# Basic Security

**Vulnerability Analysis**

## Nessus scan

### Windows OS

### Metasploitable OS

|  |  |  |  |
| --- | --- | --- | --- |
| CVE | Wat | Probleem | Oplossing |
| CVE-1999-0678 | ServerRoot is de root folder waar documentatie terug te vinden is | Door een configuratie fout kan iedereen van buiten af aan de documentatie | Verwijs de serverroot naar /etc/httpd. Dit is de standaard configuratie. |
| CVE-1999-0618 | rexecd of remote execution service loop op poort 512 en zorgt ervoor dat een gebruiker van op afstand commandos kan sturen naar de OS.  Hiervoor moet de gebruiker zijn username en wachtwoord meegeven. | Het wachtwoord wordt niet geëncrypteerd bij het sturen naar de OS.  De service vertrouwd sommige hosts en IPs blindelings | De rexecd of remote execution service uitzetten en de Firewall configureren zodat TCP over poort 512 niet mogelijk is |
| CVE-1999-0651 | rlogin of remote login is een nuttige software voor linux waarbij een gebruiker over een netwerk kan inloggen op een andere computer | Het wachtwoord wordt niet geëncrypteerd bij het sturen naar de OS.  Mogelijkheid om authenticatie te omzeilen | Verwijder de 'login' lijn in /etc/inetd.conf en herstart het proces  Deactiveer de functie en gebruik SSH |
| CVE-2008-0166 | OpenSSL biedt een versleutelde transportlaag bovenop de normale. | Er wordt een verouderde versie van OpenSSL gebruikt. Deze versie genereerd voorspelbare nummers waardoor het gemakkelijk wordt voor een hacker om dit te "brute forcen". | OpenSSL updaten naar de nieuwste versie. |
| CVE-2010-2075 | UnrealIRCD is een open source IRC server. IRC (Internet Relay Chat) is een application layer protocol in vorm van chat over het internet. | Deze versie bevat een Trojan Horse in het bestand: DEBUG3\_DOLOG\_SYSTEM. Hierdoor kunnen hackers commando's uitvoeren. | UnrealIRCd van de officiele site downloaden en installeren |

