ტესტი 10 ღია 4 | 4დან - 1ცალი 6 ქულიანი და 3ცალი 3 ქულიანი

ტესტები

--- CIA
მაგალითად
ვინმეს ფაილის გაგზავნა უნდოდა და რა დაირღვა - მთლიანობა

1. კონფიდენციალურობა: ინფორმაციის დაცვა არავტორიზირებული წვდომისგან,
2. მთლიანობა: არ შეიცვალოს მონაცემები არავტორიზირებული მხარის მხირდან,
3. ხელმისაწვდომობა: ინფორმაციაზე წვდომა ნობისმიერ დროს ავტორიზირებული მომხმარებლისთვის.

ჰაკერების ფერები - შავი, ნაცრისფერი, თერთი

--- 2 კითხვა IP-ზე
აიპების ისა იქნება და რომელი არ იქნება ფაბლიქი
ფრაივათ ადრესები უნდა გავიმეოროთ ასევე

127-ით დაწყებული ყველა ფრაივათია
10-ით დაწყბეული ყველა ფრაივათია
172.16.0.0 - 172.31.255.254 - რეინჯი ფრაივათია
192.168. - ზე რაც იწყება ყველა ფრაივათია
169.254 - ფრაივათია მაგრამ არ შეგვხვედბა ეს ტესტში

--- მომდევნო 2 კითხვა იქნება სერვისებზე

ენუმერაცია
რომელი ხელსაწყოთი შევიძლია ენუმერაციის გაკეთება - სწორი პასუხი იქნება ან NMAP ან METASPOIT

--- პორტებზე

რომელ პორტზე მუშაობს HTTPS, DNS, FTP, და კიდე სხვა პროტოკოლები

- HTTP - 80
- HTTPS - 443

- FTP - 21
- SSH - 22
- SMTP - 25
- POP3 - 110
- IMAP - 143
- DNS - 53
- SNMP - 161
- Telnet - 23
- RDP - 3389
- NTP - 123
- SFTP - 22
- LDAP - 389
- LDAPS - 636
- MySQL Database - 3306
- PostgreSQL Database - 5432
- Redis Database - 6379
- MongoDB Database - 27017
- HTTPS (Alternative) - 8443

3 ქულიანი

--- NMAP -ის ბრძანებები

დაწერეთ NMAP სკრიპტი რომ დავსკანოთ რაიმე პორზე რაიმე აიპი გვექნება რას უნდა ითვალისიწნებდეს ეს ბრძანება.

გააკეთეთ სკანირება 20-დან 25-მდე პორტამდე გავიგოთ სერვისების ვერსია
nmap p 20-25 -sV 192.168.0.2

-p <port ranges>: Only scan specified ports
-sV Probe open ports to determine service/version info
-O Enable OS detection
-T<0-5> Set timing template (higher is faster)
-sn Ping Scan - disable port scan
-Pn პინგლეს სკანირება, Treat all hosts as online -- skip host discovery
-sU UDP scan

--- 2 კითხვა მეტა სპლოიტის კონფიგურაცია
გვექნება მოცემული მოდულის სახელი და გვექნება მოცემული რომელი პარამეტრები უნდა შევცვალოთ

- ჯერ შევდივართ მეტასპოლიტში
msfconsole

- მოდულის დასასერჩად ssh და ენუმერაციის
search ssh enum

- შემდეგ შევდივართ მოდულში. მოდულში შესასვლელად
use შეგვიძლია მივუთითოთ path რომელიც გვექნება მოცემული
ან
use 4 დასერჩვის შემდეგ აიდი რაც აქვს

- რის დაკონფიგურირებასაც ვცდილობთ ეგგ რომ გამოვაჩინოთ
options

- ფილდების დასეტვა (დაკომფიგურირება) მაგალითად
  rhost-ში უნდა დავსეტოთ აიპი
set rhost 10.10.10.10

set threads 10

set user_file /user/share/wordlist/metasploit/unix_user.txt || path გვექნება მოცემული

ბოლოს options გავუშვებთ და გამოგვიტანს კონფიგურაციის ლისტს და სქრინს ჩავუგდებთ

6 ქულიანი

--- უნდა გამოვიყენთ john
მოცემული ქინება ჰეში md5 . ჰეშის ფორმატიც მოცემული იქნება.
მუშაობის პრინციპები:
1 მეთოდი - გადავცემთ ჰეშს და ვეუბნებით რომელი ფორმატის და ალგორითმის ჰეშია და გადავცემთ ვორდლისტს
ჯონი აიღებს ამ სიტყვებს დაჰეშავს და შმდეგ შეადარებს თავის დაჰეშილს და ჩვენს მიცემულ ჰეშს თუ დამეთვხვა ესეიგი ამ ჰეშის უკან გას ეს სიტყვა.

2 მეთოდი - თუ ვორდლისტს არ გადავცემთ მაშინ თვითონ აიღებს ასოს დაჰეშავს და ისევ იგივე პრიციპით შეადრებს

row-MD5 იქნება დაჰეშილი გამოცდაზე

ჰეში უნდა ჩავწეროთ ჯერ ფაილში / შევქმნით ფაილში და შემეგ ჩავაფეისთებთ შიგნით დაჰეშილ სიტყვას
ფაილს თუ დესკტოპზე შევქმნით მაშინ ჯერ დესკტოპზე უნდა გადავიდეთ cd Desktop

ფაილი შეგვძილია შევქმანთ Home ფოლდერში და აღარ დაგვჭირდება დესკტოპზე გადასვლა

--- ქომანდი
john -- format=Row-MD5 password --wordlist=/usr/share/wordlist/metasploit/password.lst

-- format=Row-MD5 - ალგორითმი
password -ფაილის სახელი| თუ არ გადავალთ თავიდანვე დეკსტოპზე მაშინ იქნება ფაილის სახელი Desktop/password
--wordlist=/usr/share/wordlist/metasploit/password.lst - ვორდლისტი