REPORT

ReverseProxy e Hardening

ITS ICT Security Specialist

rev. 1.0

Gruppo : Michele Buzenchi e Riccardo Bruzzese

**INDICE**

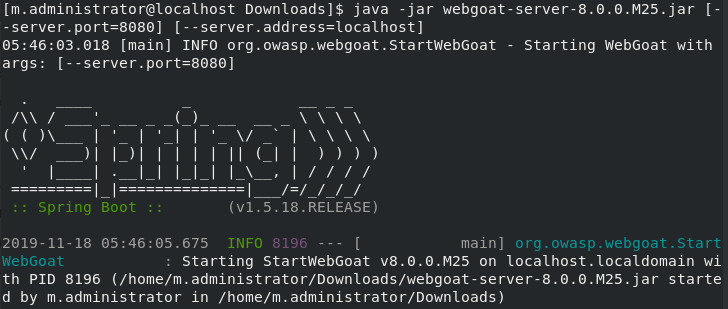
1. Obiettivo del laboratorio 2
2. Installazione di WebGoat 2
3. Installazione del Rerverse Proxy 3
   1. Apertura porte 3
4. Problemi riscontrati 4
5. Soluzione ai problemi 4
6. Hardening 5

1. Obiettivo del laboratorio

L’obiettivo del laboratorio è installare su una macchina isolata il web server WebGoat, un’applicazione insicura per testare le vulnerabilità, e un server proxy su un’altra macchina affinché un utente si connetta attraverso il proxy,dopo la prima fase di configurazione e una fase di remediation vi sarà un’altra fase in cui a gruppi ci si attaccherà a vicenda.

2. Installazione di WebGoat

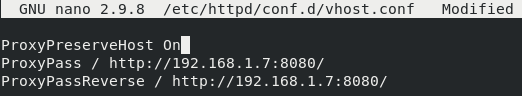
Dopo aver scaricato WebGoat da <https://github.com/WebGoat/WebGoat> e scaricato Java 11, eseguire il comando java -jar webgoat-server-8.0.0.VERSION.jar [--server.port=8080] [--server.address=192.168.1.9] per eseguire l’applicazione sulla porta 8080 e come indirizzo localhost,in questo 192.168.1.9. ( eseguire il comando nella stessa cartella di WebGoat )



3. Installazione del server proxy

Per iniziare dobbiamo eseguire il comando sudo yum install httpd per installare il proxy e dopo dobbiamo andare nel file di configurazione sudo vim /etc/httpd/conf/httpd.conf impostando l’indirizzo della macchina di destinazione ovvero WebGoat.

Oltre ciò inseriamo nel file di configurazione una riga ProxyPreserveHost On affinché neghi al server la comunicazione senza ricevere una richiesta dai vari client.



3.1 Apertura delle porte

Affinché le due macchine ( Proxy e WebGoat ) possano comunicare si devono aprire le porte 8080

firewall-cmd -permanent --add -P=8080/tcp sul WebGoat invece sul proxy 80 infine si riavvia il servizio firewall-cmd --reload.

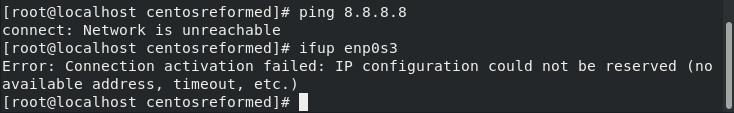
4. Problemi riscontrati

Il problema principale era proprio la difficoltà di far funzionare correttamente il Reverse Proxy affinché riuscisse ad indirizzare correttamente l’indirizzo assegnato.

Nonostante avessimo configurato correttamente il certificato SSL il client non riusciva ad autenticarsi al server e questo era un altro dei problemi riscontrati.

Avevamo anche mal configurato gli indirizzi nel file del Reverse proxy come ProxyPass e ProxyPassReverse.

Le macchine CentOS avevano problemi di comunicazione tra loro a causa di una mal configurazione dei network adapter ( questo ci ha fatto sprecare un po’ di tempo ) e avevamo problemi anche nel ottenere dal DHCP l’indirizzo ip visto che la macchina cui ospitava il WebGoat non lo otteneva correttamente.



5. Soluzioni ai problemi

Per risolvere al problema principale è bastato cambiare l’hostname nel file del Virtual Host e anche gli indirizzi del ProxyPass - ProxyPassReverse.

