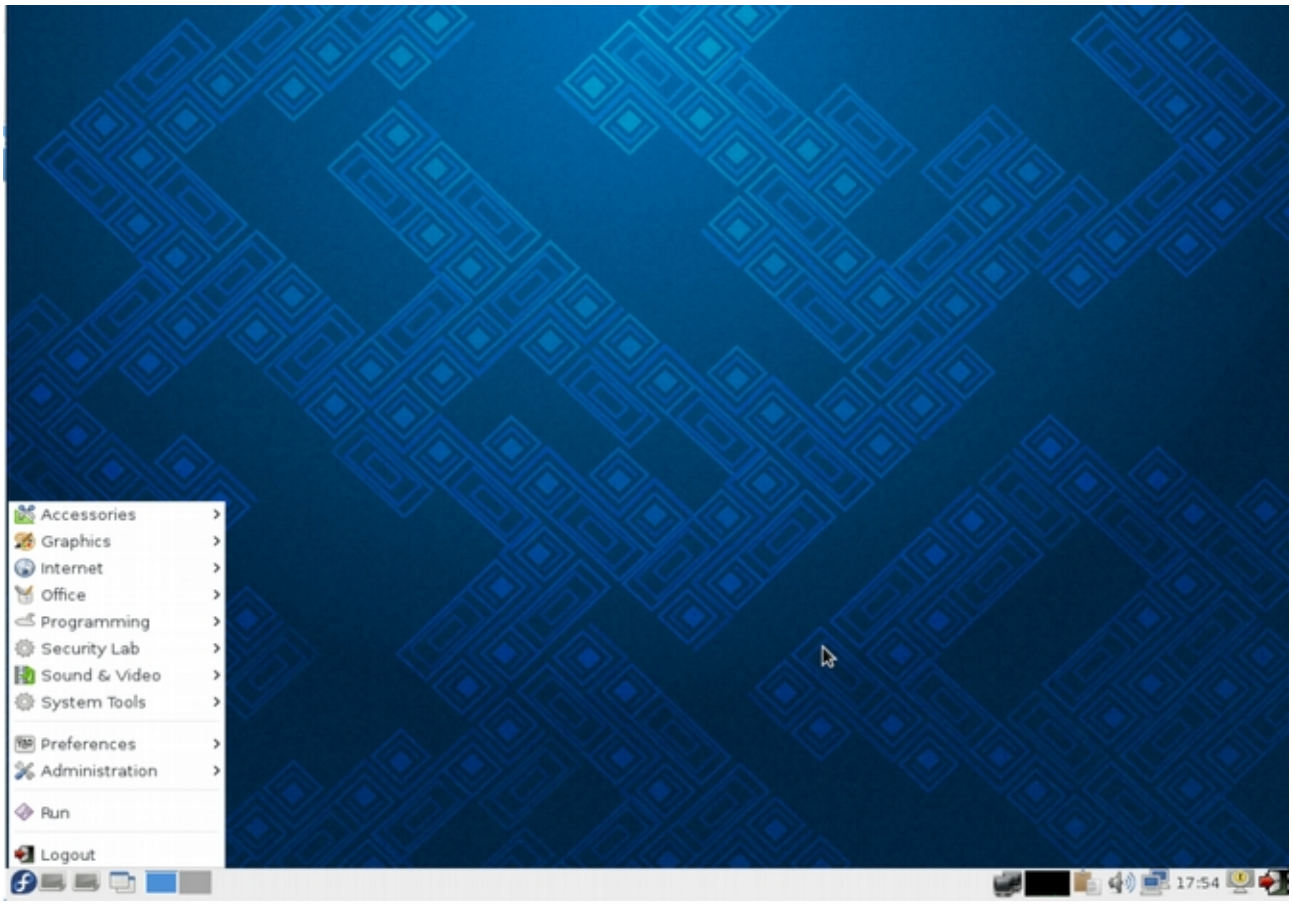
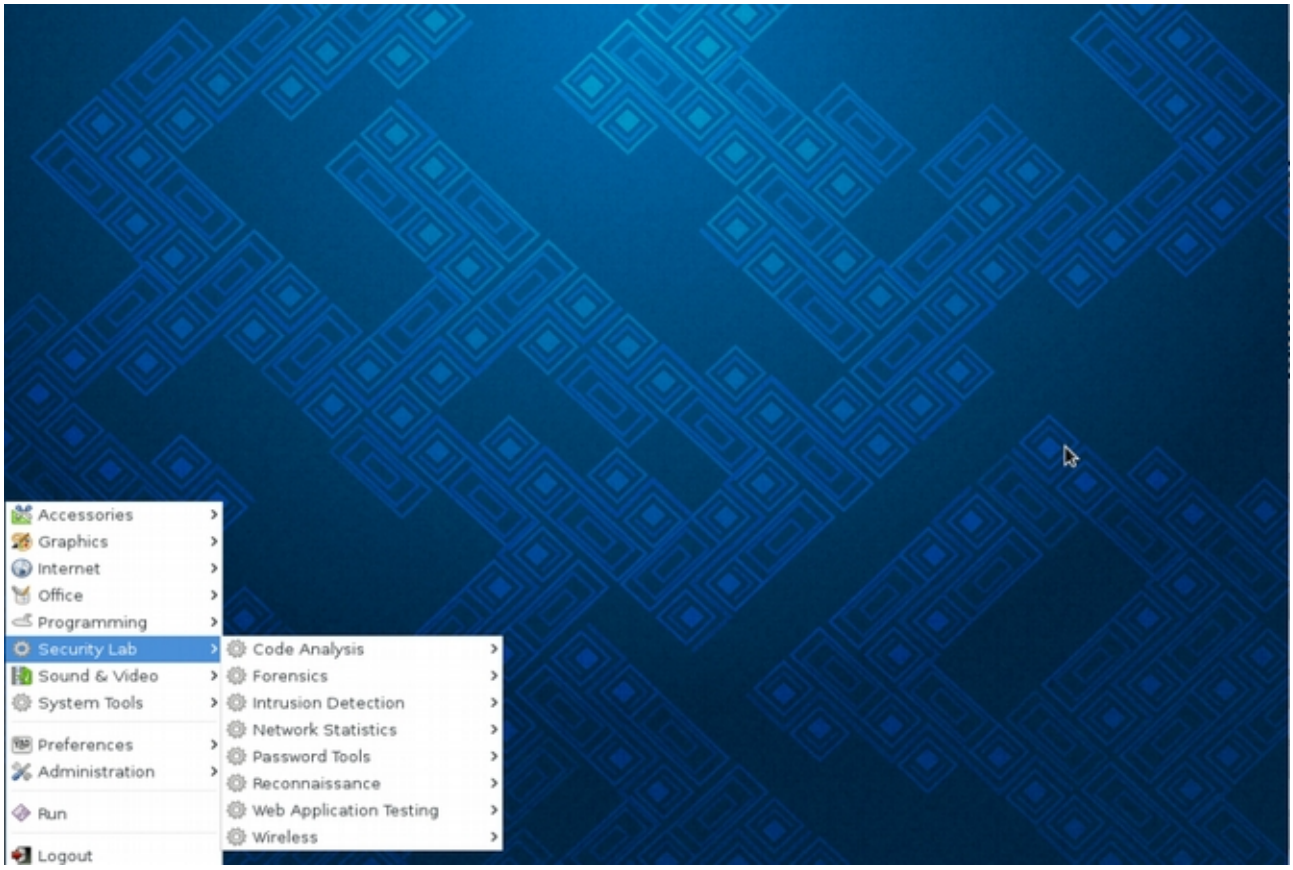
Fedora: Laboratorio di sicurezza
Strumenti di analisi della sicurezza
Vi presentiamo Fedora Security Lab



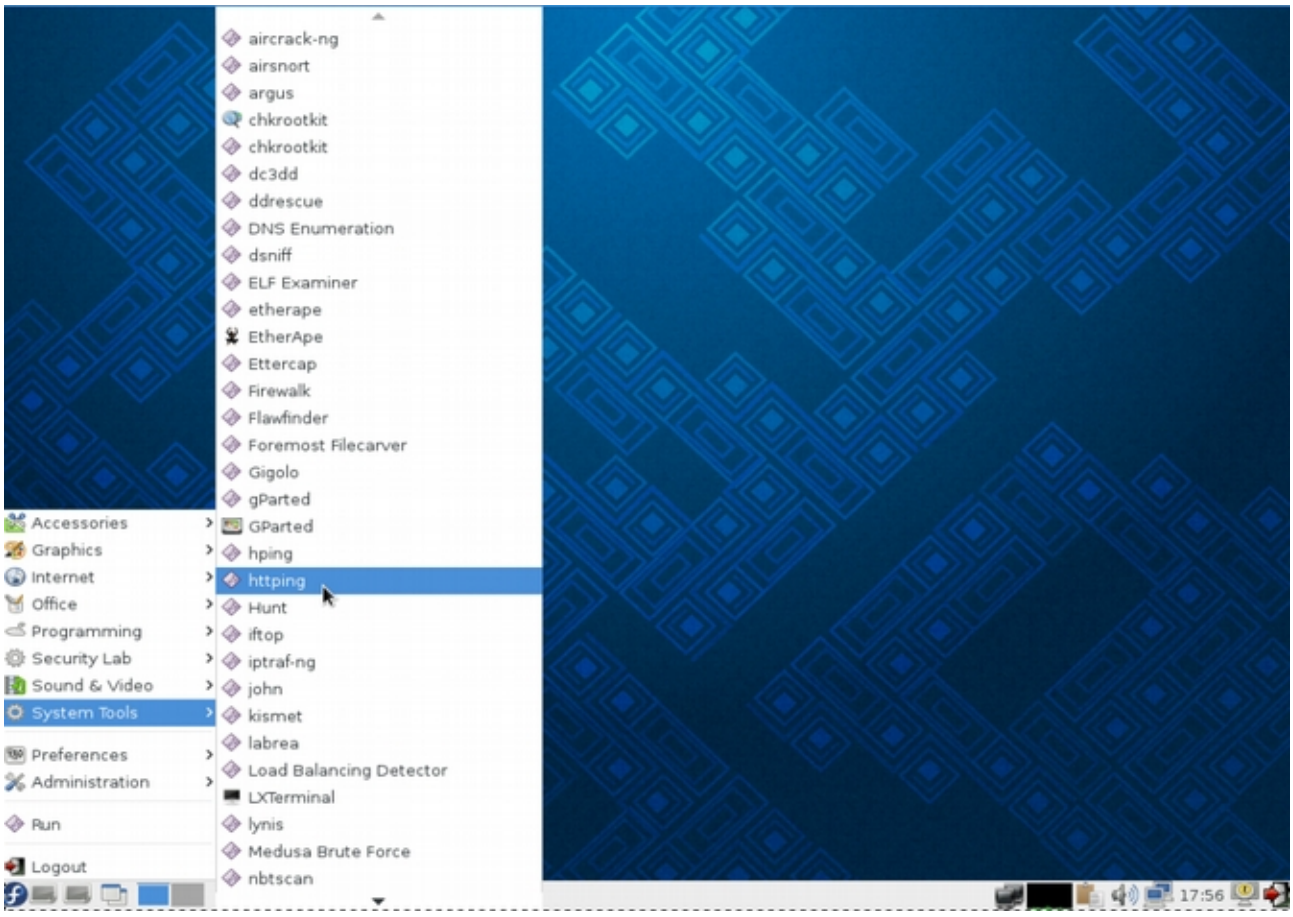
Tra le tante distribuzioni oggi in circolazione, come l'italiana Deft, Caine, NetSecL, StressLinux, la più nota e famosa Backtrack, oggi analizziamo la spin Fedora Security Lab la cui, immagine, è stata costruita per essere installata su chiavette USB. In questo prova l'ho testata in virtuale. La spin fornisce tutti gli strumenti utili, per mettere "al banco di prova" i nostri server e i nostri client, pe la verifica della sicurezza e dell'auditing, per l'analisi forense, penetration-test, o per il recupero di un sistema che è stato danneggiato. Per quanto riguarda la certificazione ISECOM, per maggiori informazioni vi rimando al sito http://www.isecom.org/ (Open Source Security Testing Methodology Manual).

