Auditor Security Collection

"A penetration-testing environment at your fingertips"

AGENDA

- Was ist das überhaupt?
- Facts & Figures
- Coole Toolsammlung, aber..
- Einige Tools im Einsatz
- Was kann es nicht?
- Final stuff

About me?

Christoph Weber
Security Engineer
wardriver@wardriving.ch

Stellvertretend für Max Moser

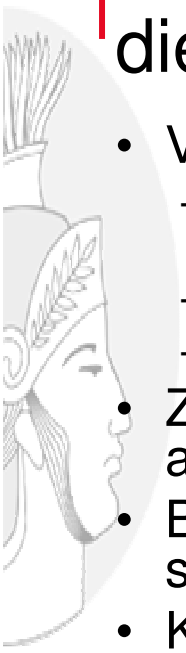
Und was ist mein Job beim Projekt:
Ideenlieferant, Zulieferer, Beta-Tester…
und natürlich Anwender…

Was ist das überhaupt?

Auditor Security Collection (ASC)

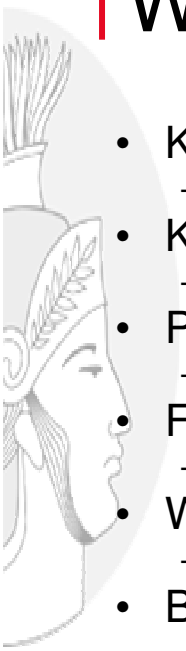
- Knoppix basiertes Linux OS, ab CD-ROM boot- und benutzbar (Neuerdings auf Kanotix basierend).
- Hauptaugenmerk auf Penetrations und Security Einsatz.

Warum eine Toolsammlung wie diese?



- Vergesslichkeit & Faulheit!
  - "Hmm, wie war doch noch der Name des Tools.....?"
  - “Welches Tool ist am besten für..."?
  - “Wo muss man das Tool noch konfigurieren...?”
- Ziel war es, eine “Klick an Run” Umgebung aufzubauen.
- Benutzbar auf der häufigsten Linux supporteten Hardware.
- Keine Installation auf der Hardware nötig.

Wer sind die Konkurrenten?



- Knoppix
  - http://www.knoppix.org
- Knoppix-STD
  - http://www.knoppix-std.org
- PHLAK
  - http://www.phlak.org
- F.I.R.E-CD
  - http://biatchux.dmzs.com
- Whoppix
  - http://www.whoppix.info
- BOSS (BSI OSS Security Suite)
  - http ://www.bsi.bund.de/produkte/boss/index.htm

Vor- und Nachteile der anderen Produkte:

- Teilweise langsames Releaseverhalten oder total veraltet.
- veraltet, out of date
- Fehlende Tools (aus unserer Sicht)
- Andere Zielausrichtung, z.B. Forensic
- Viel Handarbeit bei Konfiguration
- Keine intuitive Handhabung
- Keine Schweizer-Tastatur-Unterstützung

Die Initialisierungs-Gründe und Ziele.

- Regelmässige Update- und Wartungs-Zyklus (2-4 mal pro Jahr), um die Tools und Techniken aktuell zu halten
- Gute Benutzbarkeit und Struktur
- Automatische Anpassung des ärgerlichen Teils der Konfiguration und Abhängigkeiten
- Bereithaltung aller Wirelesstools
- Spezial Patch für RAW Packet Injektion
- Muss ein gutes “allround Kit” sein
- Verbreitung von Grundinformationen (Default Passwörter und Wortlisten)

Benutzer-Anforderung

- Transparenz
- Einfach zum Konfigurieren
- Strukturierte, intuitive Handhabung
- Regelmässige Updates
- Anpassung an Kundenwünsche
- Nicht nur für Linux Freaks

Historische Zeitpunkte

- Erste Entwicklungen im Jahr 2003
- Geplant als Distribution zum Verkauf an grosse Firmen
  - Vertrauen und Benutzbarkeit war einer der Hauptpunkte in dieser Zeit
- Seit Anfang 2004 ist es für alle verfügbar
  - Ziel ist es jetzt, handhabbar machen für alle, nicht nur für den Highend Security Spezialist
- Anfang 2005 auf Kanotix
- Linuxtage 2005 Neue Version

Facts & Figures

- Basiert auf Kanotix (http://www.kanotix.org)
  - Mehrere Verbesserungen gegenüber Knoppix
    - Sound detection
    - Neuere Applikations Pakete
    - Einfacher zum Anpassen
    - Sauberere Struktur
- Linux Kernel 2.6.11 mit Patchen
  - Viele angepasste Wireless Treiber
    - Patched für Spezialanwendungen wie “raw packet injection”
- KDE basiert (nicht mehr icewm)

Wie siehts nun aus?

