Vulnerabilità e Difesa dei Sistemi Internet

A.K.A. ETHICAL HACKING

FRANCESCO MANCINI – francesco.mancini@uniroma2.it

PASQUALE CAPORASO - pasquale.caporaso@uniroma2.it

SARA DA CANAL – sara.da.canal@uniroma2.it

PIERCIRO CALIANDRO – pierciro.caliandro@uniroma2.it

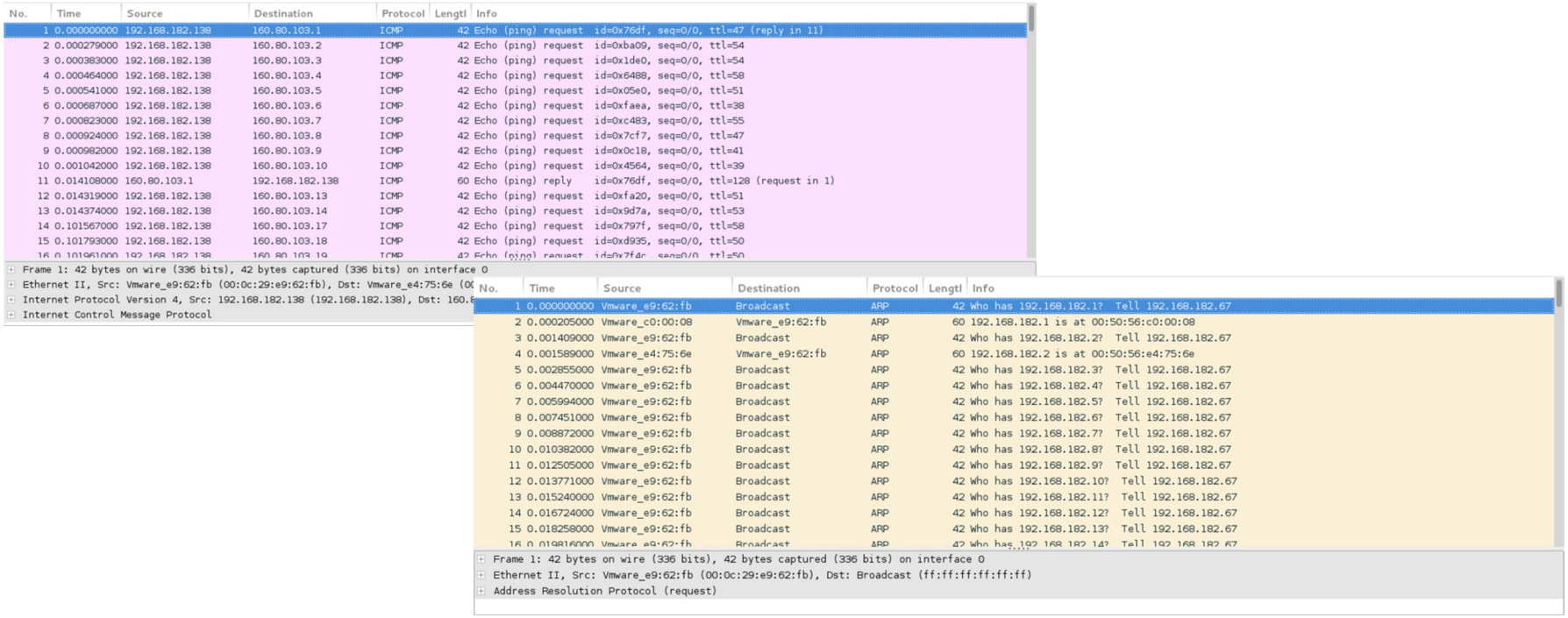
Vulnerabilità e Difesa dei Sistemi Internet

A.K.A. ETHICAL HACKING

Recap: scan the network

```
root@kali:~# nmap -sP 192.168.182.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-29 17:55 EDT
Nmap scan report for 192.168.182.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.182.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:E4:75:6E (VMware)
Nmap scan report for 192.168.182.135
Host is up (0.000097s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.182.254
Host is up (0.00031s latency).
MAC Address: 00:50:56:F1:DD:7D (VMware)
Nmap scan report for 192.168.182.138
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.00 seconds
```

Recap: scanning traces…



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.182.138	160.80.103.1	ICMP	42	Echo (ping) request id=0x76df, seq=0/0, ttl=47 (reply in 11)
2	0.000279000	192.168.182.138	160.80.103.2	ICMP	42	Echo (ping) request id=0xba09, seq=0/0, ttl=54
3	0.000383000	192.168.182.138	160.80.103.3	ICMP	42	Echo (ping) request id=0x1de0, seq=0/0, ttl=54
4	0.000464000	192.168.182.138	160.80.103.4	ICMP	42	Echo (ping) request id=0x6488, seq=0/0, ttl=58
5	0.000541000	192.168.182.138	160.80.103.5	ICMP	42	Echo (ping) request id=0x05e0, seq=0/0, ttl=51
6	0.000687000	192.168.182.138	160.80.103.6	ICMP	42	Echo (ping) request id=0xfaea, seq=0/0, ttl=38
7	0.000823000	192.168.182.138	160.80.103.7	ICMP	42	Echo (ping) request id=0xc483, seq=0/0, ttl=55
8	0.000924000	192.168.182.138	160.80.103.8	ICMP	42	Echo (ping) request id=0x7cf7, seq=0/0, ttl=47
9	0.000982000	192.168.182.138	160.80.103.9	ICMP	42	Echo (ping) request id=0x0c18, seq=0/0, ttl=41
10	0.001042000	192.168.182.138	160.80.103.10	ICMP	42	Echo (ping) request id=0x4564, seq=0/0, ttl=39
11	0.014108000	160.80.103.1	192.168.182.138	ICMP	60	Echo (ping) reply id=0x76df, seq=0/0, ttl=128 (request in 1)
12	0.014319000	192.168.182.138	160.80.103.13	ICMP	42	Echo (ping) request id=0xfa20, seq=0/0, ttl=51
13	0.014374000	192.168.182.138	160.80.103.14	ICMP	42	Echo (ping) request id=0x9d7a, seq=0/0, ttl=53
14	0.101567000	192.168.182.138	160.80.103.17	ICMP	42	Echo (ping) request id=0x797f, seq=0/0, ttl=58
15	0.101793000	192.168.182.138	160.80.103.18	ICMP	42	Echo (ping) request id=0xd935, seq=0/0, ttl=50
16	0.101961000	192.168.182.138	160.80.103.19	ICMP	42	Echo (ping) request id=0x7f4c, seq=0/0, ttl=50

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Vmware_e9:62:fb (00:0c:29:e9:62:fb), Dst: Vmware_e4:75:6e (00
- Internet Protocol Version 4, Src: 192.168.182.138 (192.168.182.138), Dst: 160.8
- Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.1? Tell 192.168.182.67
2	0.000205000	Vmware_c0:00:08	Vmware_e9:62:fb	ARP	60	192.168.182.1 is at 00:50:56:c0:00:08
3	0.001409000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.2? Tell 192.168.182.67
4	0.001589000	Vmware_e4:75:6e	Vmware_e9:62:fb	ARP	60	192.168.182.2 is at 00:50:56:e4:75:6e
5	0.002855000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.3? Tell 192.168.182.67
6	0.004470000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.4? Tell 192.168.182.67
7	0.005994000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.5? Tell 192.168.182.67
8	0.007451000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.6? Tell 192.168.182.67
9	0.008872000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.7? Tell 192.168.182.67
10	0.010382000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.8? Tell 192.168.182.67
11	0.012505000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.9? Tell 192.168.182.67
12	0.013771000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.10? Tell 192.168.182.67
13	0.015240000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.11? Tell 192.168.182.67
14	0.016724000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.12? Tell 192.168.182.67
15	0.018258000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.13? Tell 192.168.182.67
16	0.019816000	Vmware_e9:62:fb	Broadcast	ARP	42	Who has 192.168.182.14? Tell 192.168.182.67

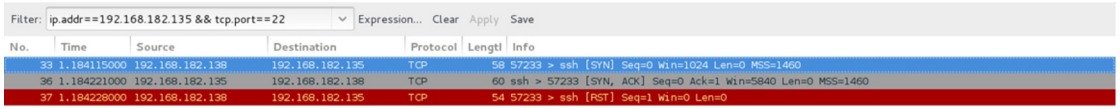
- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Vmware_e9:62:fb (00:0c:29:e9:62:fb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

