Benchmark M3

esercitazione finale modulo 3

Ignazio Saba

INTRODUZIONE

In questo benchmark dovremmo effettuare delle scansioni, tramite Nessus, verso una macchina target “meta” da una macchina attaccante “Kali” passando attraverso un firewall gestito da “pfsense”

fatte le scansioni valutare le vulnerabilità trovate e risolverne alcune

configurazioni

pfsense farà da firewall è configurato con una porta WAN e due LAN
la WAN è lasciata in dhcp in modo di avere libero accesso a internet

LAN kali IP: 192.168.32.1
LAN METASPLOIT IP: 192.168.50.1

kali e meta saranno anch’essi in dhcp ma su lan differenti gestite da PFsense
IP KALI: 192.168.32.10
IP META: 192.168.50.2
tutte le macchine si vedono in rete e hanno accesso a internet

SCANSIONE NESSUS

192.168.50.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
12	9	27	10	92

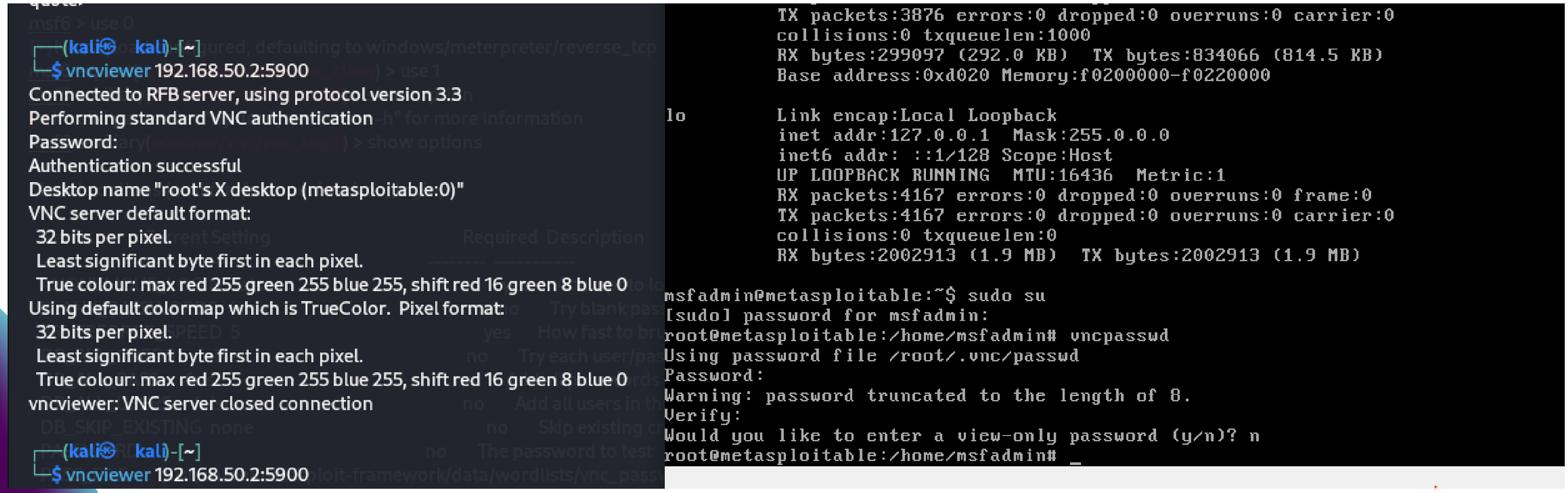
Vulnerabilities Total: 150

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

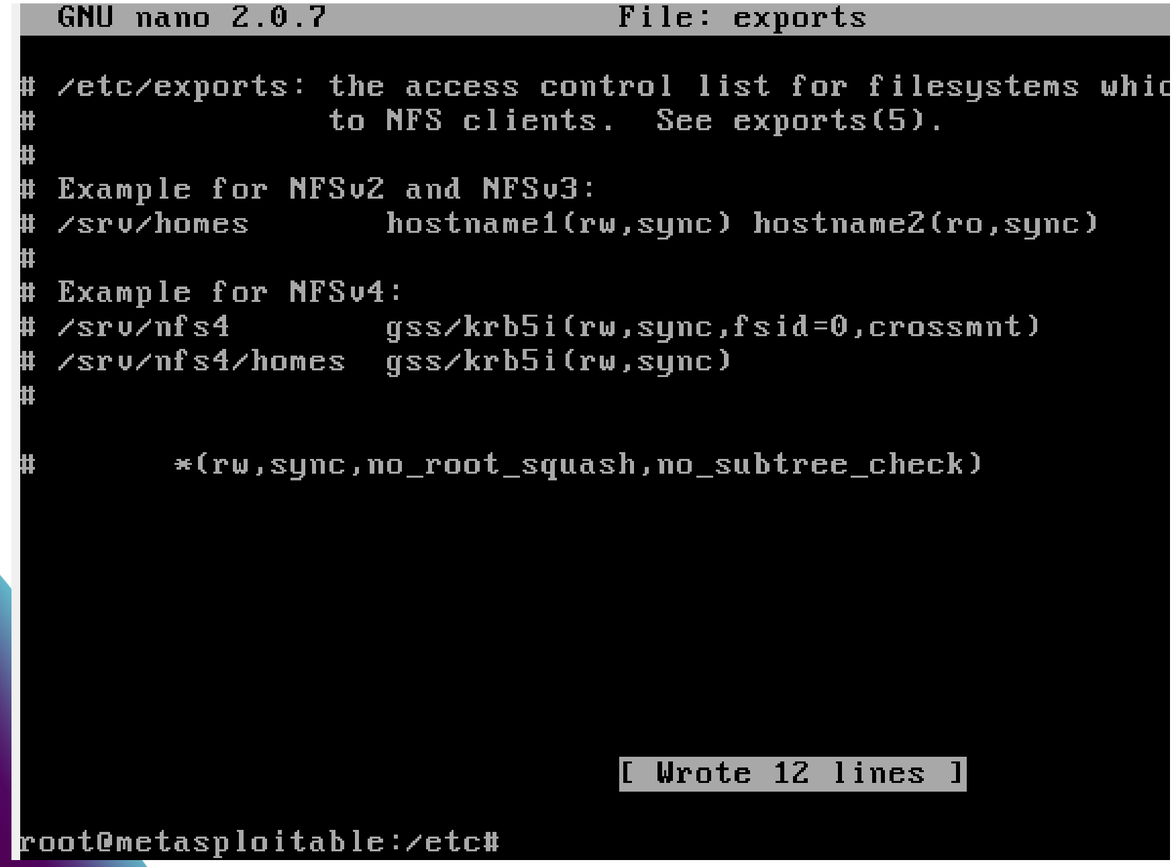
lista compatta delle vulnerabilità trovate

le vulnerabilità riguardanti tomcat sono state risolte con il comando " apt-get install update e apt-get upgrade"
di cui purtroppo non ho screen a causa delle ridotte righe di comando visibili su metasploit