Desktop

- Aufgeräumt und einfach
- Bekanntes “Look & Feel”
- Batterie Monitor & Uhr
- Schnelle Keyboard-Umstellung möglich
- Virtual Desktop-Unterstützung
- Quicklaunch Bar
- Einfacher Menü-Zugriff

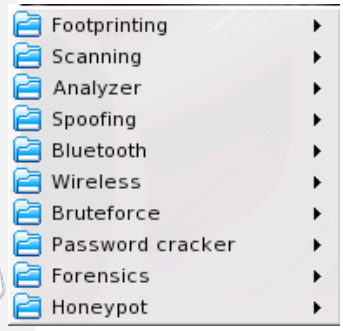
Menü

Zielstellung:

- Klar struktiuriert
  - Unterstreicht das richtige Werkzeug für den richtigen Zweck.
- Skalierbar
  - Die Anzahl und Anordnung variert bei jedem Release.
- Einfach zum Verwalten und Ausbauen
  - Neue Applikationen können einfach in die entsprechenden Kategorien eingefügt werden.

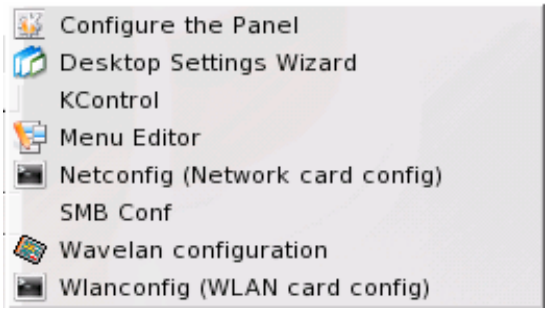
Haupt Menüs

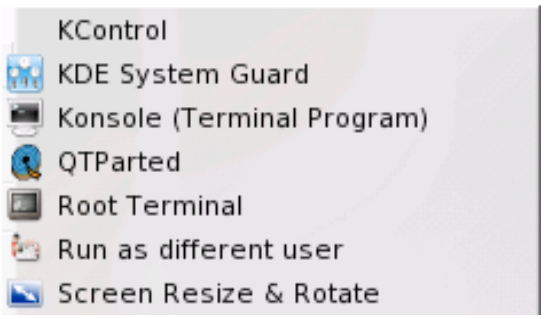
Auditor



Applikationen

Konfiguration & System





Applikationen und Utilities

- Editoren
  - Khexedit, Kwrite, Kate
- Grafische Tools
  - GIMP, KPDF, Ksnapshot
- Internet Clients / Browser
  - Gftp, Xchat, Mozilla, Konqueror
- Remote Clients
  - Rdesktop, Terminal Server Client, NX Client
- Konfigurations Tools
  - HW/SW configuration, Qparted

Das Auditor Menü

Aufgeteilt in sinnvolle Kategorien, die dem Ablauf der Penetrationtests/Audits angepasst sind

- Footprinting
- Scanning
- Analyzing
- Spoofing
- Bluetooth
- Wireless
- Bruteforce
- Password cracker
- Forensics
- Honeypot

Footprinting

- Whois (Greenwich, Gnetutils)
- Traceroute (Itrace, TCTrace)
- DNS lookup (DNSWalk, Host, NSTX [IP over DNS])
- HTTP / HTTPS (Links, Curls, Socat, Stunnel)
- SNMP (SNMPWalk, Tkmib, Arpfetch)
- LDAP (LDAP browser GQ)
- SMB / Netbios (Komba2, NET-Utils, SMB clients)
- OS Detection (NmapFE, Queso, Cheops, P0f, XProbe2)

Scanning

- Security scanner
  - Nessus, Raccess, Metasploit, Cisco global exploiter
- Webserver scanner
  - HTTPrint, Nikto, Socat, Stunnel, Elinks, Curl, Browsers
- Network scanner
  - GTK-Knocker, NMAP(FE), Netenum, Scanrand, IKE-Scan, Knocker
- OS Detection
  - NmapFE, Queso, Cheops, P0f, XProbe2
- Application scanner
  - AMAP, ScanSSH
- SMB scanner
  - NBTscan, SMB-NAT, SMBGet, SMB-clients
- Router scanner
  - Autonomous system scanner (ASS)
- Protocol scanner
  - Protos

