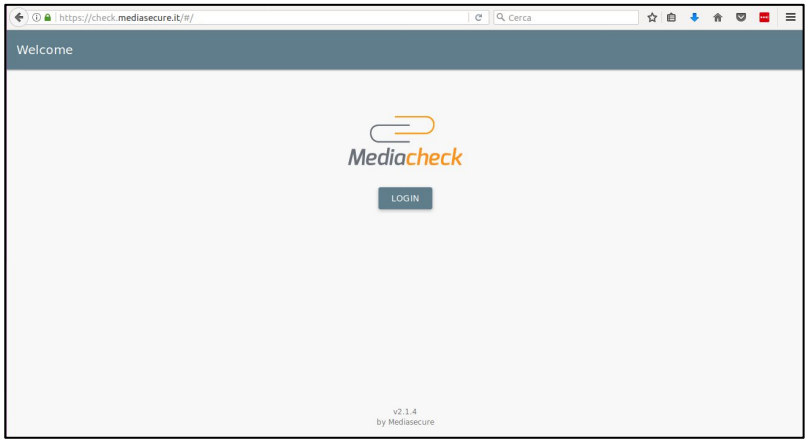


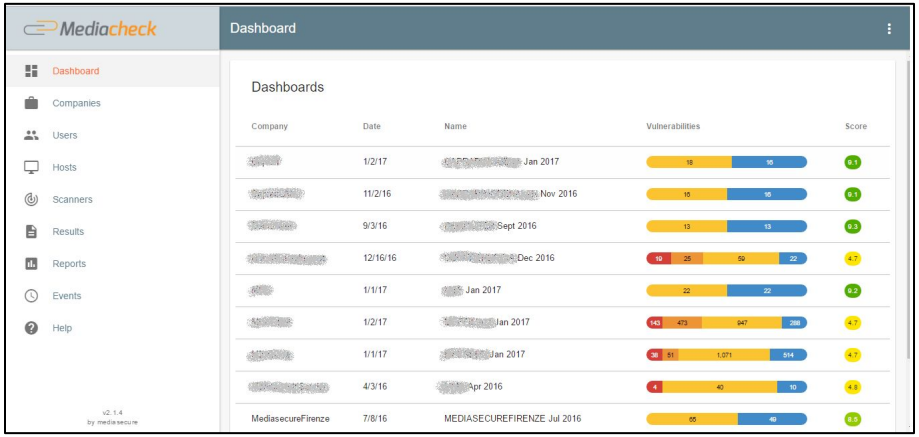
→ DEMO ←

Nessus

Mediasecure

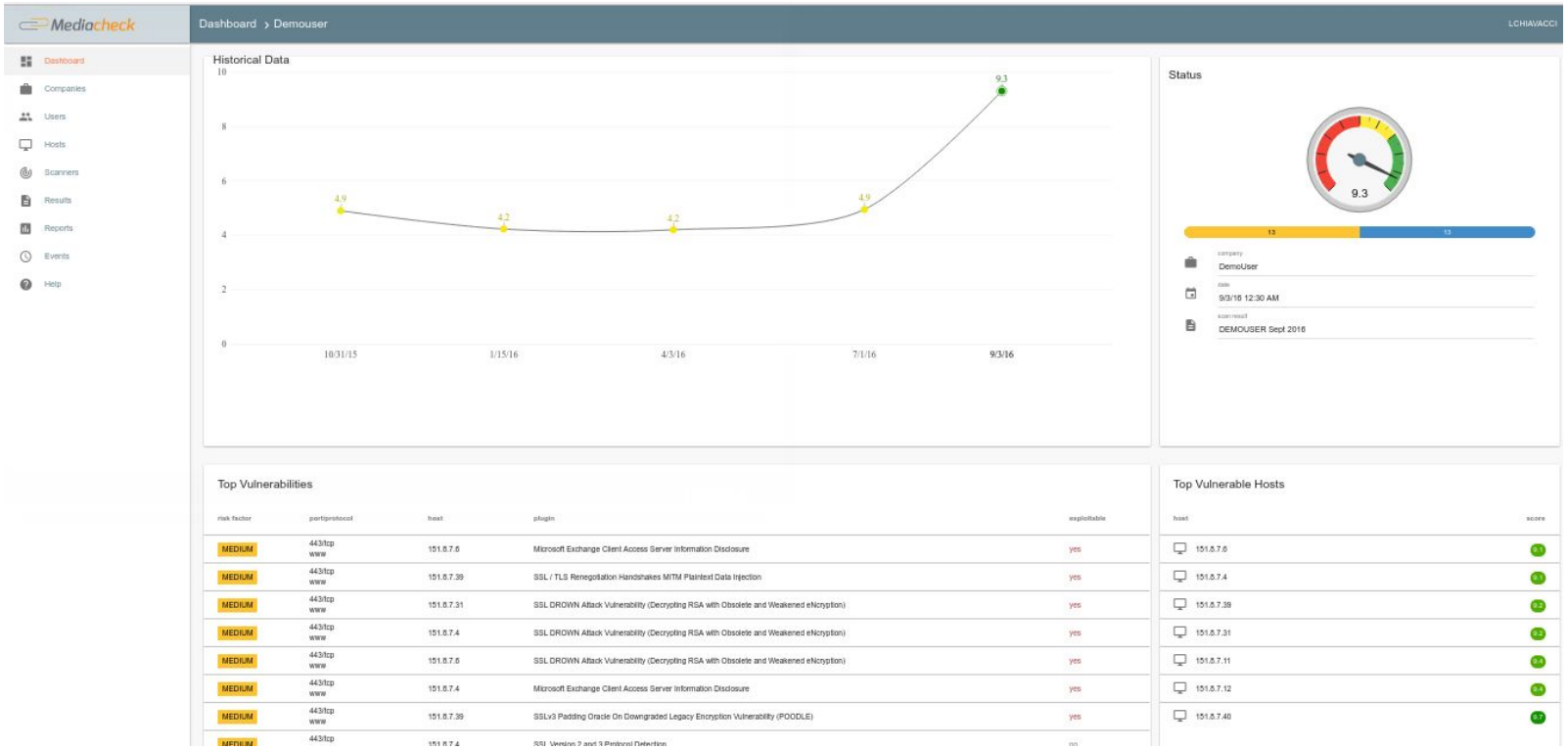
Fase 2: PICCOLO SPAZIO PUBBLICITARIO MEDIACHECK