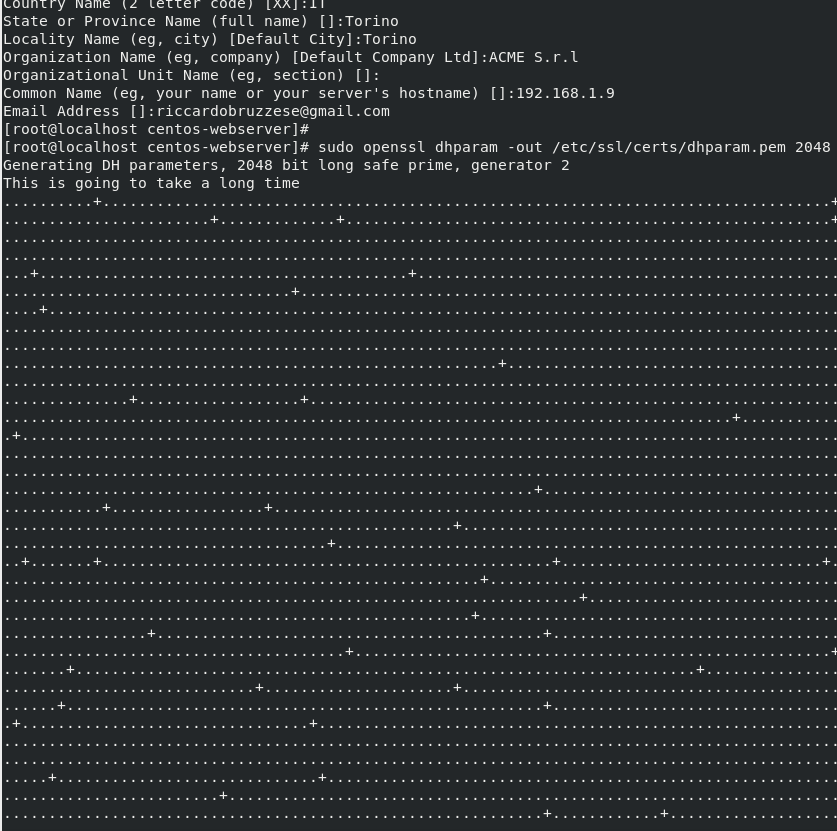
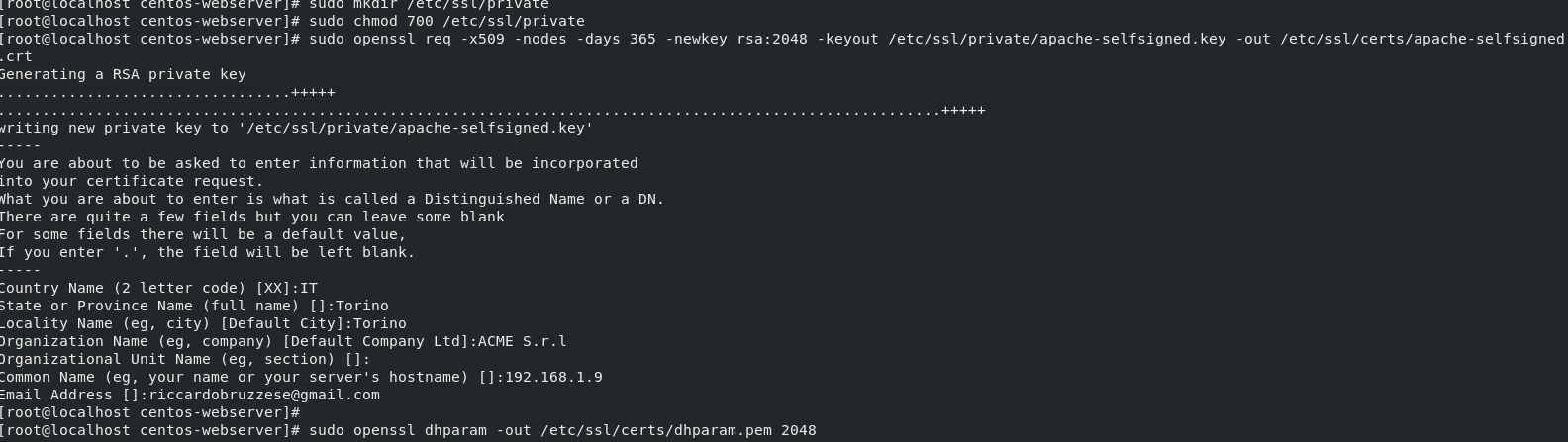
Abbiamo avuto dei problemi per quanto riguarda la configurazione de

Abbiamo rigenerato il certificato SSL e mancava un listen sulla porta 443 per risolvere il problema della mancanza di autenticazione con il certificato.

Per risolvere il problema dei network adapter li abbiamo cambiati da schede in bridge in schede in rete interna, dopo aver riattivato la scheda di rete ( ifup ) abbiamo ottenuto gli indirizzi correttamente ( dhclient ) e così le macchine riuscivano a comunicare tra di loro.