Analyzer

- Applications
  - AIM-Sniff, Driftnet, Mailsnarf, Paros, URLSnarf
- Network
  - Ethereal, Etherape, Ettercap, Hunt, IPTraf, Ngrep, NetSed
- Password
  - Dsniff

Spoofing

- Address resolution protocol (ARP)
  - Arpspoof, macof, Nemesis-ARP, Nemesis-Ethernet
- Cisco discovery protocol (CDP)
  - CDP generator
- Dynamic Host Configuration protocol (DHCP)
  - DHCPX (Flooder)
- Domain Name Service (DNS)
  - DNSSpoof, Nemesis-dns
- ICMP spoofing
  - hping2, ICMPRedirect, ICMPush, Nemesis-icmp
- Routing protocols
  - HSRP, IGRP, IRDP, IRDPResponder, Nemesis-IGMP/RIP
- UDP/TCP/IP
  - File2Cable, Nemesis-Ethernet/IP/TCP/UDP, TCPReplay
- Wake on LAN
  - Etherwake

Bluetooth

- Scanners
  - BTScanner, Ghettotool, RedFang, HCITool
- Snarfers
  - Bluesnarfer, RFComm
- OBEX transfer tools
  - OBEXftp, USSP-Push
- Serial connection
  - RFComm, Minicom
- Phone Managers
  - Kandy, Gnome Phone Manager

Wireless

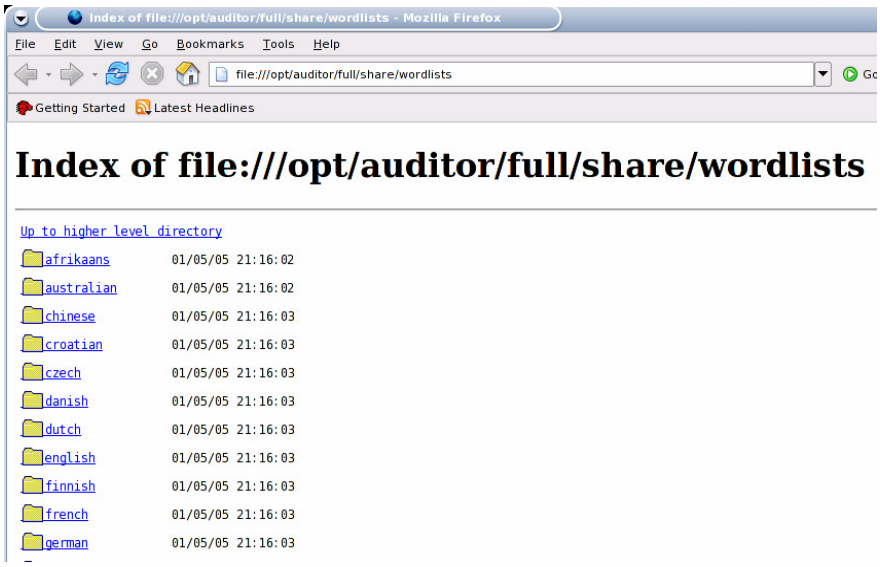
- Scanners / Analyzer
  - Kismet, Gkismet, Wellenreiter
- Crackers
  - WEP (Aircrack, WEP-Tools, Airsnort (new), ChopChop, Dwepcrack, WEPAttack, WEPlab, Decrypt)
  - LEAP/PPTP (ASLeap)
  - WPA (COWPatty)
- Client penetration
  - Hotspotter, APMode
- RAW packet injection
  - File2Air, Void11
- Tools
  - GPSD, Change-MAC

Bruteforce

- Universal Tools
  - Xhydra, Hydra
- Spezial Tools
  - ADMSNMP (SNMP)
  - Guess-Who (SSH)
  - K0ld (LDAP)
  - Obiwan (HTTP)
  - SMB-NAT (SMB)
  - VNCrack (VNC)

Bruteforce

- Wordlists (7,211,729 Wörter)



Password cracker (1)

- Universal Tools
  - John (gepatched mit vielen weiteren Modulen)
- Spezial Tools
  - BKHive, Samdump2 (SAM info gatherer)
  - FCrackzip (ZIP files)
  - Rainbow crack (Precomputed hashes using Rainbow tables)

Password cracker (2)

- Aktuelle Default Passwortliste
  - Aktuelle Liste von http://www.phenoelit.de/dpl/dpl.html

Default Password List

2005-05-28

Manufactor	Product	Revision	Protocol	User ID	Password	Access
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	
3COM	LANplex	2500	Telnet	debug	synnet	
3COM	LANplex	2500	Telnet	tech	tech	
3COM	LinkSwitch	2000/2700	Telnet	tech	tech	