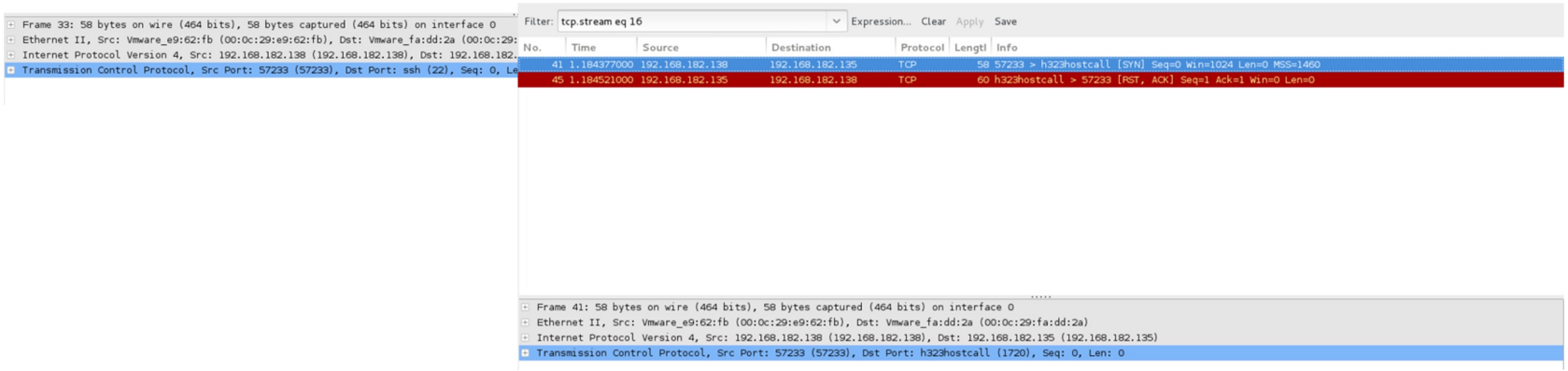
Recap: scan the host

```
root@kali:~# nmap -sS 192.168.182.135

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-29 17:53 EDT
Nmap scan report for 192.168.182.135
Host is up (0.00012s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

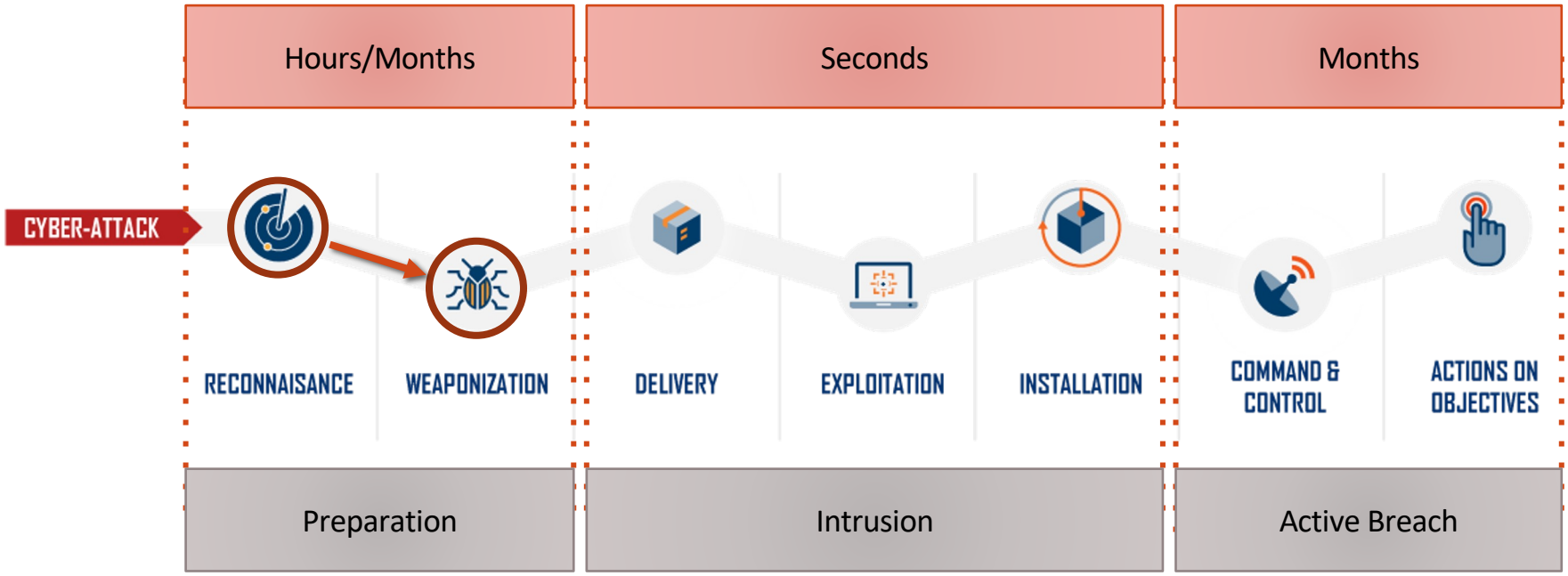
```
root@kali:~# nmap -sS -A 192.168.182.135

Starting Nmap 6.47 ( http://nmap.org ) at 2015-04-29 17:50 EDT
Nmap scan report for 192.168.182.135
Host is up (0.00048s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=
| Not valid before: 2010-03-17T13:07:45+00:00
|_Not valid after:  2010-04-16T13:07:45+00:00
|_ssl-date: 2015-04-29T20:43:30+00:00; -1h07m19s from local time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-methods: No Allow or Public header in OPTIONS response (status code 2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3     35393/tcp  mountd
|_  100005  1,2,3     54881/udp  mountd
```

Recap: scanning traces…





How a cyber-attack starts?



SMB Enumeration

The Server Message Block

- Provides shared access to files, printers and serial ports
- Usato a partire da Windows 95, Samba permette di utilizzarlo su sistemi unix
- Security track record has been poor for over a decade
  - Due to its complex implementation and open nature
  - From unauthenticated SMB null sessions in Windows 2000 and XP, to a plethora of SMB bugs and vulnerabilities over the years, SMB has seen its fair share of action
- The SMB NetBIOS service listens on TCP ports **139** and **445**
  - as well as several UDP ports
  - **nmap -v -p 139,445 -oG smb.txt <ip range>**
  - **nbtscan -r <subnet or ip address>**

SMB Enumeration

The Server Message Block

- Provides shared access to files, printers and serial ports
- Security track record has been poor for over a decade
  - Due to its complex implementation and open nature
  - From unauthenticated SMB null sessions in Windows 2000 and XP, to a plethora of SMB bugs and vulnerabilities over the years, SMB has seen its fair share of action (**EternalBlue**)

- Enumeration
  - Smbclient
  - Enum4linux
  - Nullinux
  - …

SMB Enumeration

Nmap contains many useful NSE scripts that can be used to discover and enumerate SMB services

- These scripts can be found in ***/usr/share/nmap/scripts***