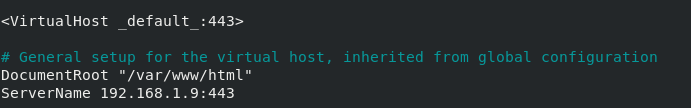
6. Hardening

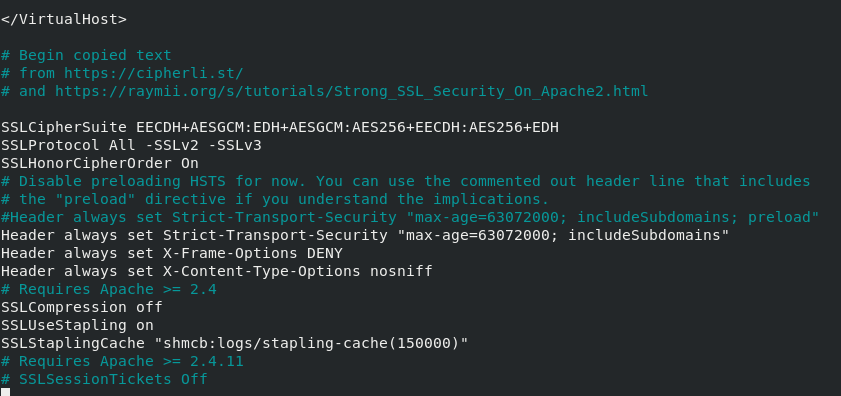
Il primo passo dell’hardening è stato generare un certificato ssl per autenticarsi alla CA.

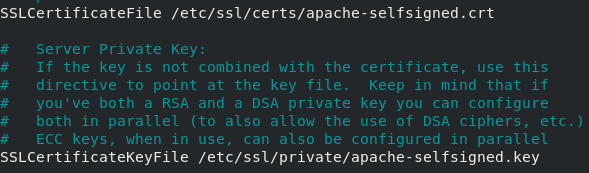


Qua abbiamo re-indirizzato il virtual host sulla porta 443 e successivamente abbiamo modificato il file httpd con l’integrazione dei certificati ssl.

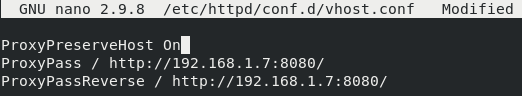
Redirect:





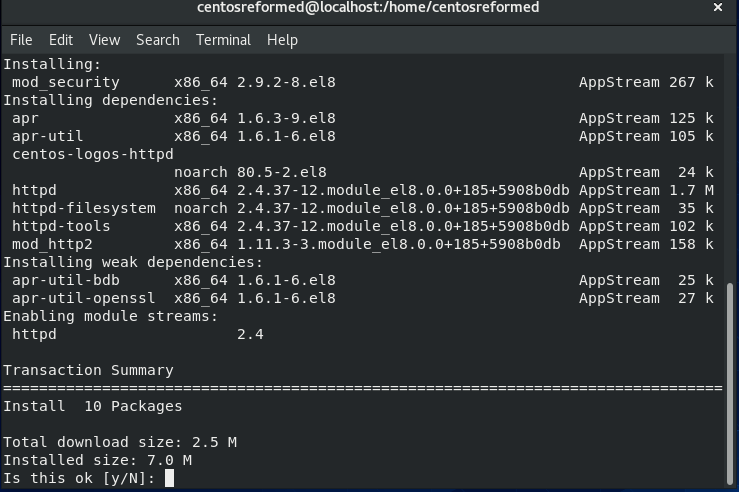


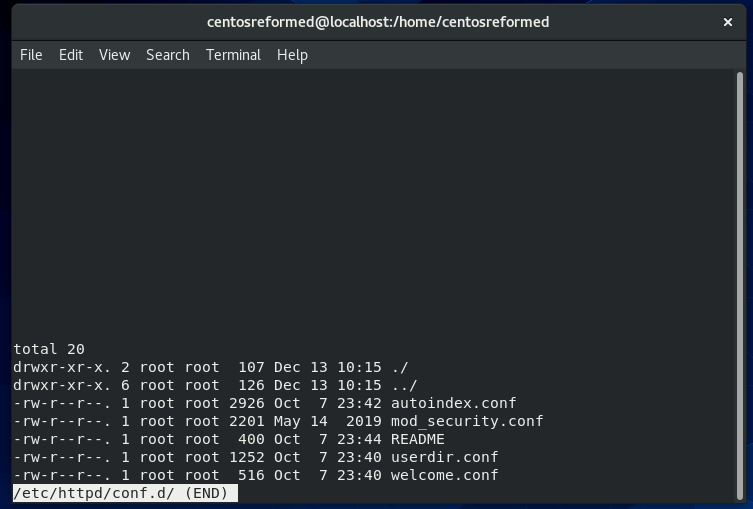
Con la prima riga ci permette di disabilitare dal server la possibilità di far chiamate ai client e così svolgere puramente il lavoro da server ovvero di essere passivo, così non potrà veicolare le macchine nel caso in cui un hacker riesca a penetrare nella macchina.



**Integrazione Mod\_security:**

Abbiamo installato il mod\_security yum install mod\_security e poi riavviato il servzio /etc/init.d/httpd





"Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/vaivgr/trarengr"