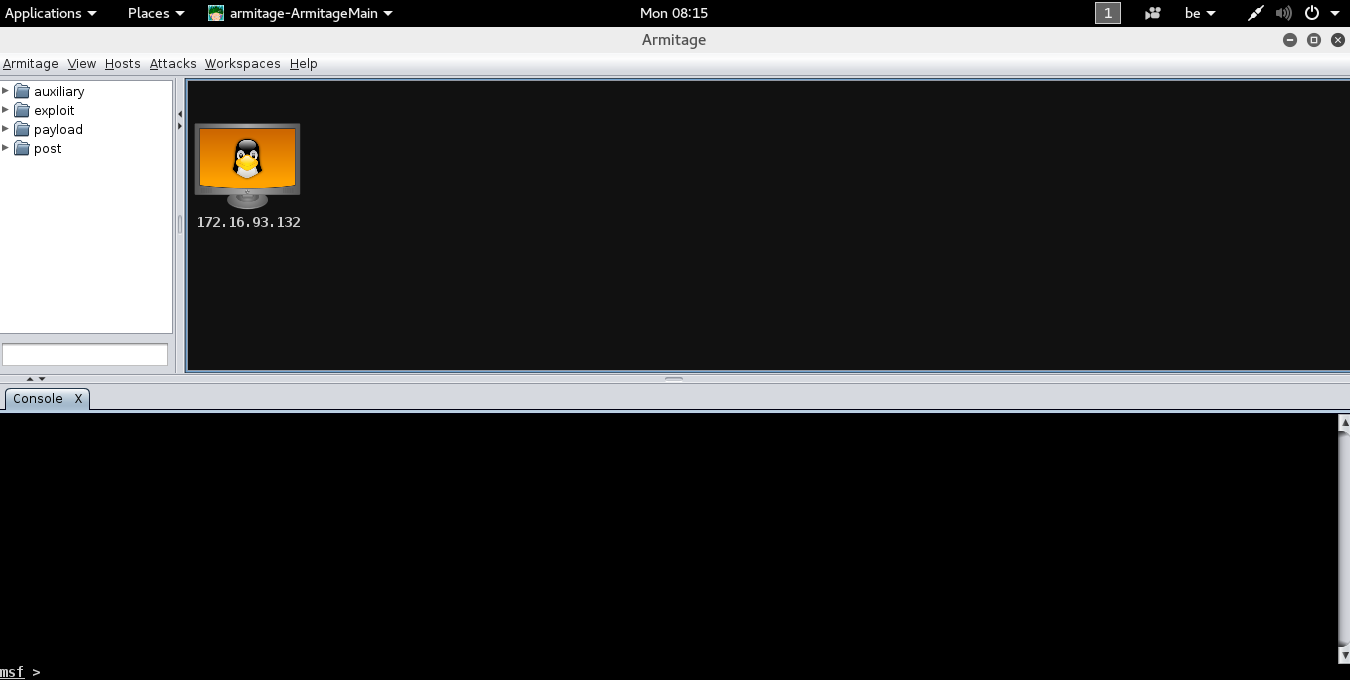
## OpenVAS

## Armitage

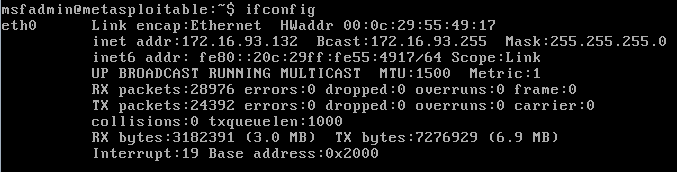
### Hoe Armitage gebruiken

Om te beginnen starten we Kali-Linux op en openen we Armitage. Wanneer er geen verbinding kan gemaakt worden met de database voeren we het volgende commando uit:

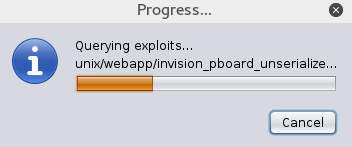
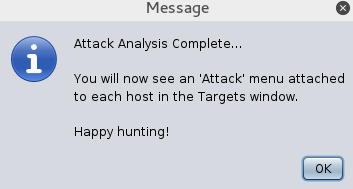
Sudo /etc/init.d/postgresql start



Nadat Armitage is opgestart voegen we een nieuwe host toe. Door op ‘Hosts’ te klikken en daarna ‘Add hosts’. Hier voeren we dan het ip-address van onze ‘target’ in.



Daarna kunnen we ‘Attacks’ zoeken die kunnen worden uitgevoerdt op onze host. Dit doen we door op ‘Attacks’ te klikken en dan op ‘Find attacks’.



Nu kunnen we met rechter muisknop op onze host ‘Attacks’ selecteren en uitvoeren. Wanneer een ‘attack’ gelukt is opent er meestal een nieuwe shell en krijgen we dit te zien.



### Windows OS

### Metasploitable OS

Op de Metasploitable OS hebben we veel ‘attacks’ uitgevoerd. We hebben eerst bij elke categorie een check gedaan welke exploits zouden kunnen werken. Daarna hebben we deze uitgeprobeerd. Uiteraard hebben we niet alles kunnen uitproberen maar dit was ons resultaat.

|  |  |  |
| --- | --- | --- |
| Categorie | Exploitable | Exploit |
| FTP | Exploitable | vsftpd\_234\_backdoor |
| Http | Not Exploitable (niet alles geprobeerd) |  |
| IRC | Exploitable | unreal\_ircd\_3281\_backdoor |
| Misc | Exploitable | java\_rmi\_server |
| Postgress | Not exploitable |  |
| Realserver | Not exploitable (Niet aanwezig) |  |
| Samba | Exploitable | usermap\_script |
| Smtp | Not exploitable |  |
| Ssh | Not exploitable |  |
| Telnet | Not exploitable |  |
| Vnc | Not exploitable |  |
| Webapp | Not exploitable (niet aanwezig) |  |
| Wyse | Not exploitable |  |
| X11 | Not exploitable (niet aanwezig) |  |

Armitage is gemakkelijk en zeer krachtig. Op enkele minuten tijd zat je binnen in het systeem. Uiteraard was Metasploitable OS een gemakkelijk target maar toch waren we verbaasd over hoe snel en gemakkelijk het wel niet was om binnen te geraken.