```
root@kali:~# nmap -p445,139 --script=smb-os-discovery 172.28.128.5

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-25 23:38 CEST
Nmap scan report for 172.28.128.5
Host is up (0.00032s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:F5:89:C0 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2016-10-25T17:38:50-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
root@kali:~#
```

SMB Enumeration

Enum4Linux permette di estrarre diverse informazioni dall'SMB server target

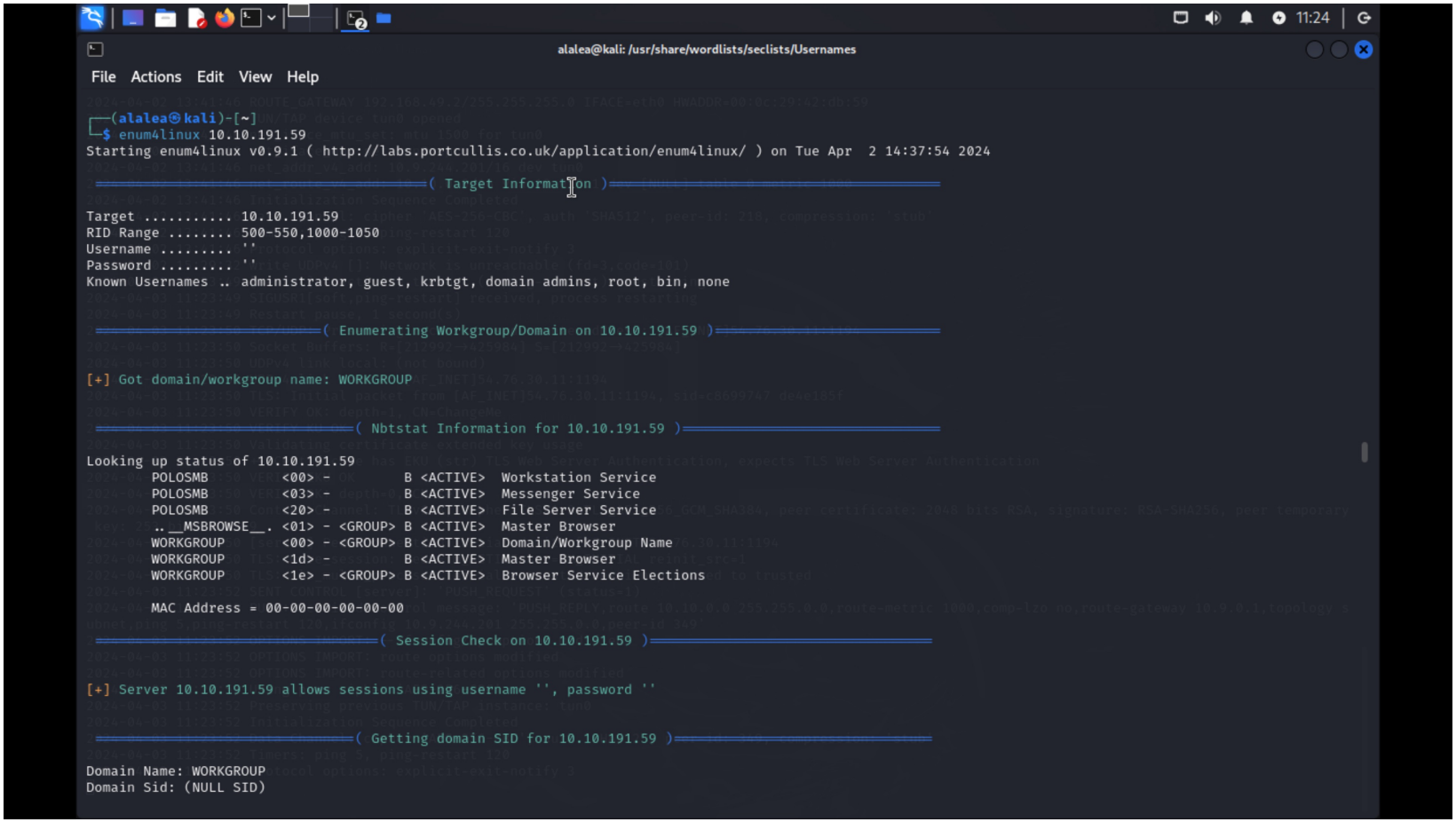
Diverse opzioni:

TAG	FUNCTION
-U	get userlist
-M	get machine list
-N	get namelist dump (different from -U and-M)
-S	get sharelist
-P	get password policy information
-G	get group and member list
-a	all of the above (full basic enumeration)

Sintassi:

"enum4linux [options] ip"

SMB Enumeration



NMAP scripting

Simply specify -sC to enable the most common scripts

- Or specify the --script option to choose your own scripts to execute by providing categories, script file names, or the name of directories full of scripts you wish to execute.
- You can customize some scripts by providing arguments to them via the --script-args and --script-args-file options.
- The --script-help shows a description of what each selected script does
- Script scanning is also included as part of the -A(aggressive scan) option.

Script scanning is normally done in combination with a port scan, because scripts may be run or not run depending on the port states found by the scan.

- With the -sn option it is possible to run a script scan without a port scan, only host discovery. In this case only host scripts will be eligible to run.
- To run a script scan with neither a host discovery nor a port scan, use the -Pn -sn options together with -sC or --script.
- Every host will be assumed up and still only host scripts will be run. This technique is useful for scripts like whois that only use the remote system's address and don't require it to be up.

NMAP scripting

NSE scripts define a list of categories:

- **auth** These scripts deal with authentication credentials (or bypassing them) on the target system
- **broadcast** Scripts in this category typically do discovery of hosts not listed on the command line by broadcasting on the local network
- **brute** These scripts use brute force attacks to guess authentication credentials of a remote server
- **discovery** These scripts try to actively discover more about the network by querying public registries, SNMP-enabled devices, directory services, etc.
  - Examples include html-title (obtains the title of the root path of web sites), smb-enum-shares (enumerates Windows shares), and snmp-sysdescr (extracts system details via SNMP).
- **dos** Scripts in this category may cause a denial of service. These tests sometimes crash vulnerable services.
- **exploit** These scripts aim to actively exploit some vulnerability.
- **external** Scripts in this category may send data to a third-party database or other network resource. An example of this is whois, which makes a connection to whois server.
- **fuzzer** This category contains scripts which are designed to send server software unexpected or randomized fields in each packet
- **intrusive** These are scripts that cannot be classified in the safe category because the risks are too high that they will crash the target system, use up significant resources on the target host (such as bandwidth or CPU time), or otherwise be perceived as malicious by the target's system administrators
- **malware** These scripts test whether the target platform is infected by malware or backdoors
- **safe** Scripts which weren't designed to crash services, use large amounts of network bandwidth or other resources, or exploit security holes are categorized as safe
- **version** The scripts in this special category are an extension to the version detection feature and cannot be selected explicitly. They are selected to run only if version detection (-sV) was requested
- **vuln** These scripts check for specific known vulnerabilities and generally only report results if they are found

NMAP scripting

- **default** These scripts are the default set and are run when using the -sC or -A options rather than listing scripts with --script. Many factors are considered in deciding whether a script should be run by default:
  - **Speed** A default scan must finish quickly
  - **Usefulness** Default scans need to produce valuable and actionable information
  - **Verbosity** Nmap output is used for a wide variety of purposes and needs to be readable and concise
  - **Reliability** Many scripts use heuristics and fuzzy signature matching to reach conclusions about the target host or service. If the script is often wrong, it doesn't belong in the default category where it may confuse or mislead casual users
  - **Intrusiveness** Some scripts are very intrusive because they use significant resources on the remote system, are likely to crash the system or service, or are likely to be perceived as an attack by the remote administrators. The more intrusive a script is, the less suitable it is for the default category
  - **Privacy** Some scripts, particularly those in the external category described later, divulge information to third parties by their very nature. The more privacy-invasive a script is, the less suitable it is for default category inclusion

NMAP scripting

nmap --script default,safe
- Loads all scripts in the default and safe categories.

nmap --script smb-os-discovery
- Loads only the smb-os-discovery script. Note that the .nse extension is optional.

nmap --script default,banner,/home/user/customscripts
- Loads the script in the default category, the banner script, and all .nse files in the directory /home/user/customscripts.

nmap --script "http-*”
- Loads all scripts whose name starts with http-, such as http-auth and http-open-proxy. The argument to --script had to be in quotes to protect the wildcard from the shell

nmap --script "not intrusive”
- Loads every script except for those in the intrusive category

nmap --script "default and safe”
- Loads those scripts that are in *both* the default and safe categories

nmap --script "(default or safe or intrusive) and not http-*”
- Loads scripts in the default, safe, or intrusive categories, except for those whose names start with http-…

nmap -sC --script-args 'user=foo,pass=",{}=bar",whois={whodb=nofollow+ripe},xmpp-info.server_name=localhost’ …
- Pass arguments to the scripts

Anatomy of NMAP scripts

When writing Nmap NSE scripts (LUA)

- We need a way to check the information that was already gathered about the scanning host or network when running a script
- This can be achieved by passing certain arguments to the NSE script within the **action** function

```
action = function( host, port )
    local out = grab_banner(host, port)
    return output( out )
end
```

We can see that the action function accepts two parameters

- the **host** and **port**
- The host argument passed into the action function contains information about the host we're about to scan
- The port argument contains the port about to be scanned.

We can then use the **host** and **port** objects in the NSE script to request specific information that we require.

Discover vulnerabilities with NMAP

Vulnerability scanning is the process of using automated tools to

- Discover and identify vulnerabilities in a network
- Vulnerability scanners come in many different forms
  - Simple scripts that identify a single vulnerability
  - Complex commercial software engines that scan for thousands of them
- Vulnerability scans can generate a great deal of traffic and can even result in denial of service conditions on many network devices

- **cd /usr/share/nmap/scripts/**
- **ls -l *vuln***
- **nmap -v -p 21 --script=ftp-anon.nse <ip address>**

Discover vulnerabilities with NMAP

```
root@kali:~# nmap -p445,139 --script=smb-vuln-cve2009-3103.nse 172.28.128.5

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-25 23:51 CEST
Nmap scan report for 172.28.128.5
Host is up (0.00029s latency).
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:F5:89:C0 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys i
n Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote att
ackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a
 Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of
an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103

Nmap done: 1 IP address (1 host up) scanned in 5.56 seconds
```

Telnet

Telnet è un protocollo applicativo che consente, con l'uso di un client telnet, di connettersi ed eseguire comandi su un computer remoto che ospita un server telnet.

Il client telnet stabilisce una connessione con il server. Il client diventa quindi un terminale virtuale che consente di interagire con l'host remoto.

Utilizzo:

telnet [ip] [port]

Telnet invia tutti i messaggi in chiaro e non dispone di meccanismi di sicurezza specifici.

SMTP Enumeration

SMTP mail servers can also be used to gather information

- A *VRFY* request asks the server to verify an email address
- *EXPN* asks the server for the membership of a mailing list
- These can often be abused to verify existing users on a mail server

```
macbook-markin:~ markin$ telnet smtpauth.uniroma2.it 25
Trying 160.80.6.47...
Connected to smtpauth.uniroma2.it.
Escape character is '^]'.
220 smtpauth.uniroma2.it ESMTP Sendmail 8.14.3/8.14.3/Debian-9.4; Tue, 25 Oct 2016 23:56:18 +0200;
142-119-172-5-dyn-dsl.customer.digitelitalia.com [5.172.119.142] (may be forged)
EHLO pentester
250-smtpauth.uniroma2.it Hello ip-142-119-172-5-dyn-dsl.customer.digitelitalia.com [5.172.119.142]
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-STARTTLS
250-DELIVERBY
250 HELP
VRFY alberto.caponi
550 5.1.1 alberto.caponi... User unknown
VRFY root
250 2.1.5 root <root@smtpauth.uniroma2.it>
```

SMTP Enumeration

```
#!/usr/bin/python import socket
import sys
if len(sys.argv) != 3:
    print "Usage: vrfy.py <server> <username>"
    sys.exit(0)