- ✓ MEDIASECURE 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

Dictionary Attack

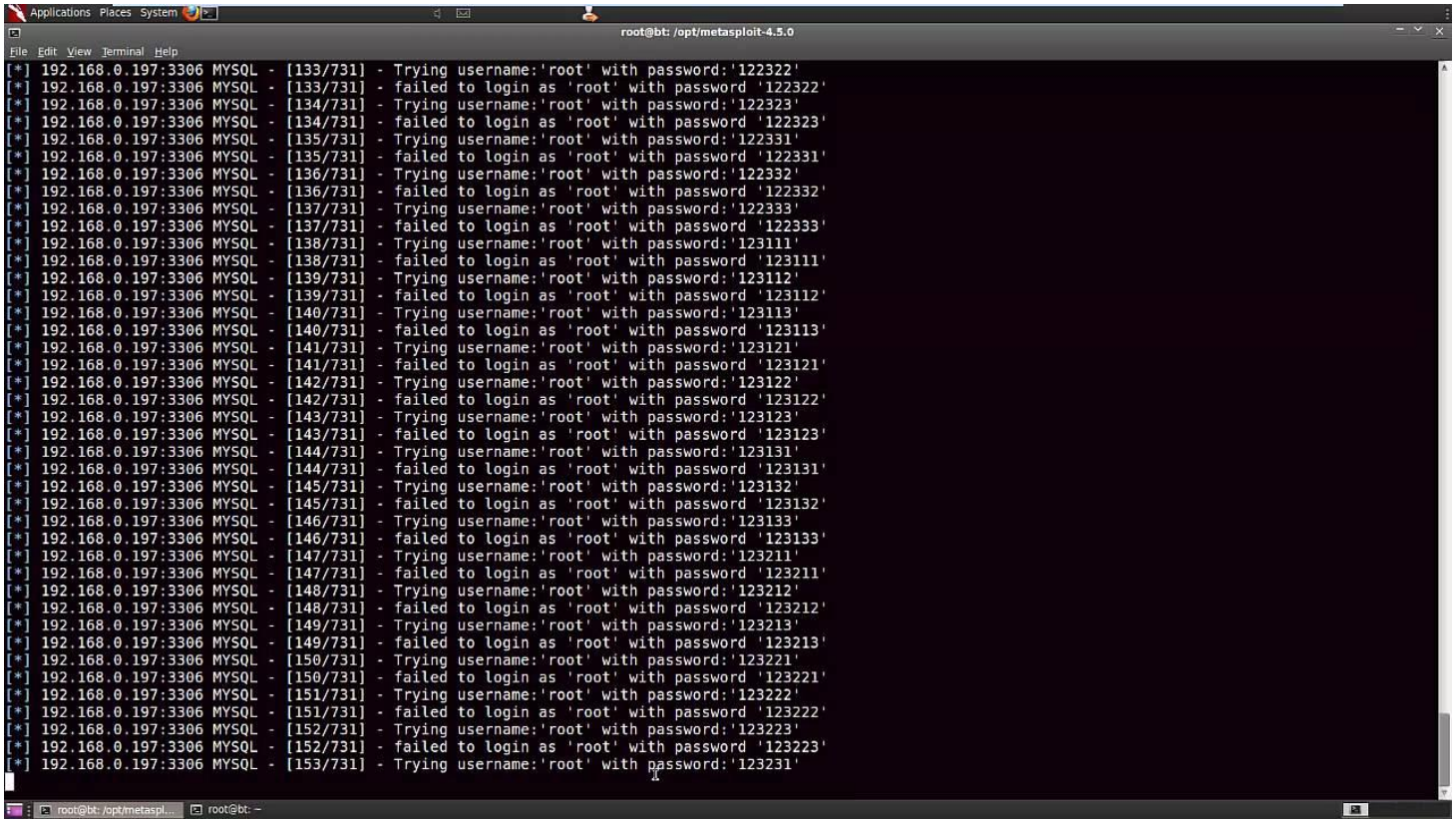
- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

