BackTrack

A Security Auditor Toolkit

WARNING

- Do Not Use This Tool to Violate Local Policies
- Do Not Use This Tool to Break Laws
- Do Not Enumerate or Attack Networks without Permission

Hacker Ethics

- It is easier to destroy than to create.
  - (Hackers usually will not destroy their targets, because they want to use the resources.)
- If you can do no good, then at least do no harm.
- The Golden Rule: do unto others as you would have them do unto you.

BackTrack, What is it?

- A Bootable LiveCD Linux Distribution
- Based on Slax http://www.slax.org/
- A Security Auditor Toolkit
- Focus on Vulnerability Assessment and Penetration Testing (PENTEST)
- 300+ Tools
- Many Linux Wireless Drivers

BackTrack, Where do I get it?

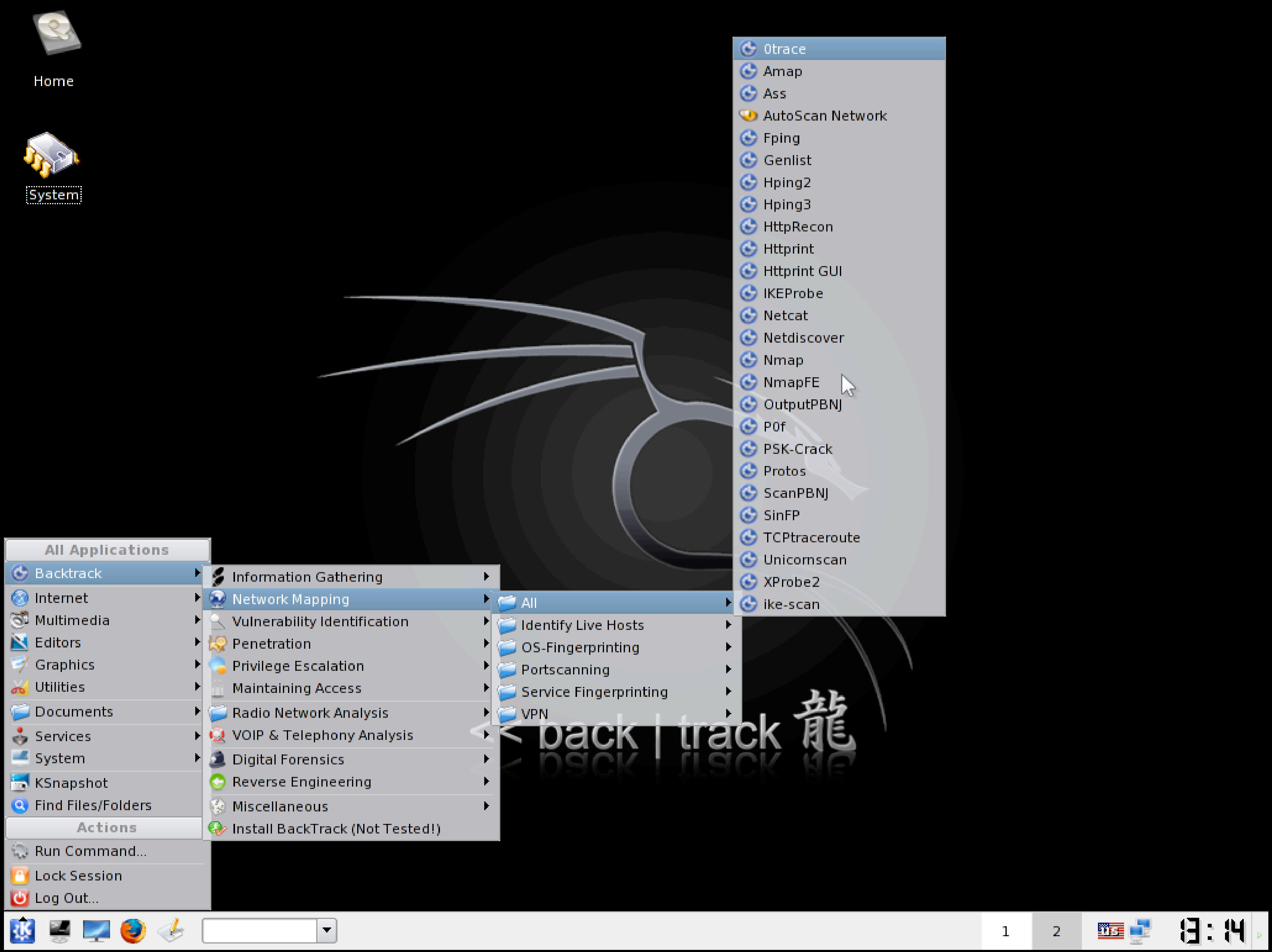
- BackTrack
  - http://www.remote-exploit.org/
  - http://www.remote-exploit.org/backtrack_download.html
- Different Install Versions Available:
  - 700MB and 1GB Versions
  - BackTrack 3 Beta CD-ROM - 14-12-2007
  - BackTrack 3 Beta USB - 14-12-2007
  - BackTrack 2 Stable - 06-03-2007

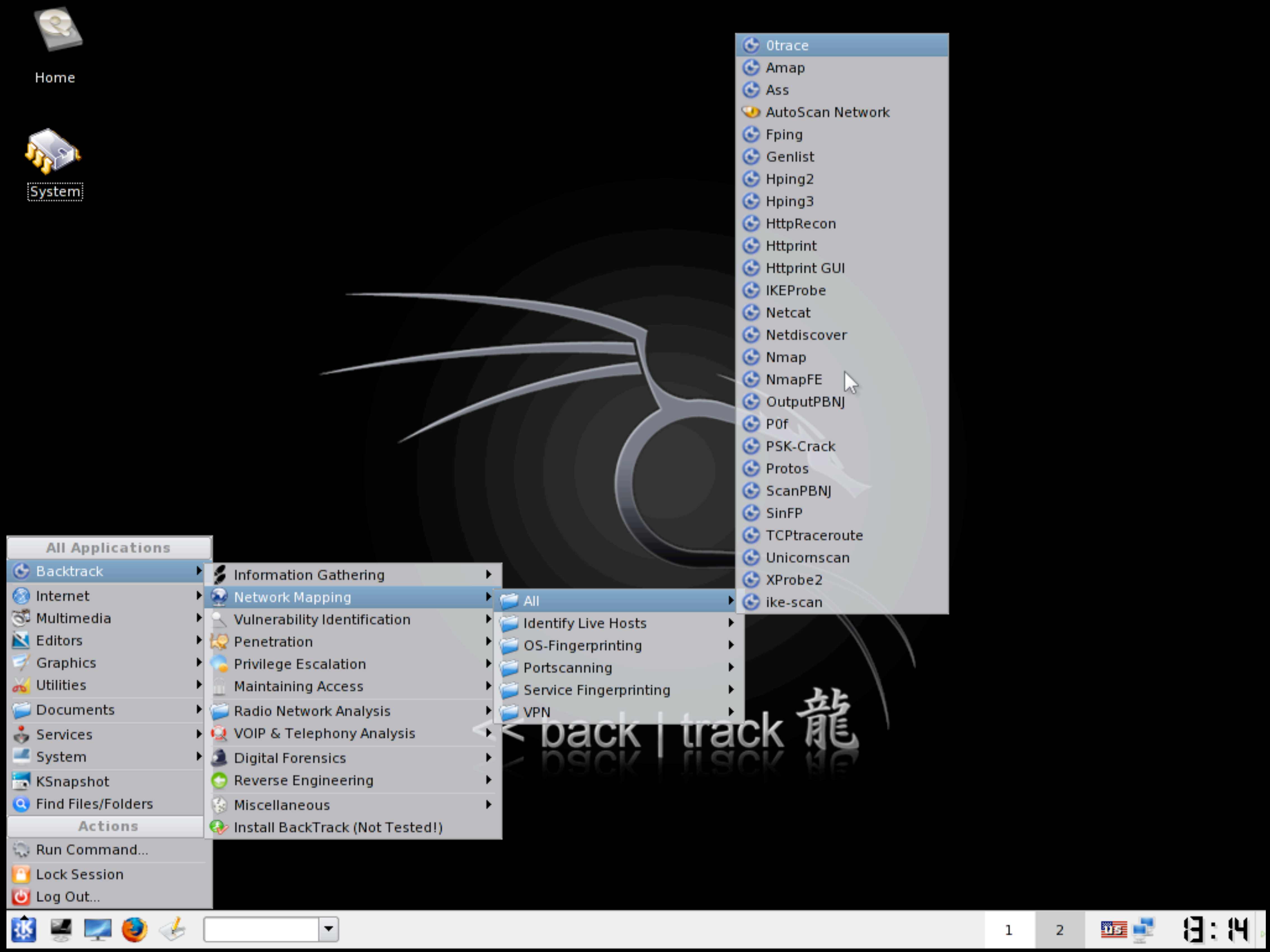
BackTrack, How do I Install It?