# Create a Socket
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
# Connect to the Server
connect=s.connect((sys.argv[1],25))
# Receive the banner
banner=s.recv(1024)
print banner
# VRFY a user
s.send('VRFY ' + sys.argv[2] + '\r\n')
result=s.recv(1024)
print result
# Close the socket
s.close()
```

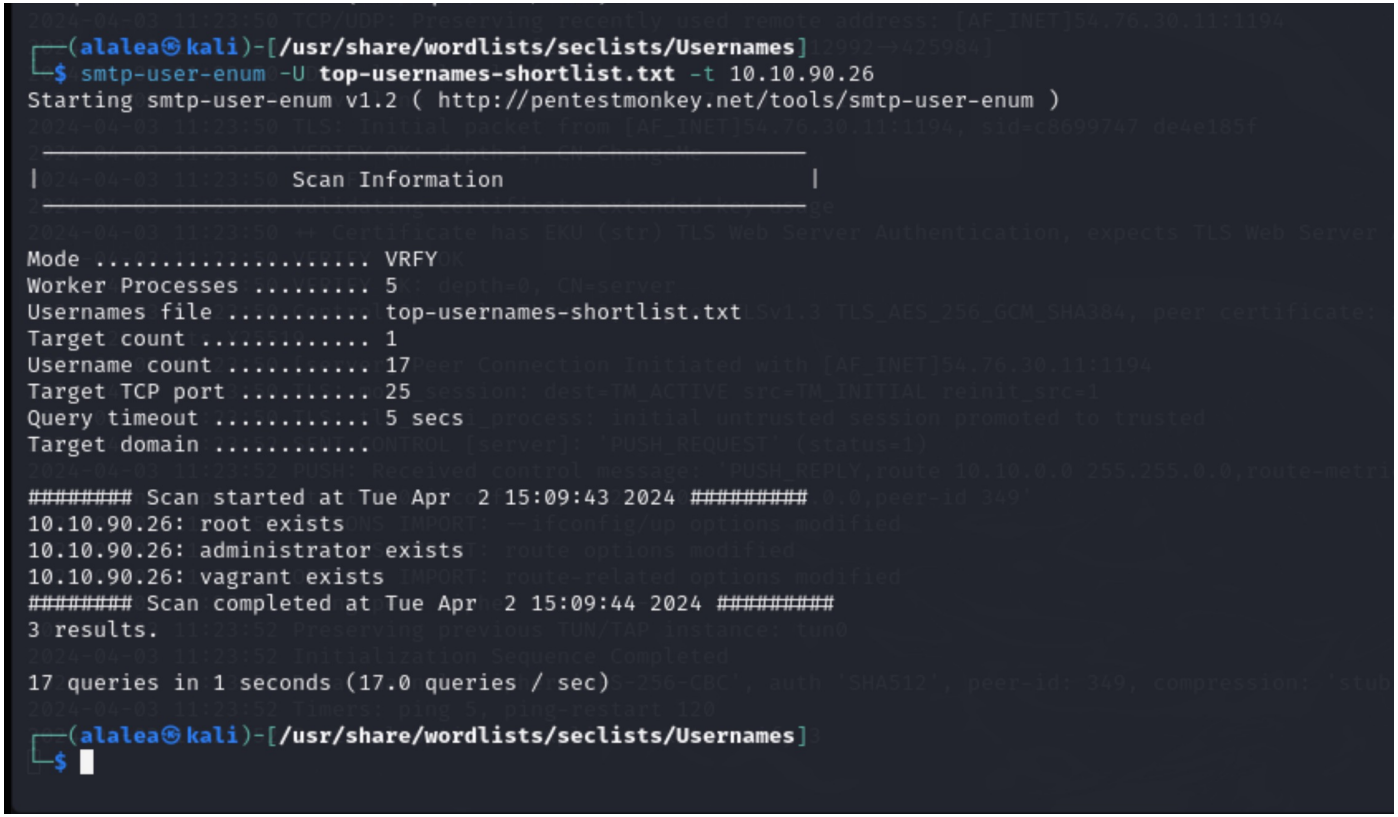
SMTP Enumeration

smtp-user-enum enumera gli utenti di un server mail usando VRFY, EXPN o RCPT

Utilizzo:

smtp-user-enum [options] (-u username | -U file-of-usernames) (-t host | -T file-of-targets)

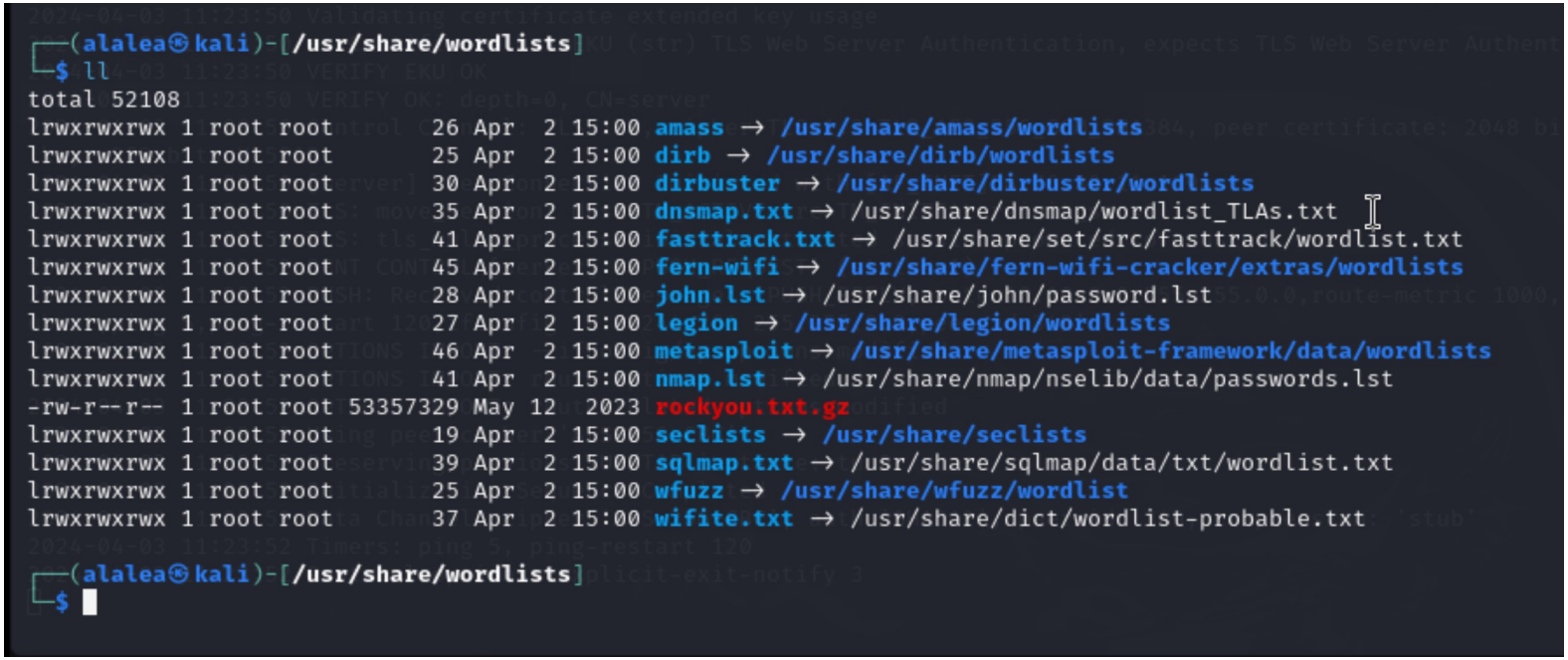
SMTP Enumeration



Wordlists

Presenti di default in /usr/share/wordlists.

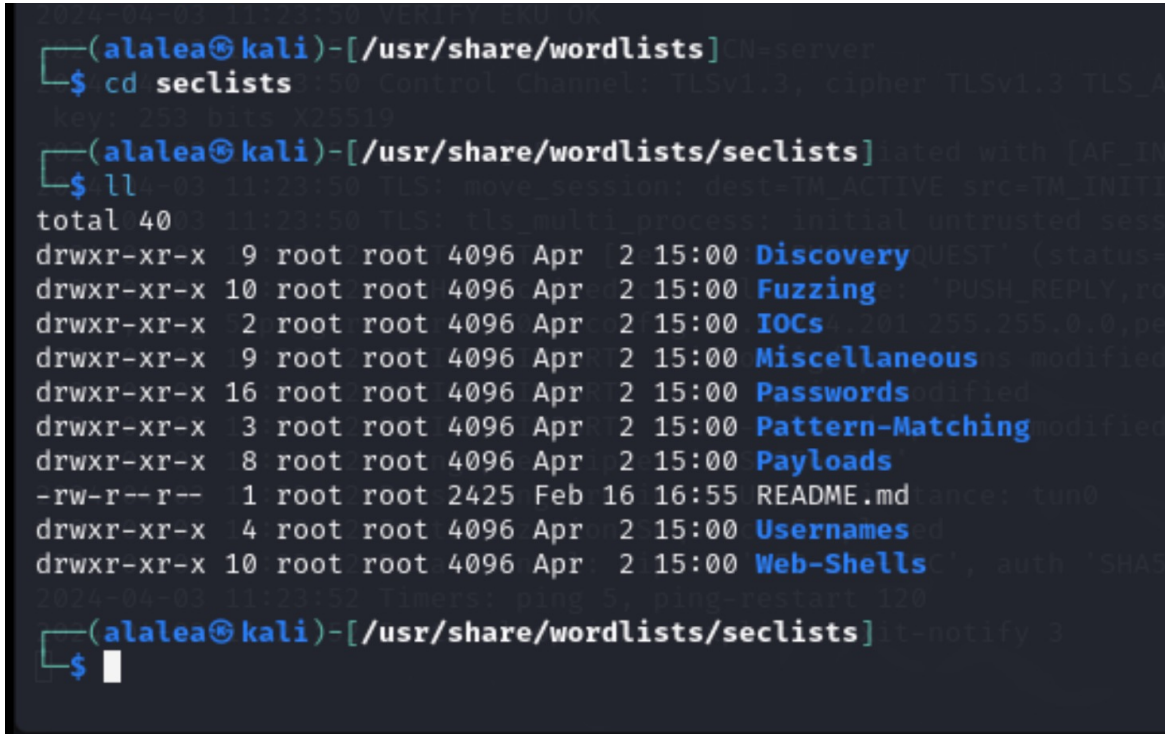
Contengono nomi comuni per utenti, password, enumerazione di directory…



Wordlists

Altre possono essere installate:

sudo apt install seclists



FTP

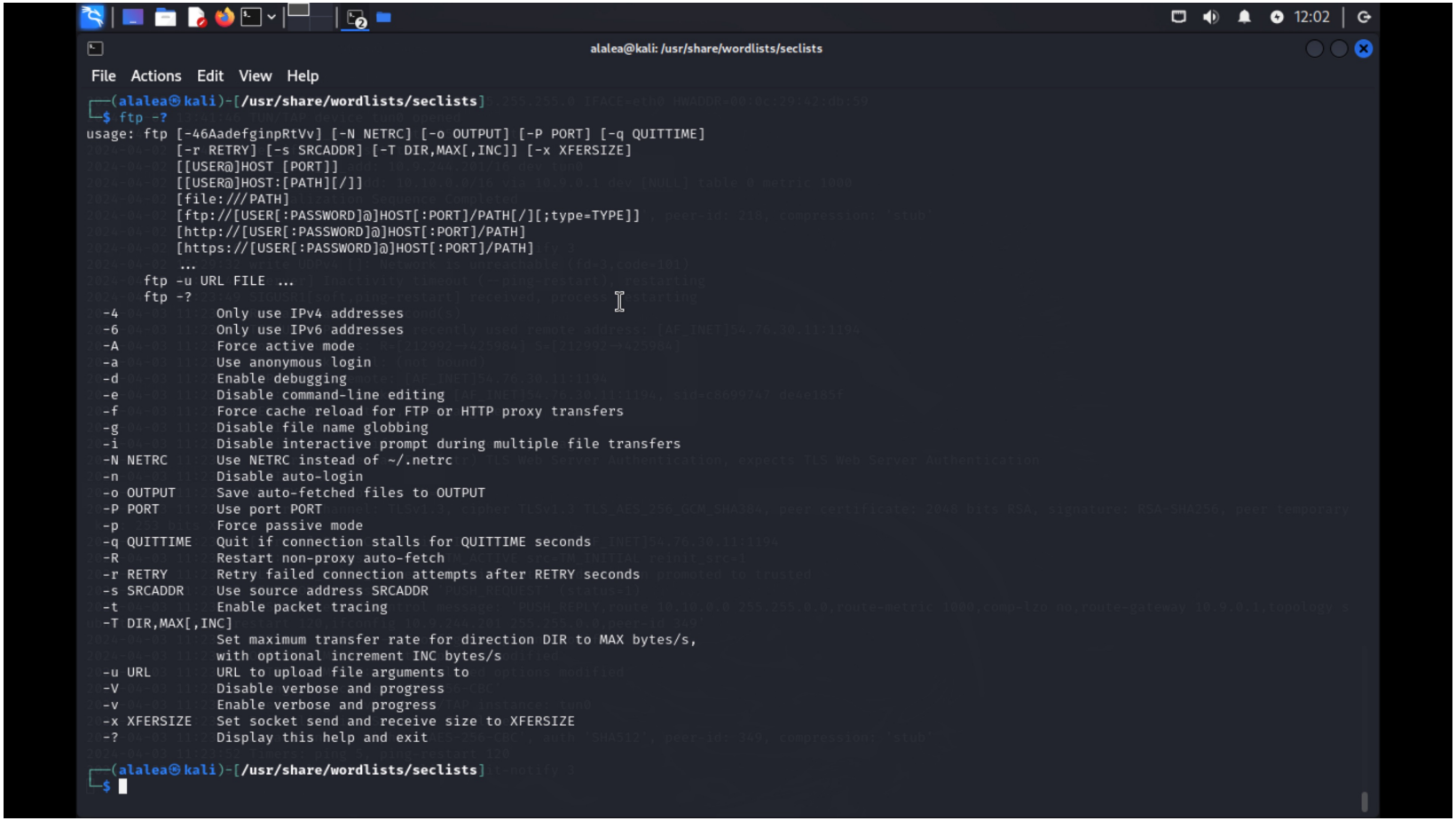
Una tipica sessione FTP funziona utilizzando due canali:

- un canale di comando (talvolta chiamato di controllo)
- un canale dati.

La separazione delle informazioni di comando e dei dati in canali separati è un modo per poter inviare comandi al server senza dover aspettare che il trasferimento di dati in corso finisca. Se i due canali fossero interconnessi, si potrebbero inserire i comandi solo tra un trasferimento di dati e l'altro, il che non sarebbe efficiente né per i trasferimenti di file di grandi dimensioni né per le connessioni Internet lente.

Porta di default: 21

FTP


alalea@kali: /usr/share/wordlists/seclists
File Actions Edit View Help
(alalea㉿kali)-[/usr/share/wordlists/seclists]
$ ftp -?
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
[-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
[[USER@]HOST [PORT]]
[[USER@]HOST:[PATH][/]]
[file:///PATH]
[ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
[http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
[https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
...
ftp -u URL FILE ...
ftp -?
-4 Only use IPv4 addresses
-6 Only use IPv6 addresses
-A Force active mode
-a Use anonymous login
-d Enable debugging
-e Disable command-line editing
-f Force cache reload for FTP or HTTP proxy transfers
-g Disable file name globbing
-i Disable interactive prompt during multiple file transfers
-N NETRC Use NETRC instead of ~/.netrc
-n Disable auto-login
-o OUTPUT Save auto-fetched files to OUTPUT
-P PORT Use port PORT
-p Force passive mode
-q QUITTIME Quit if connection stalls for QUITTIME seconds
-R Restart non-proxy auto-fetch
-r RETRY Retry failed connection attempts after RETRY seconds
-s SRCADDR Use source address SRCADDR
-t Enable packet tracing
-T DIR,MAX[,INC]
Set maximum transfer rate for direction DIR to MAX bytes/s,
with optional increment INC bytes/s
-u URL URL to upload file arguments to
-V Disable verbose and progress
-v Enable verbose and progress
-x XFERSIZE Set socket send and receive size to XFERSIZE
-? Display this help and exit
(alalea㉿kali)-[/usr/share/wordlists/seclists]
$

FTP

Problemi con FTP: login anonimo

Abilita l’accesso ad utenti non autorizzati e senza password

```
┌──(alalea㉿kali)-[~]
└─$ ftp anonymous@10.10.113.20
Connected to 10.10.113.20.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
331 Password required for anonymous
Password:
230 Logged on
```

NFS

NFS è l'acronimo di "Network File System" e consente a un sistema di condividere directory e file con altri su una rete.

Utilizzando NFS, gli utenti e i programmi possono accedere ai file dei sistemi remoti quasi come se fossero file locali. Questo avviene montando tutto o una parte di un file system su un server.

Alla porzione di file system montata possono accedere i client con i privilegi assegnati a ciascun file.

NFS-Common

comandi per interagire con NFS:
lockd, statd, **showmount**, **nfsstat, gssd**, **idmapd** and **mount.nfs**

Installazione:

sudo apt install nfs-common

NFS

Accedere a file su NFS server:

sudo mount -t nfs IP:share /tmp/mount/ -nolock

Tag	Function
sudo	Run as root
mount	Execute the mount command
-t nfs	Type of device to mount, then specifying that it's NFS
IP:share	The IP Address of the NFS server, and the name of the share we wish to mount
-nolock	Specifies not to use NLM locking

NFS

Possibili exploit: privilege escalation

Per impostazione predefinita, sulle condivisioni NFS è abilitato il Root Squashing, che impedisce a chiunque si connetta alla condivisione NFS di avere accesso root al volume NFS. Agli utenti root remoti, al momento della connessione, viene assegnato l'utente "nfsnobody", che ha i privilegi locali minimi. Se questa funzione è disattivata, può permettere a un utente remoto di accedere come root al sistema collegato.

Vulnerability Assessment and Penetration Testing

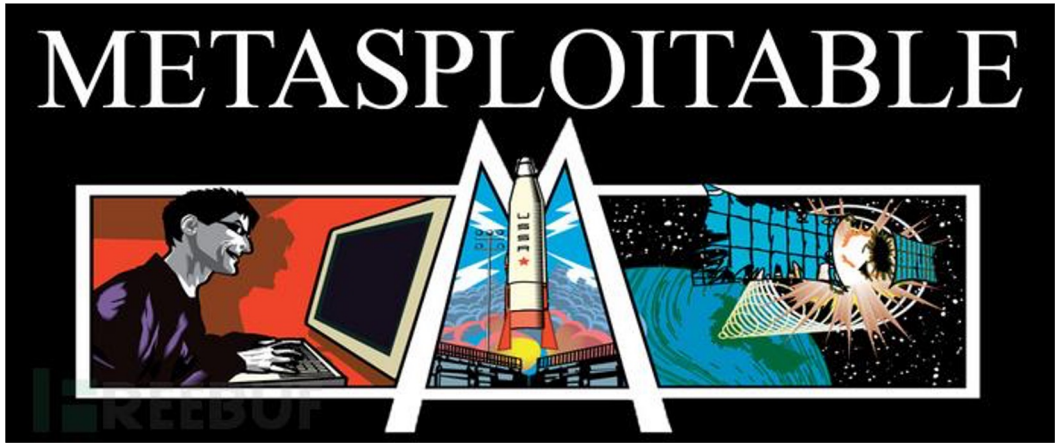
VULNERABILITY SCANNING

Metasploitable

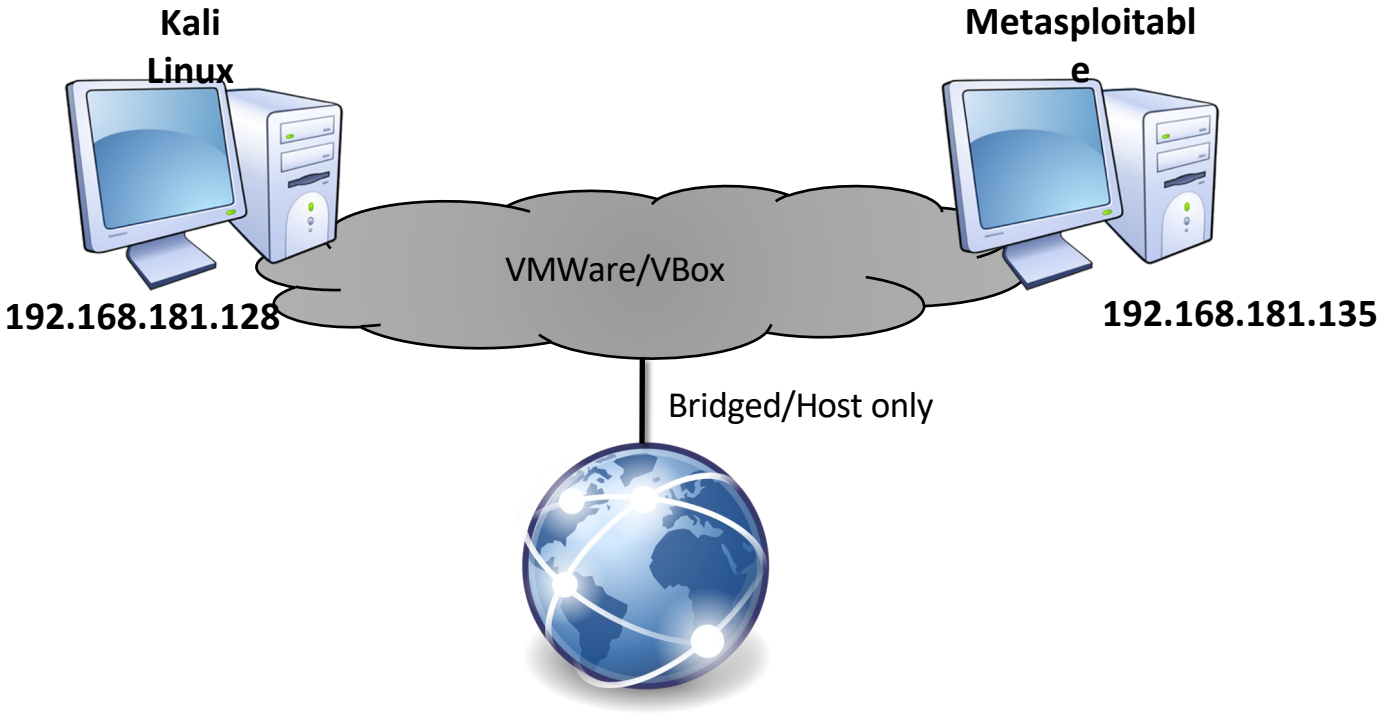
The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common (easy) vulnerabilities.

Download: http://sourceforge.net/projects/metasploitable/files/latest/download

Tutorial: https://community.rapid7.com/docs/DOC-1875



VM Network Topology



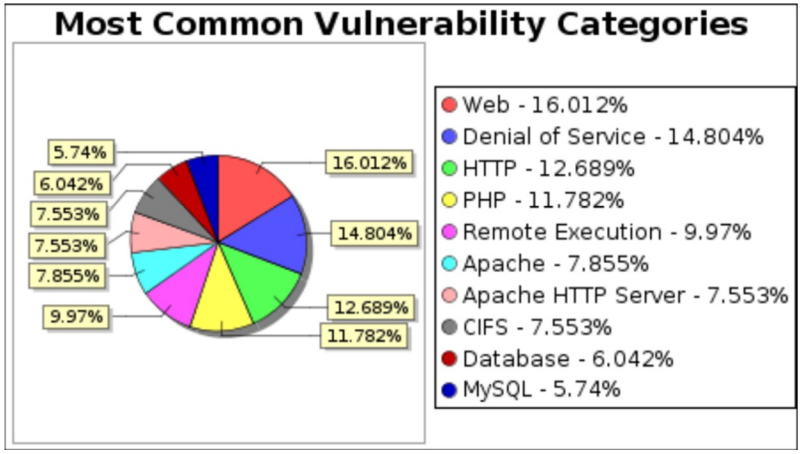
Metasploitable services

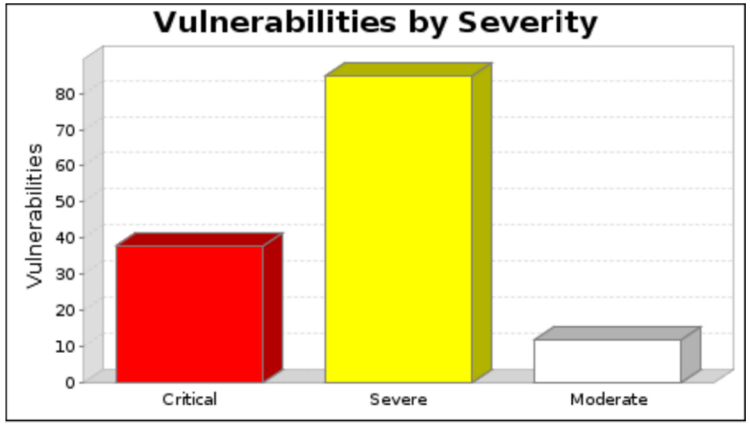
Apache 2.2.8, Tomcat Password , Samba NDR Parsing, Heap Overflow, BIND libbind inet_network(), PHP 5.2.12, 5.2.6, 5.2.8, PHP Fixed security issue, VNC password is "password“, Samba 'reply_netbios_packet' Nmbd Buffer Overflow, cve-2012-1667, HTML Output Script Insertion XXS, Key algorithm rollover bug, DNS service BIND 9.4.2, MySQL 5.0.51a and so on…

About 135 in All

40 are critical vulnerabilities!

Metasploitable services

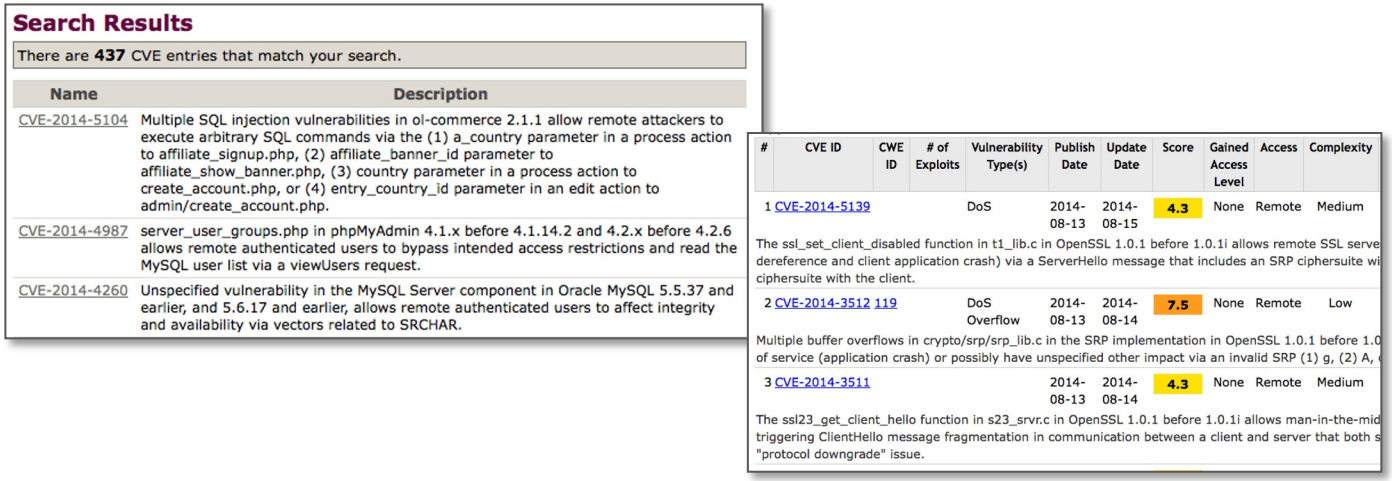




Classification of Vulnerabilities

CVE: Common Vulnerabilities and Exposures

- A structured means to exchange information on security vulnerabilities and exposures and provides a common identifier for publicly-known problems.
- http://cve.mitre.org/



Search Results

There are **437** CVE entries that match your search.

Name	Description
CVE-2014-5104	Multiple SQL injection vulnerabilities in ol-commerce 2.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) a_country parameter in a process action to affiliate_signup.php, (2) affiliate_banner_id parameter to affiliate_show_banner.php, (3) country parameter in a process action to create_account.php, or (4) entry_country_id parameter in an edit action to admin/create_account.php.
CVE-2014-4987	server_user_groups.php in phpMyAdmin 4.1.x before 4.1.14.2 and 4.2.x before 4.2.6 allows remote authenticated users to bypass intended access restrictions and read the MySQL user list via a viewUsers request.
CVE-2014-4260	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier, and 5.6.17 and earlier, allows remote authenticated users to affect integrity and availability via vectors related to SRCHAR.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2014-5139			DoS	2014-08-13	2014-08-15	4.3	None	Remote	Medium
The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL serve dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite wi ciphersuite with the client.										
2	CVE-2014-3512	119		DoS Overflow	2014-08-13	2014-08-14	7.5	None	Remote	Low
Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0 of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A,										
3	CVE-2014-3511				2014-08-13	2014-08-14	4.3	None	Remote	Medium
The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-mid triggering ClientHello message fragmentation in communication between a client and server that both s "protocol downgrade" issue.										

Taxonomy of vulnerabilities

CWE: Common Weakness Enumeration

- Group same kind of vulnerabilities into a weakness, and give it a distinct number
- Provides common names for publicly known problems in the commercial or open source software