La spin si divide in diverse categorie come analisi del codice, analisi forense, strumenti per l'analisi di rete, rilevazione intrusioni, strumenti per le password, test per applicazioni web, test per il VoIP e per le rete WiFi.



Tra i pacchetti più noti che non hanno certo bisogno di presentazione fanno parte della spin distro: pscan, ddrescue, gparted, testdisk, foremost, sectool, firstaidkit, driftnet, scrub, hfsutility, macchanger, ntfs-3g, ntfsprogs, net-snmp, openvas, sleuthkit, netsed, dnstop, telnet, dnstracer, chkrootkit, aide, rkhunter, vnstat, prelude, tripwire, iftop, ntop, htop, dsniff, wireshark, nmap, tcpdump, ettercap, dnsmap, whois, nmbscan, dhcping, httping, airsnort, kismet, kismon. Nominarle tutte ci sarebbe da fare una lunga lista che trovate direttamente a questo link:

https://fedorahosted.org/security-spin/wiki/availableApps



Un piccolo personalissimo consiglio. Se installata su USB, il consiglio di aggiungere anche LMD, Linux Malware Detect. Ci aggiungerei l'installazione anche di Nessus. A seguito troverete le note di come installare entrambi

Installazione Linux Malware Detect:

[root@localhost ~]# wget http://www.rfxn.com/downloads/maldetect-current.tar.gz

[root@localhost ~]# tar -zxvf maldetect-current.tar.gz

[root@localhost ~]# cd maldetect-1.4.2/

[root@locahost maldetect-1.4.2]# ./install.sh

Dove trovare il file di configurazione:

/usr/local/maldetect/conf.maldet

Ammettiamo di dover eseguire l'antimalware nella nostra web server directory:

[root@localhost maldetect-1.4.2]# maldet --scan-all /var/www/

Ovviamente questo documento è da intendersi solo ed unicamente a scopi didattici ed è per questo che non entrerò più di tanto nello specifico.

Sabbo – z9milinux@gmail.com

Link di riferimento:

https://fedoraproject.org/wiki/Security_Lab?rd=Security_Spin

https://fedorahosted.org/security-spin/wiki/availableApps

http://spins.fedoraproject.org/it/security/

http://docs.fedoraproject.org/en-US/Fedora/19/pdf/Security_Guide/Fedora-19-Security_Guide-en-US.pdf

Linux Malware Detect: http://www.unixmen.com/linux-malware-detect-lmd-in-rhel-centos-and-fedora/