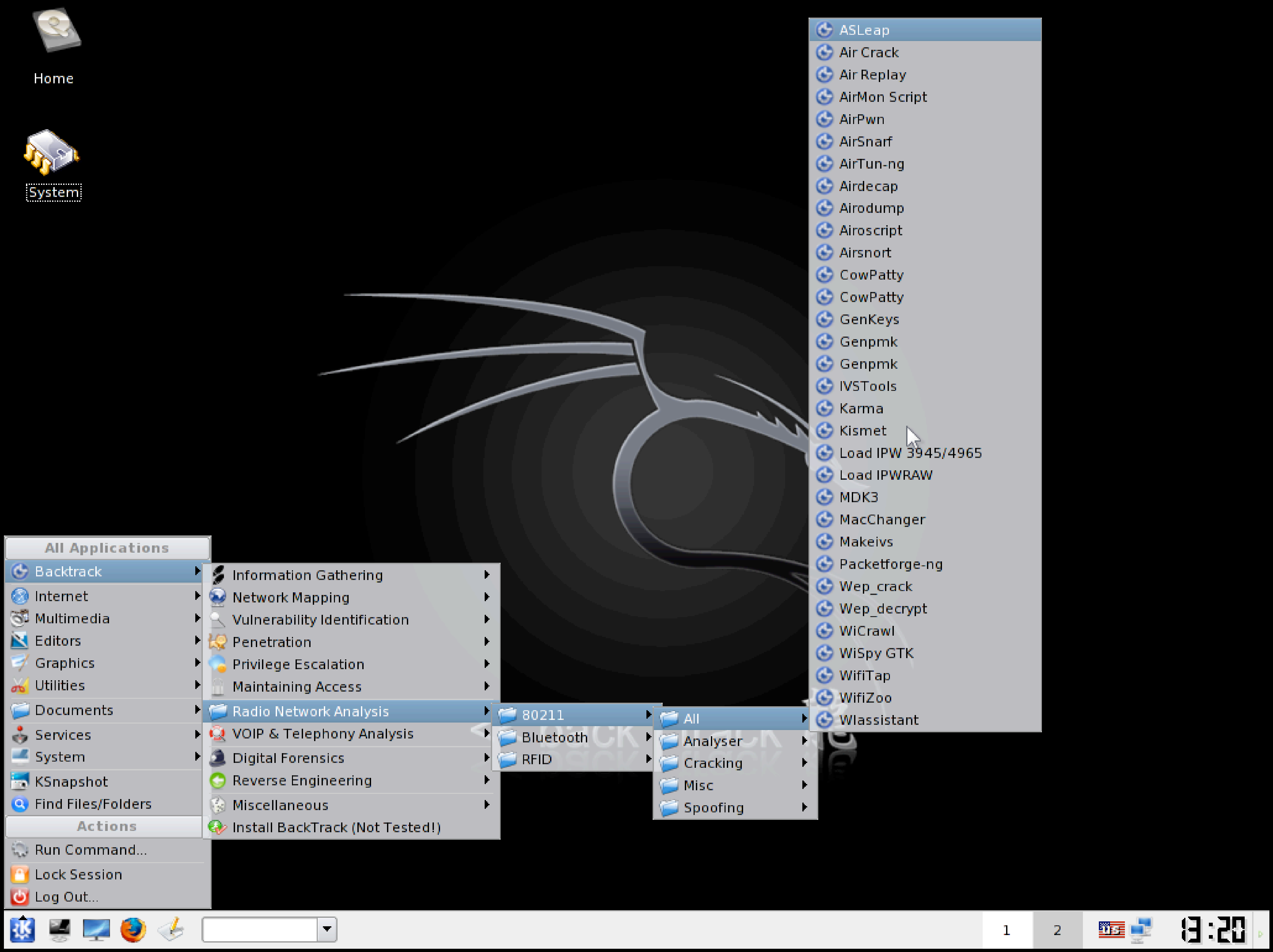
- Burn the CD-ROM ISO
- Write the USB Distro to a USB Key
- Install to Hard Drive