- Intended for security tools and services that can find weaknesses in source code and operational systems
- Helps better understand and manage software weaknesses related to architecture and design

- http://cwe.mitre.org/

CWE top

Prioritized list of dangerous software errors

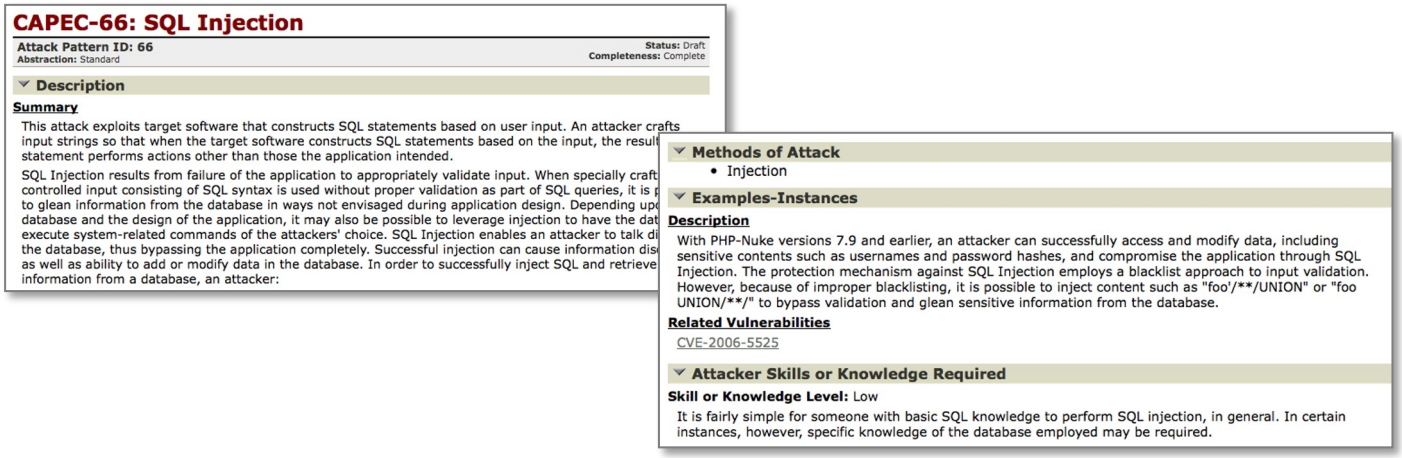
- Intended to minimize software vulnerability and data breach
- Any software for data protection needs serious consideration of these failure modes, among others
- Useful for:
  - Procurement
  - Development, etc.
  - http://cwe.mitre.org/top25/

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command
[3]	79	CWE-120	Buffer Copy without Checking Size of Input
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75	CWE-798	Use of Hard-coded Credentials
[8]	75	CWE-311	Missing Encryption of Sensitive Data
[9]	74	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges

Attack patterns

CAPEC: Common Attack Pattern Enumeration and Classification

- Dictionary of attack patterns, solutions & mitigations
- Facilitates communication of incidents, issues, as well as validation techniques and mitigation strategies
- http://capec.mitre.org/



CAPEC-66: SQL Injection

Attack Pattern ID: 66
Abstraction: Standard
Status: Draft
Completeness: Complete

Description

Summary

This attack exploits target software that constructs SQL statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the result statement performs actions other than those the application intended.

SQL Injection results from failure of the application to appropriately validate input. When specially craft controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is p to glean information from the database in ways not envisaged during application design. Depending up database and the design of the application, it may also be possible to leverage injection to have the dat execute system-related commands of the attackers' choice. SQL Injection enables an attacker to talk di the database, thus bypassing the application completely. Successful injection can cause information dis as well as ability to add or modify data in the database. In order to successfully inject SQL and retrieve information from a database, an attacker:

Methods of Attack

- Injection

Examples-Instances

Description

With PHP-Nuke versions 7.9 and earlier, an attacker can successfully access and modify data, including sensitive contents such as usernames and password hashes, and compromise the application through SQL Injection. The protection mechanism against SQL Injection employs a blacklist approach to input validation. However, because of improper blacklisting, it is possible to inject content such as "foo'/**/UNION" or "foo UNION/**/" to bypass validation and glean sensitive information from the database.

Related Vulnerabilities

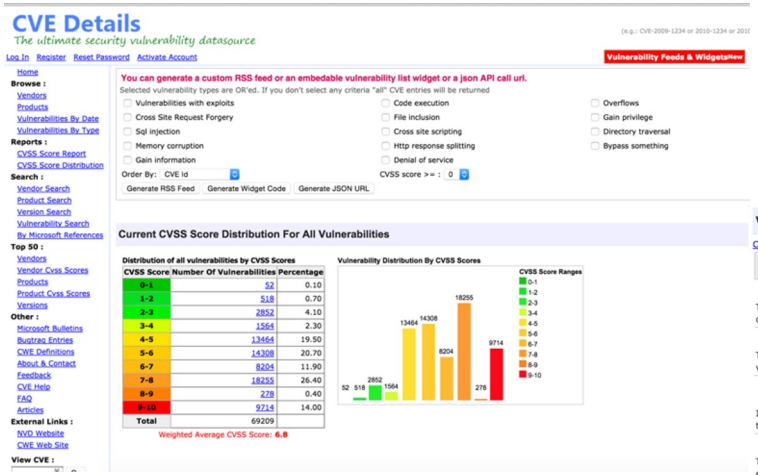
CVE-2006-5525

Attacker Skills or Knowledge Required

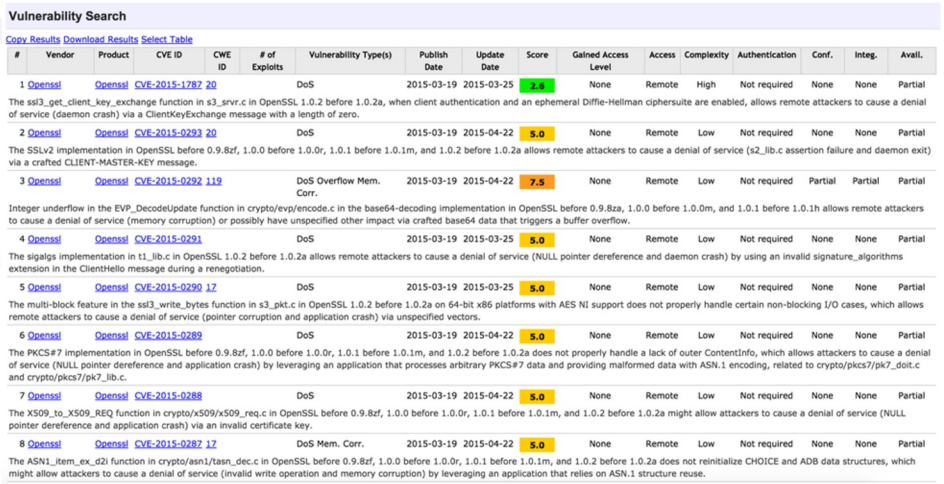
Skill or Knowledge Level: Low

It is fairly simple for someone with basic SQL knowledge to perform SQL injection, in general. In certain instances, however, specific knowledge of the database employed may be required.

Search for vulnerabilities



http://www.cvedetails.com/

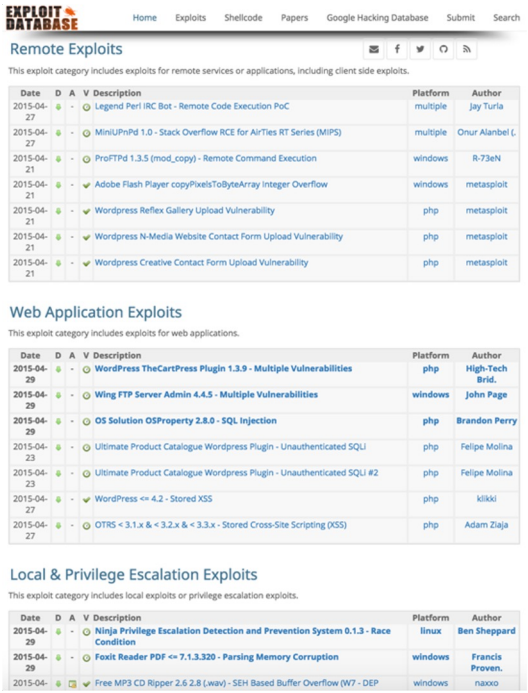


Vulnerability Search

Copy Results Download Results Select Table

#	Vendor	Product	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	Openssl	Openssl	CVE-2015-1787	20		DoS	2015-03-19	2015-03-25	2.6	None	Remote	High	Not required	None	None	Partial
The ssl3_get_client_key_exchange function in s3_srvr.c in OpenSSL 1.0.2 before 1.0.2a, when client authentication and an ephemeral Diffie-Hellman ciphersuite are enabled, allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.																
2	Openssl	Openssl	CVE-2015-0293	20		DoS	2015-03-19	2015-04-22	5.0	None	Remote	Low	Not required	None	None	Partial
The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.																
3	Openssl	Openssl	CVE-2015-0292	119		DoS Overflow Mem. Corr.	2015-03-19	2015-04-22	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.																
4	Openssl	Openssl	CVE-2015-0291			DoS	2015-03-19	2015-03-25	5.0	None	Remote	Low	Not required	None	None	Partial
The sigalgs implementation in t1_lib.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by using an invalid signature_algorithms extension in the ClientHello message during a renegotiation.																
5	Openssl	Openssl	CVE-2015-0290	17		DoS	2015-03-19	2015-03-25	5.0	None	Remote	Low	Not required	None	None	Partial
The multi-block feature in the ssl3_write_bytes function in s3_pkt.c in OpenSSL 1.0.2 before 1.0.2a on 64-bit x86 platforms with AES NI support does not properly handle certain non-blocking I/O cases, which allows remote attackers to cause a denial of service (pointer corruption and application crash) via unspecified vectors.																