Modifica password VNC

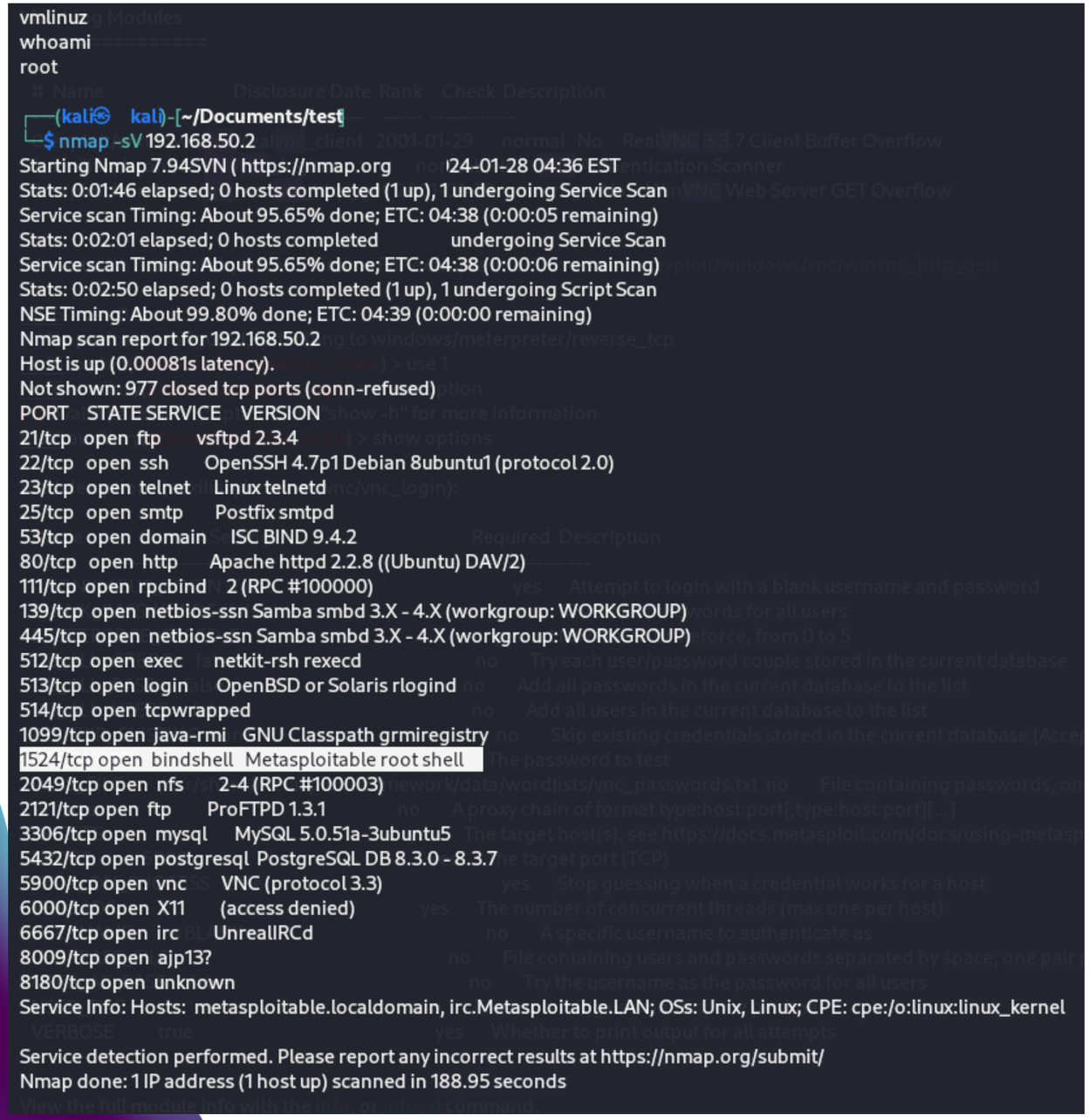


NFS



rinominato il file exports originale e ricreato vuoto

Bind Shell backdoor



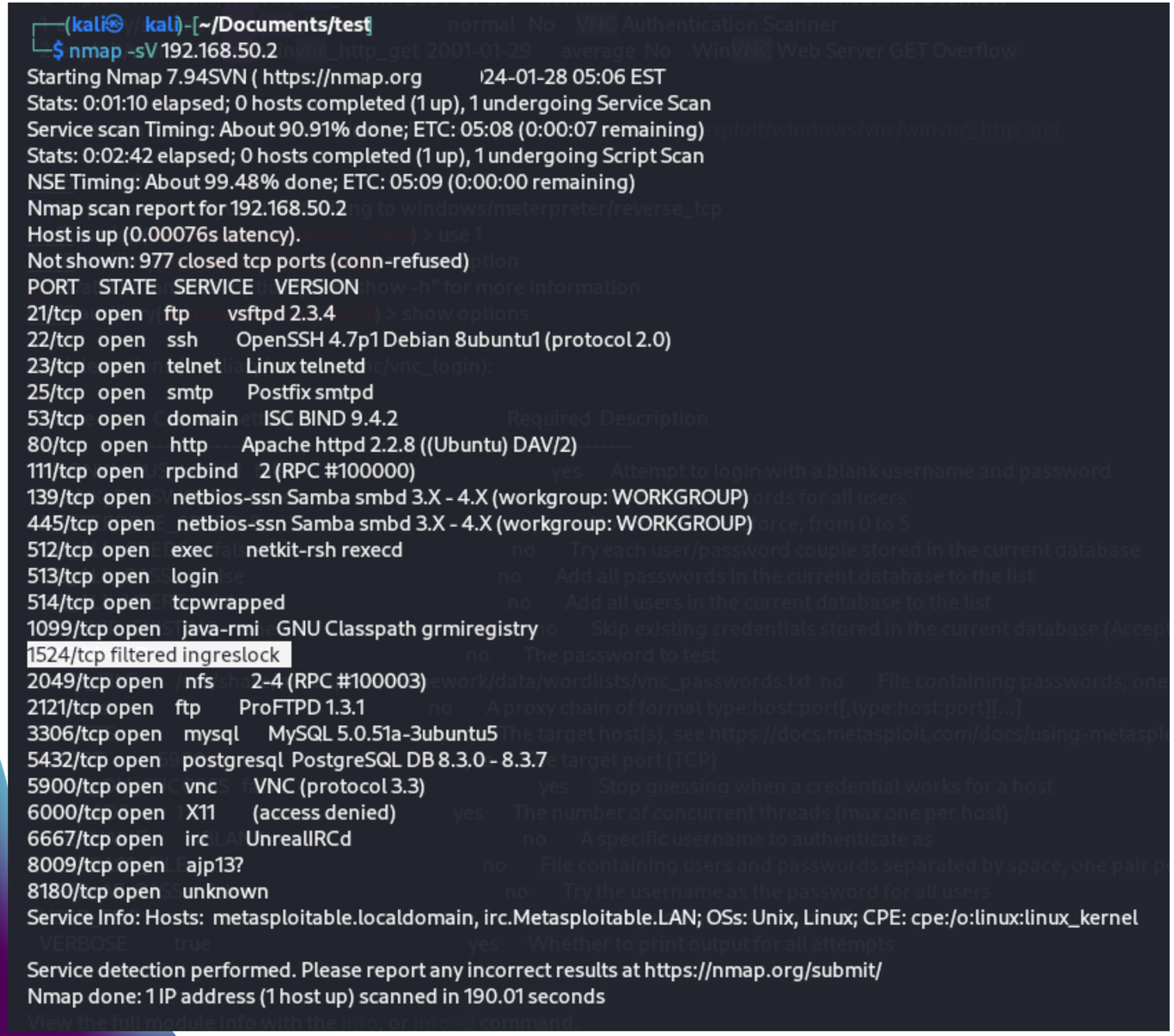
sulla macchina meta veniva esposta una porta la 1524 si procede con iptables a creare una regola che blocca il traffico su quella porta dall’indirizzo di kali

Bind Shell backdoor

```
root@metasploitable:/#
root@metasploitable:/# iptable -L
bash: iptable: command not found
root@metasploitable:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@metasploitable:/# iptables -A INPUT -p tcp -s 192.168.32.10 --dport 1524 -j
 DROP
root@metasploitable:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.32.10        anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@metasploitable:/#
```

creata regola sulle iptables che impedisce all’indirizzo di kali 192.168.32.10 di raggiungere la porta 1524

Bind Shell backdoor



una nuova scansione di nmap mostra come la porta ora sia filtrata

nuova scansione nessus

192.168.50.2

Vulnerabilities Total: 136

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

come s può vedere dalla nuova scansione le vulnerabilità sono diminuite, non solo quelle critiche ma anche quelle di minore importanza sicuramente dipendenti da quelle con un cvss più alto