BackTrack: Tools on the CD

- Builtin Servers: HTTP/SSHD/TFTPD/VNC
- Port Scanners: NMap/NMapFE/Zenmap, Nikto (web server scanner)
- Sniffers: Pads, Ethereal, Ettercap
- Wireless Tools: Kismet, Aircrack
- Enumeration Tools: DNS, LDAP, NetBIOS/SMB, SNMP, Web
- Password Tools: Crackers, DSniff
- Spoofers: ARP, DNS
- Exploit Tools: Metasploit Framework, Milw0rm


Home
System
All Applications
Backtrack
Internet
Multimedia
Editors
Graphics
Utilities
Documents
Services
System
KSnapshot
Find Files/Folders
Actions
Run Command...
Lock Session
Log Out...
Information Gathering
Network Mapping
Vulnerability Identification
Penetration
Privilege Escalation
Maintaining Access
Radio Network Analysis
VOIP & Telephony Analysis
Digital Forensics
Reverse Engineering
Miscellaneous
Install BackTrack (Not Tested!)
All
Identify Live Hosts
OS-Fingerprinting
Portscanning
Service Fingerprinting
VPN
0trace
Amap
Ass
AutoScan Network
Fping
Genlist
Hping2
Hping3
HttpRecon
Httprint
Httprint GUI
IKEProbe
Netcat
Netdiscover
Nmap
NmapFE
OutputPBNJ
P0f
PSK-Crack
Protos
ScanPBNJ
SinFP
TCPtraceroute
Unicornscan
XProbe2
ike-scan
<< back | track 龍
1
2
13:14


Home
System
All Applications
Backtrack
Internet
Multimedia
Editors
Graphics
Utilities
Documents
Services
System
KSnapshot
Find Files/Folders
Actions
Run Command...
Lock Session
Log Out...
Information Gathering
Network Mapping
Vulnerability Identification
Penetration
Privilege Escalation
Maintaining Access
Radio Network Analysis
VOIP & Telephony Analysis
Digital Forensics
Reverse Engineering
Miscellaneous
Install BackTrack (Not Tested!)
All
Identify Live Hosts
OS-Fingerprinting
Portscanning
Service Fingerprinting
VPN
0trace
Amap
Ass
AutoScan Network
Fping
Genlist
Hping2
Hping3
HttpRecon
Httprint
Httprint GUI
IKEProbe
Netcat
Netdiscover
Nmap
NmapFE
OutputPBNJ
P0f
PSK-Crack
Protos
ScanPBNJ
SinFP
TCPtraceroute
Unicornscan
XProbe2
ike-scan
<< back | track 龍
1
2
13:14


Home
System
All Applications
Backtrack
Internet
Multimedia
Editors
Graphics
Utilities
Documents
Services
System
KSnapshot
Find Files/Folders
Actions
Run Command...
Lock Session
Log Out...
Information Gathering
Network Mapping
Vulnerability Identification
Penetration
Privilege Escalation
Maintaining Access
Radio Network Analysis
VOIP & Telephony Analysis
Digital Forensics
Reverse Engineering
Miscellaneous
Install BackTrack (Not Tested!)
80211
Bluetooth
RFID
All
Analyser
Cracking
Misc
Spoofing
ASLeap
Air Crack
Air Replay
AirMon Script
AirPwn
AirSnarf
AirTun-ng
Airdecap
Airodump
Airoscript
Airsnort
CowPatty
CowPatty
GenKeys
Genpmk
Genpmk
IVSTools
Karma
Kismet
Load IPW 3945/4965
Load IPWRAW
MDK3
MacChanger
Makeivs
Packetforge-ng
Wep_crack
Wep_decrypt
WiCrawl
WiSpy GTK
WifiTap
WifiZoo
Wlassistant
1
2
13:20

BackTrack, Wireless Config

- /etc/rc.d/rc.inet1 -> /etc/rc.d/rc.wireless
- settings in /etc/rc.d/wireless.conf
- matching based on wireless MAC prefix
- Possible Settings Variables
  - ESSID, MODE, CHANNEL …
- Possible Commands Invoked
  - ifconfig, iwconfig, iwpriv, iwspy, dhcpcd
- Stop/Start
  - /etc/rc.d/rc.inet1 stop
  - /etc/rc.d/rc.inet1 start

BackTrack

Lab Time!