6	Openssl	Openssl	CVE-2015-0289			DoS	2015-03-19	2015-04-22	5.0	None	Remote	Low	Not required	None	None	Partial
The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.																
7	Openssl	Openssl	CVE-2015-0288			DoS	2015-03-19	2015-04-22	5.0	None	Remote	Low	Not required	None	None	Partial
The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.																
8	Openssl	Openssl	CVE-2015-0287	17		DoS Mem. Corr.	2015-03-19	2015-04-22	5.0	None	Remote	Low	Not required	None	None	Partial
The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.																

Search for vulnerabilities (and exploits)



EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Remote Exploits

This exploit category includes exploits for remote services or applications, including client side exploits.

Date	D	A	V	Description	Platform	Author
2015-04-27		-		Legend Perl IRC Bot - Remote Code Execution PoC	multiple	Jay Turla
2015-04-27		-		MiniUPnPd 1.0 - Stack Overflow RCE for AirTies RT Series (MIPS)	multiple	Onur Alanbel (.
2015-04-21		-		ProFTPd 1.3.5 (mod_copy) - Remote Command Execution	windows	R-73eN
2015-04-21		-		Adobe Flash Player copyPixelsToByteArray Integer Overflow	windows	metasploit
2015-04-21		-		Wordpress Reflex Gallery Upload Vulnerability	php	metasploit
2015-04-21		-		Wordpress N-Media Website Contact Form Upload Vulnerability	php	metasploit
2015-04-21		-		Wordpress Creative Contact Form Upload Vulnerability	php	metasploit

Web Application Exploits

This exploit category includes exploits for web applications.

Date	D	A	V	Description	Platform	Author
2015-04-29		-		WordPress TheCartPress Plugin 1.3.9 - Multiple Vulnerabilities	php	High-Tech Brid.
2015-04-29		-		Wing FTP Server Admin 4.4.5 - Multiple Vulnerabilities	windows	John Page
2015-04-29		-		OS Solution OSProperty 2.8.0 - SQL Injection	php	Brandon Perry
2015-04-23		-		Ultimate Product Catalogue Wordpress Plugin - Unauthenticated SQLi	php	Felipe Molina
2015-04-23		-		Ultimate Product Catalogue Wordpress Plugin - Unauthenticated SQLi #2	php	Felipe Molina
2015-04-27		-		WordPress <= 4.2 - Stored XSS	php	klikki
2015-04-27		-		OTRS < 3.1.x & < 3.2.x & < 3.3.x - Stored Cross-Site Scripting (XSS)	php	Adam Ziaja

Local & Privilege Escalation Exploits

This exploit category includes local exploits or privilege escalation exploits.

Date	D	A	V	Description	Platform	Author
2015-04-29		-		Ninja Privilege Escalation Detection and Prevention System 0.1.3 - Race Condition	linux	Ben Sheppard
2015-04-29		-		Foxit Reader PDF <= 7.1.3.320 - Parsing Memory Corruption	windows	Francis Proven.
2015-04-				Free MP3 CD Ripper 2.6 2.8 (.wav) - SEH Based Buffer Overflow (W7 - DEP	windows	naxxo

http://www.exploit-db.com/

PoC & Denial of Service Exploits

This exploit category includes proof of concept code or code that results in a denial of service or application crash.

Date	D	A	V	Description	Platform	Author
2015-04-28				i.FTP 2.21 - SEH Overflow Crash PoC	windows	Avinash Thapa
2015-04-23		-		ZYXEL P-660HN-T1H_IPv6 - Remote Configuration Editor / Web Server DoS	hardware	Koorosh Ghorba.
2015-04-21		-		Mac OS X - Local Denial of Service	osx	Maxime Villard
2015-04-17		-		Oracle Hyperion Smart View for Office 11.1.2.3.000 - Crash PoC	windows	sajith
2015-04-17		-		Oracle - Outside-In DOCX File Parsing Memory Corruption	windows	Francis Proven.
2015-04-16		-		MS Windows (HTTP.sys) - HTTP Request Parsing DoS (MS15-034)	windows	laurent gaffie
2015-04-15		-		Microsoft Window - HTTP.sys PoC (MS15-034)	windows	rhcp011235

Exploit Shellcode Archive

This category includes archived shellcode.

Date	D	Description	Platform	Author
2015-04-29		Linux x86 - Execve /bin/sh Shellcode Via Push (21 bytes)	lin_x86	noviceflux
2015-04-29		Linux x86-64 - Execve /bin/sh Shellcode Via Push (23 bytes)	lin_x86-64	noviceflux
2015-04-03		Disable ASLR in Linux (84 bytes)	lin_x86	Mohammad Reza .
2015-04-14		linux/x86 setreuid(0, 0) + execve("/sbin/halt") + exit(0) (49 bytes)	lin_x86-64	Febriyanto Nug.
2015-04-17		Linux/x86 execve "/bin/sh" - shellcode (35 bytes)	lin_x86	Mohammad Reza .
2015-04-17		win32/xp sp3 Create ("file.txt") (83 bytes)	win32	TUNISIAN CYBER
2015-04-17		win32/xp sp3 - Restart computer	win32	TUNISIAN CYBER

Archived Security Papers

Archived security papers in all languages.

Date	D	Description	Author
2015-04-21		Developing MIPS Exploits to Hack Routers	Onur Alanbel (.
2015-04-03		[Hebrew] Digital Whisper Security Magazine #60	cp77fk4r & Und.
2015-03-		PoC || GTFO 0x07	Rt. Revd. Dr.

Search for vulnerabilities (and exploits)

Embedded in Kali Linux:

searchsploit < key1> <key2>