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

Fase 3: HYDRA

→ DEMO ←

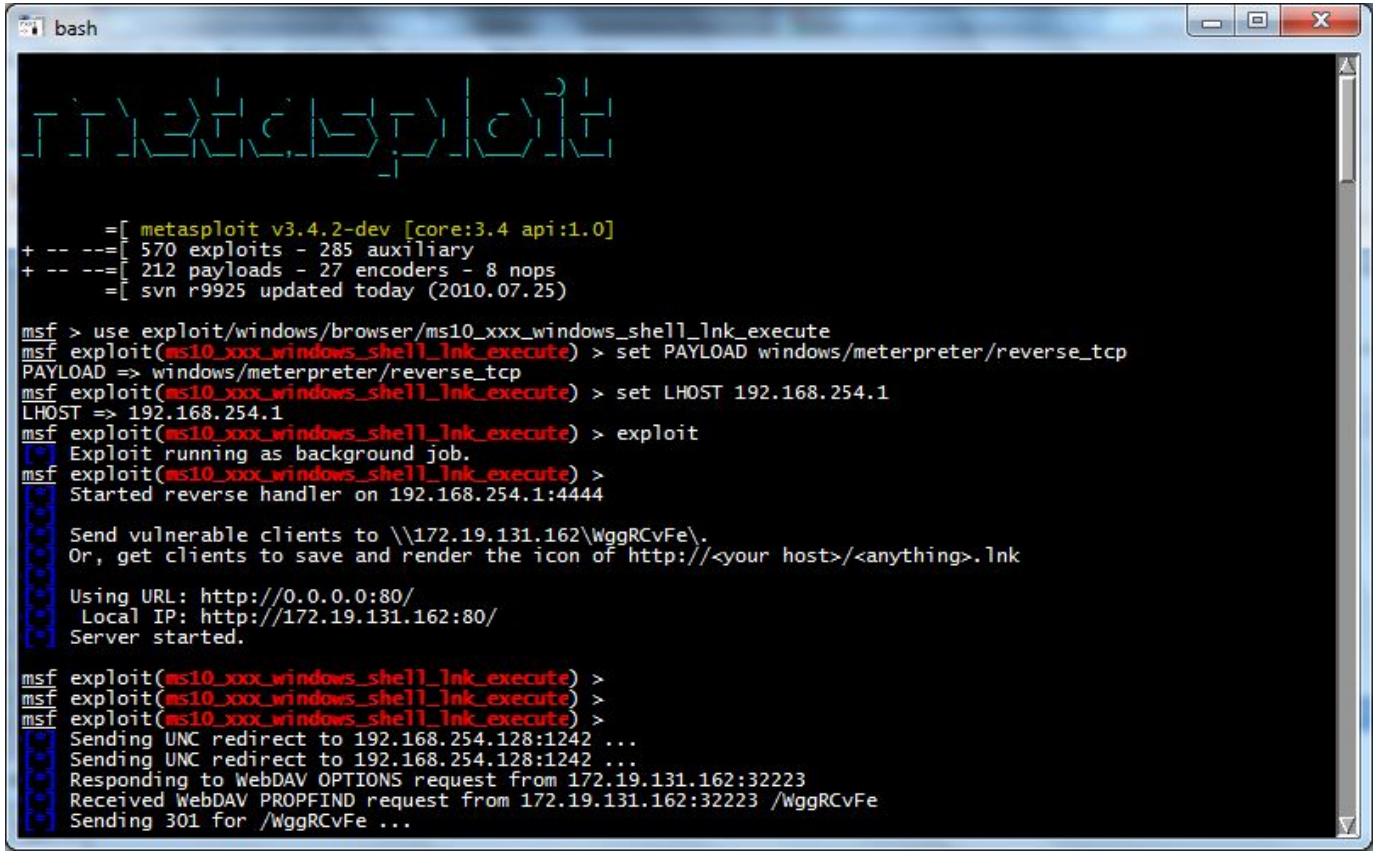
Hydra



Fase 3: SFRUTTARE LE VULNERABILITÀ

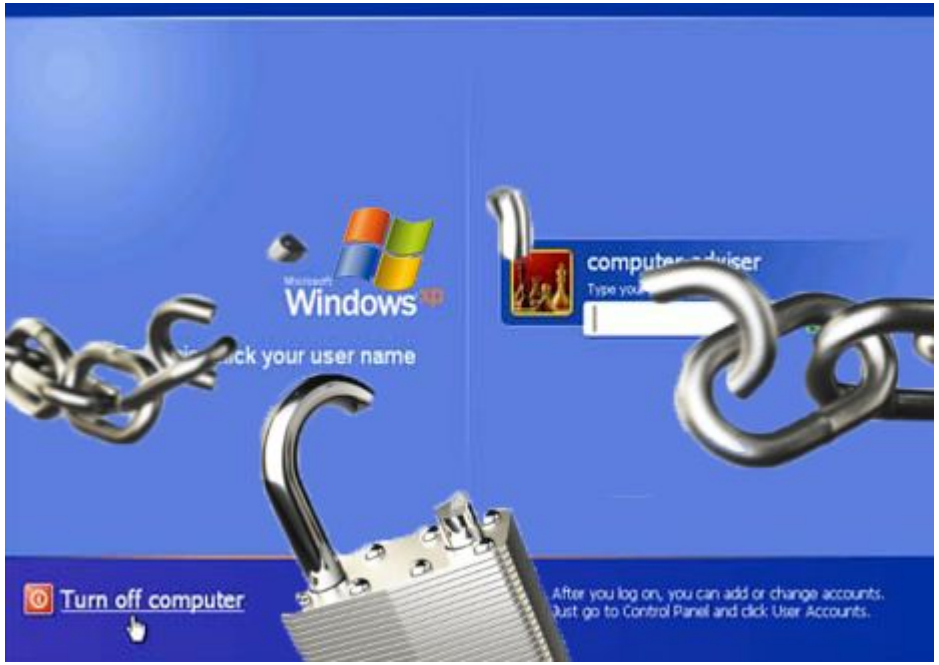
- ✓ ADESSO IL GIOCO SI FA DURO
- ✓ ABBIAMO LE POSSIBILI STRADE DI ACCESSO E DOBBIAMO VERIFICARE SE QUALCHE PORTA E’ DEBOLE
- ✓ EXPLOIT DB (https://www.exploit-db.com/)
- ✓ METASPLOIT - DISPONIBILE SU KALI LINUX

Fase 3: METASPLOIT

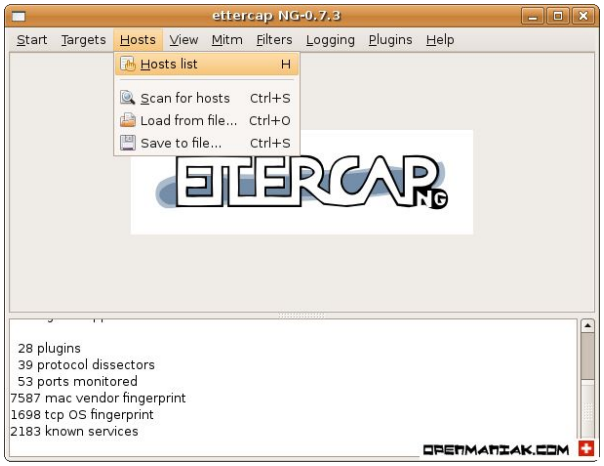


→ DEMO ←

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

- 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

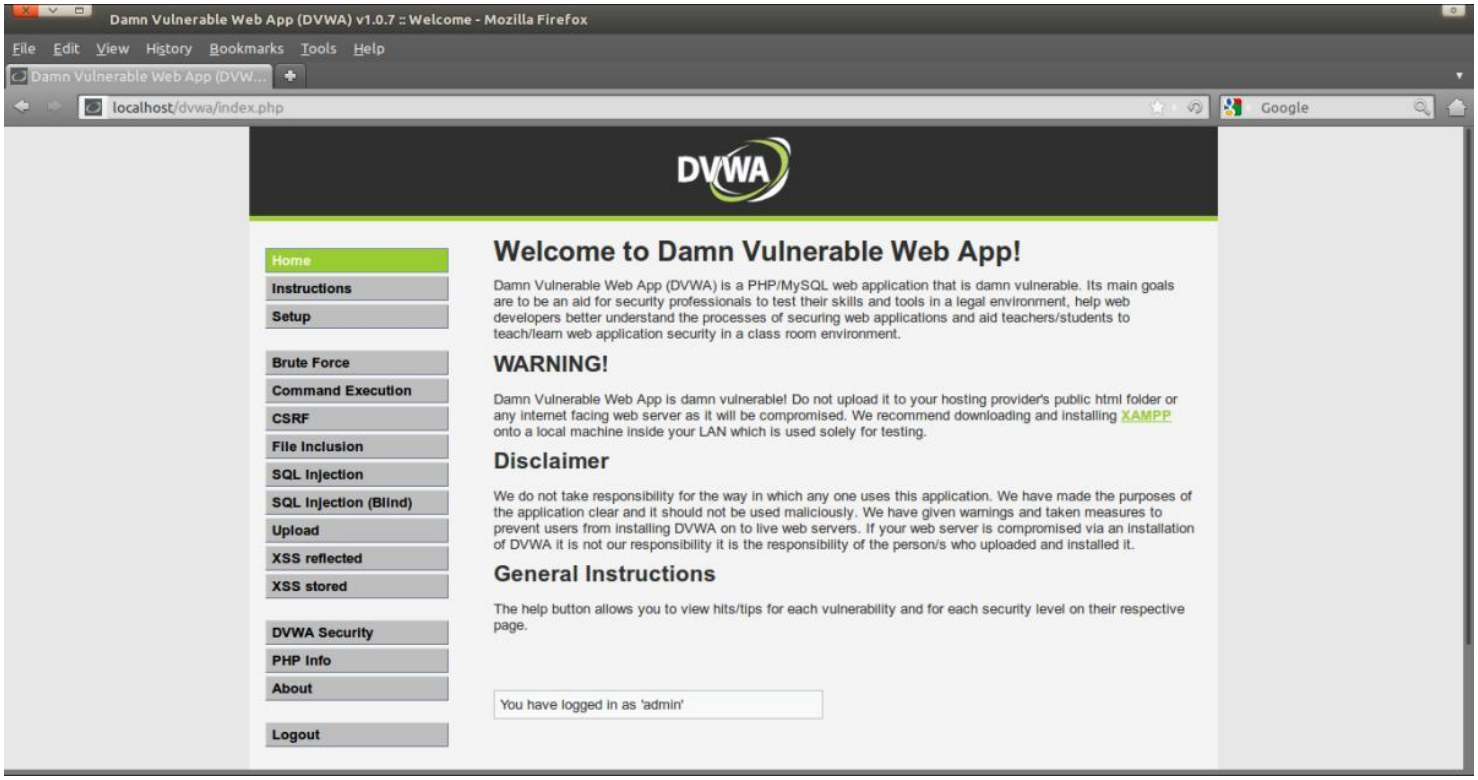
WEB APPLICATION PENTESTING

- ✓ ANALIZZARE UNA APPLICAZIONE WEB E SCOPRIRNE 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)

→ DEMO ←
Ambiente DVWA



E ADESSO METTIAMOCI A STUDIARE...

- ✓ CIBRARY (www.cibrary.it)
- ✓ ELEARNSECURITY (www.elearnsecurity.it)
- ✓ SANS INSTITUTE (www.sans.org)

Mediasecure