

الtechniques المستخدمة	الهدف	الخطوة	
الهندسة الاجتماعية، كسر كلمة المرور	الهدف هو تحطيم نظام الحماية وكسر كلمة المرور للدخول على النظام	الدخول على الجهاز	1
معرفة الثغرات في النظام	الهدف السببي على صلاحيات مستخدم عادي أو مدير	التحكم من الصلاحيات	2
Trojan Horse, Spyware, Keyloggers, Backdoor	الهدف المطلوب على الدخول في النظام بعد والبقاء داخل الجهاز	التحكم في النظام	3
Rootkits	الهدف (فكاء) تشغيل البرمجيات الخبيثة وبيانات المسروقة بواسطة المخترق	إفشاء الملفات	4
Clear the logs	الهدف إخفاء ومسح أي دليل أو أثر للخنزير	إغلاق الأثر	5

www.CHC-course.com

13

#CHC\_Course

## OWASP Top 10




OWASP Top 10 - 2013

A1 – Injection	→ A1-2017 Injection
A2 – Broken Authentication and Session Management	→ A2-2017 Broken Authentication
A3 – Cross-Site Scripting (XSS)	→ A3-2017-Sensitive Data Exposure
A4 – Insecure Direct Object References (Hardcoded)	→ A4-2017 XML External Entities (XXE) [INFO]
A5 – Security Misconfiguration	→ A5-2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	→ A6-2017 Security Misconfiguration
A7 – Missing Function Level Access Control (Hardcoded)	→ A7-2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	→ A8-2017 Insecure Deserialization [INFO, CONVENTION]
A9 – Using Components with Known Vulnerabilities	→ A9-2017 Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	→ A10-2017 Insufficient Logging/Monitoring [INFO, CONVENTION]

https://www.owasp.org/images/7/72/OWASP\_Top\_10-2017\_%28en%29.pdf.pdf

www.CHC-course.com

15

#CHC\_Course

## أنواع Password Cracking



## Rule-based Attack



يستخدم هذا الهجوم عندما يحصل المهاجم على بعض المعلومات حول كلمة المرور

## Brute Forcing Attack



هو برنامج يحاول تجربة مجموعة مختلفة من الأحرف حتى يتم كسر كلمة المرور

## Dictionary Attack



يتم دفع ملف في تطبيق كسر كلمات المرور الذي يتم كسر كلمات المستخدمين ضد حسابات المستخدمين

www.CHC-course.com

17

#CHC\_Course

## Malicious Software Malware



www.CHC-course.com

23

#CHC\_Course

### كلمات المرور الافتراضية

أدوات لبحث عن كلمات المرور الافتراضية

<a href="https://default-password.info/">https://default-password.info/</a>
<a href="http://www.passwordsdatabase.com">http://www.passwordsdatabase.com</a>
<a href="https://cirt.net/passwords">https://cirt.net/passwords</a>
<a href="https://w3dt.net/">https://w3dt.net/</a>
<a href="http://www.routerpasswords.com/">http://www.routerpasswords.com/</a>
<a href="https://www.fortypoundhead.com/tools_default.asp">https://www.fortypoundhead.com/tools_default.asp</a>

https://default-password.info/



- <https://default-password.info/>
- <http://www.passwordsdatabase.com>
- <https://cirt.net/passwords>
- <https://w3dt.net/>
- <http://www.routerpasswords.com/>
- [https://www.fortypoundhead.com/tools\\_default.asp](https://www.fortypoundhead.com/tools_default.asp)

#CHC\_Course

\* Quasar App  
for hacking  
system

## Rainbow Table - الدخول على الجهاز



سهل استعادة كلمة المرور بالمقارنة بين هاشات كلمة المرور و precomputed table



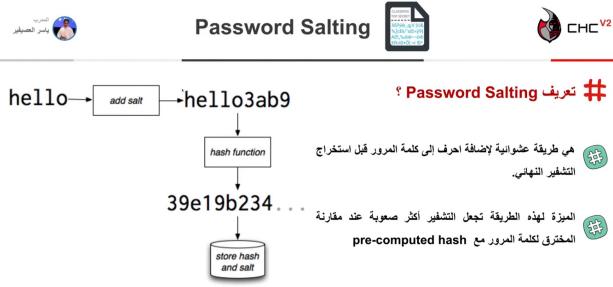
مقارنة الـ Hash لكلمة المرور و مقارنتها مع جدول الهاشات precomputed table

- هي طريقة لفترة الكلمات مثل جدول directory files and Brute force list and ( their hash values )



\* in windows, The file Sam is where passwords stored.

pwdump.exe is a program to get passwords from the system



و اضغط على باسورد الم 🔑 حتى ينبع . admin . بناءً على



The screenshot shows the 'Active@ Password Changer' software interface. It displays a list of users with their names, accounts, descriptions, and status. The first user listed is 'Administrator'. Below the list is a message: 'Select a User Account and press the "Next" button.' At the bottom of the window are buttons for 'Back', 'Next', 'Cancel', and 'Help'. To the left of the software window is a large graphic of a golden keyhole with a silhouette of a person standing in front of it, holding a key. The background of the slide features a red banner at the top with the text 'أداة الصالحيات' (Active@) and 'Active@ Password Changer' in white. On the right side, there are two small icons: a black cat-like figure with the text 'CNC V2' and a red skull with the text 'برمجة CNC'.



\* for decrypt our SAM.  
> john /root/sam --users=...  
-format=NT

john /root/sam --users=...  
-format=NT



```
root@kali:~#
File Edit View Search Terminal Help
root@kali:~# get SAM File
root@kali:~# fdisk -l
Disk /dev/sda: 1.01 GiB, 96737427456 bytes, 188940288 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xfa6be5f

Device     Boot   Start     End   Sectors  Size Id Type
/dev/sda1  *      20648    206847   204800  100G  7 HPFS/NTFS/exFAT
/dev/sda2          206848 188938239 188731392   96G  7 HPFS/NTFS/exFAT

Disk /dev/loop0: 3 GiB, 3148537856 bytes, 6149488 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@kali:~# mount -t ntfs /dev/sda2 /mnt
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
root@kali:~#
```

\* for protection user Bitblocker to encrypt your disk.

## Web Hacking :

**مخاطر برمج الويب**

### Unvalidated Input

**Input validation**

هو إدخال المستخدم بيانات غير صحيحة قبل استمرارية الدخول على الويب و الخواص.

المخترق يتبع ثغرة المدخلات الغير صلحة للاستخدام سرقة Scripting, Buffer overflow, injection attacks ببيانات وتحطيم النظام.

**مخاطر برمج الويب**

### Parameter/Form manipulation

مُعنَّى التلاعب في التسازج والمدخلات

التلاعب في البيانات parameters المنشطة بين المستخدم والخادم لفرض تحويل بيانات البرنامج مثل الصالحيات و بيانات الدخول والأسعار و عدد المنتجات

النلاع في Parameters هي ثغرة خطيرة موجودة في هيئة XSS, SQL Injection, etc

**مخاطر برمج الويب**

### File Injection Attack

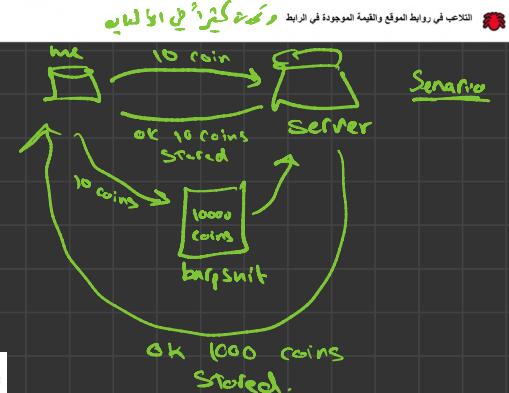
**تعريف File Injection Attack**

يمكن للمخترق أن يكتب ثغرة في الخادم يستخدم الملف عن بعد بدلاً من تثبيت ملف في المتصفح.

المخترق يحقن ملف الاستئناف لتحميل الثغرة

الخطوات:

- Validation
- From the server
- Attack
- Exploit



**مخاطر برمج الويب**

### XSS

كيف يعمل XSS?

Perpetrator injects the website with a malicious script that steals each visitor's session cookies.

For each visit to the website, the malicious script is activated.

User sends cookie to Server.

Hacker intercepts cookie and sends it to Server.

**كيفية الحماية ضد هجمات الويب**

**SQL injection**

**Error Based SQL Injection**

**Blind SQL Injection**

- End of Line Comment
- Tautology
- System Stored Procedure
- UNION SQL Injection
- Boolean Exploitation
- Time Delay