Forensics

- Neuer Menüteil, hinzugefügt um eure Interessen zu überprüfen.
  - Autopsy (Automatic configuration and startup)
  - Recover
  - Testdisk
  - Wipe

Honeypot

- Neuer Menüteil, hinzugefügt um eure Interessen zu überprüfen.
  - HoneyD
  - IISEmulator
  - Tinyhoneypot
  - Password collectors
    - IMAP
    - POP3

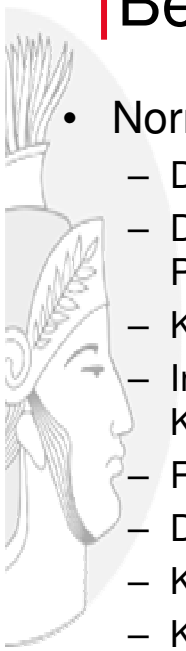
Ok, Coole Toolsammlung, schönes Menü,.....

Aber ist das alles?

Autokonfiguration

- Wegen der Natur eines “READ-ONLY” Mediums, müssen die nervigen Konfigurationen der Tools und Applikationen beim Start jederzeit automatisch gemacht werden, sowie auch bei jedem Wechsel der Umgebung.

Beispiel: Kismet verschiedene Karten



- Normaler Vorgang:
  - Download Kernel Sourcen
  - Download Treiber und Patches
  - Kompilieren des Kernels
  - Installation des Wireless Kartentreibers
  - Recompile des Kernels
  - Download Kismet Sourcen
  - Kompilieren von Kismet
  - Kismet für Karte konfigurieren
  - Konfigurieren von Logfile Name
  - Konfiguration von Logfile Lokation
  - Abhängig von Karte und Kismet Version, anpassen des Monitoring Moeds
  - Start Kismet_server
  - Start Kismet_client mit p
  - Parametern für Login

Und wenn die Karte wechselt, alles von vorne!

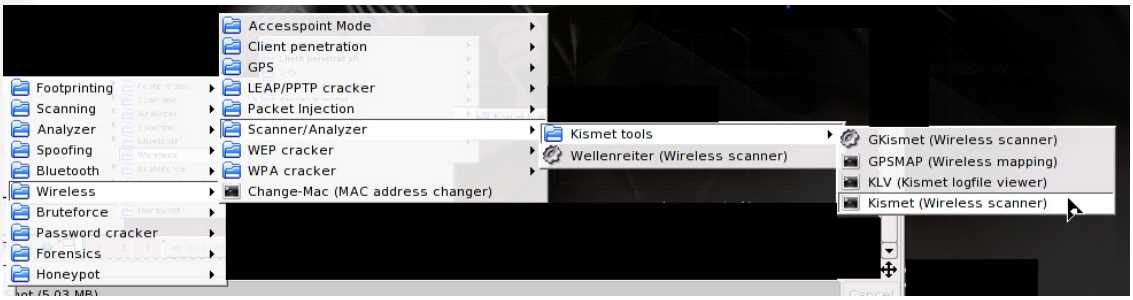
Beispiel: Kismet mit verschiedenen Karten

- Auditor Security Collection:
  - Karte einfügen
  - Klick auf "Kismet" im Menü
  - Interface im Menü auswählen (nicht immer notwendig)
  - Logfile Ablage wählen
  - Logfile Präfix auswählen

Der gleiche Ablauf, bei jedem Kartenwechsel!

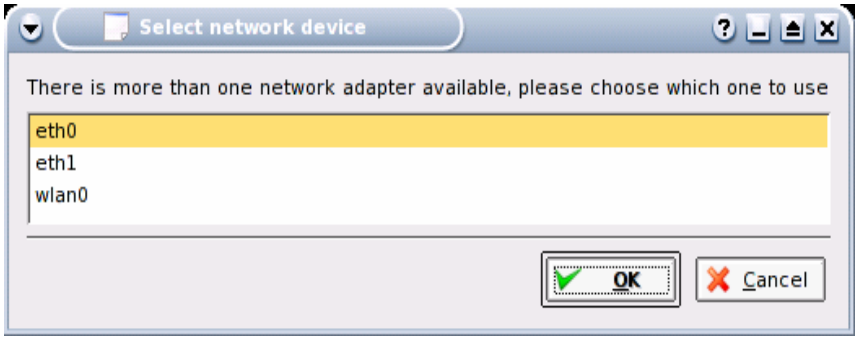
Beispiel: Kismet mit verschiedenen Karten

- