Kali-Linux presentation 04/16/15

Aircrack-ng http://www.aircrack-ng.org/ made by tdotreppe@aircrack-ng.org

There are several tools in the Aircrack-ng toolset:

Aireplay-ng – it can generate or accelerate traffic on the Access point, potentiall run WEP and WPA2 password attacks as well as ARP injection.

Airdecap-ng – decrypt wireless traffic once the key is cracked

Airtun-ng – virtual tunnel interface creator

Airolib-ng – stores or manages ESSIDs to help crack the password cracking.

Airbase-ng can make the laptop/computer into an Access point.

Burpsuite http://portswigger.net/burp/ made by Portswigger Java application

The Burp suite spider is a tool that can enumerate and map out the various pages and parameters of a web site. For this, the spider examines cookies and initiates connections with these web applications.

- Intercept and modify all HTTP/S traffic passing in both directions.
- Easily analyze all kinds of content, with automatic colorizing of request and response syntax, rendering of web content, and parsing of serialization schemes like AMF.
- Apply fine-grained rules to determine which requests and responses are intercepted for manual testing.
- View all traffic in the detailed Proxy history, with advanced filters and search functions.
- Send interesting items to other Burp Suite tools with a single click.
- Save all of your work, and resume working later.
- Quickly search and highlight interesting content within HTTP messages.
- Work with custom SSL certificates and non-proxy-aware clients.
- Define rules to automatically modify requests and responses without manual intervention.

Hydra https://www.thc.org/ written by van Hauser/THC & maintained by **David Maciejak's** **david.maciejak@gmail.com**

John the Ripper written by Solar Designer solar@openwall.com http://www.openwall.com/john/

a tool to find weak passwords of your users

Maltego made by Paterva, open source intelligence http://www.paterva.com/

Maltego takes various bits of information (referred to as Entities within the application), and converts these (via code known as transforms) to other Entities. An example of this

would be if you were to put a website Entity on a graph within Maltego with the value of 'www.paterva.com' and run the 'To IP Address [DNS]' transform.
You would then notice that a new Entity, namely an IP Address with the value of 74.207.243.85 has been generated as a child of the original website Entity.

Metasploit framework by http://www.metasploit.com/

Msfconsole is where it is at:

The msfconsole is probably the most popular interface to the MSF. It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the Metasploit Framework.

Nmap ("Network Mapper") http://nmap.org/

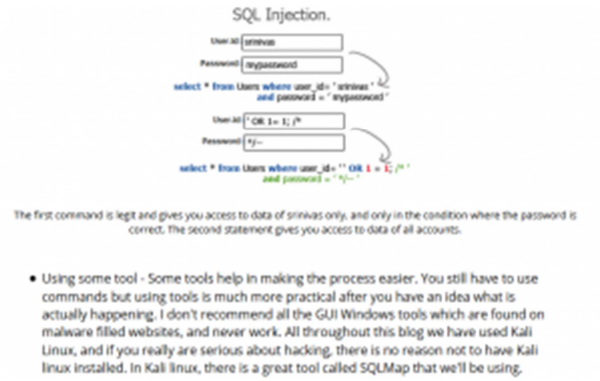
Nmap 6.47 is available -

Owasp-zap OWASP Zed Attack Proxy (ZAP)

penetration testing tool for finding vulnerabilities in web applications.

Sqlmap

http://www.kalitutorials.net/2014/03/sql-injection-how-it-works.html



Notice the bottom entryuser-id field: ' OR 1= 1; /*

and in password field: */–

Wireshark Originally named Ethereal in May 2006 due to trademark issues.

graphical tcpdump