```
root@kali:~# searchsploit proftpd
---------------------------------------------------------------------------------------------------------------------------------------------
 Description                                                                                                                 |  Path
---------------------------------------------------------------------------------------------------------------------------------------------
ProFTPD 1.2.9RC1 (mod_sql) Remote SQL Injection Exploit                                                                      | /linux/remote/43.pl
ProFTPD 1.2.9rc2 ASCII File Remote Root Exploit                                                                              | /linux/remote/107.c
ProFTPD 1.2.7 - 1.2.9rc2 - Remote Root & brute-force Exploit                                                                 | /linux/remote/110.c
ProFTPD 1.2.0 (rc2) - memory leakage example Exploit                                                                         | /linux/dos/241.c
ProFTPD <= 1.2.0pre10 - Remote Denial of Service Exploit                                                                     | /linux/dos/244.java
ProFTPd Local pr_ctrls_connect Vulnerability - ftpdctl                                                                       | /linux/local/394.c
ProFTPD <= 1.2.10 - Remote Users Enumeration Exploit                                                                         | /linux/remote/581.c
ProFTPD 1.3.0 (sreplace) Remote Stack Overflow Exploit (meta)                                                                | /linux/remote/2856.pm
ProFTPD <= 1.3.0a (mod_ctrls support) Local Buffer Overflow PoC                                                              | /linux/dos/2928.py
ProFTPD <= 1.2.9 rc2 (ASCII File) Remote Root Exploit                                                                        | /linux/remote/3021.txt
ProFTPD 1.3.0/1.3.0a (mod_ctrls support) Local Buffer Overflow Exploit                                                       | /linux/local/3330.pl
ProFTPD 1.3.0/1.3.0a (mod_ctrls support) Local Buffer Overflow Exploit 2                                                     | /linux/local/3333.pl
ProFTPD 1.3.0/1.3.0a (mod_ctrls) Local Overflow Exploit (exec-shield)                                                        | /linux/local/3730.txt
ProFTPD 1.x (module mod_tls) Remote Buffer Overflow Exploit                                                                  | /linux/remote/4312.c
ProFTPd with mod_mysql Authentication Bypass Vulnerability                                                                   | /multiple/remote/8037.txt
ProFTPd 1.3.0 mod_ctrls Local Stack Overflow (opensuse)                                                                      | /unix/local/10044.pl
ProFTPD IAC - Remote Root Exploit                                                                                            | /linux/remote/15449.pl
ProFTPD 1.3.3c - Compromised Source Remote Root Trojan                                                                       | /linux/remote/15662.txt
ProFTPD mod_sftp Integer Overflow DoS PoC                                                                                    | /linux/dos/16129.txt
ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)                                                                 | /linux/remote/16851.rb
ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)                                                                         | /linux/remote/16852.rb
ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)                                                               | /linux/remote/16878.rb
ProFTPD-1.3.3c Backdoor Command Execution                                                                                    | /linux/remote/16921.rb
FreeBSD ftpd and ProFTPd on FreeBSD Remote r00t Exploit                                                                      | /freebsd/remote/18181.txt
ProFTPD 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (1)                                                            | /linux/remote/19475.c
ProFTPD 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (2)                                                            | /linux/remote/19476.c
ProFTPD 1.2 pre6 snprintf Vulnerability                                                                                      | /linux/remote/19503.txt
ProFTPD 1.2 SIZE Remote Denial of Service Vulnerability                                                                      | /linux/dos/20536.java
ProFTPD 1.2.x STAT Command Denial of Service Vulnerability                                                                   | /linux/dos/22079.sh
ProFTPD 1.2.7/1.2.8 ASCII File Transfer Buffer Overrun Vulnerability                                                         | /linux/dos/23170.c
ProFTPD 1.3 - 'mod_sql' Username SQL Injection Vulnerability                                                                 | /multiple/remote/32798.pl
---------------------------------------------------------------------------------------------------------------------------------------------
```

OpenVAS

OpenVAS è uno scanner di vulnerabilità completo. Le sue capacità includono test non autenticati e autenticati, vari protocolli internet e industriali di alto e basso livello, regolazione delle prestazioni per scansioni su larga scala e un potente linguaggio di programmazione interno per implementare qualsiasi tipo di test di vulnerabilità.

https://www.openvas.org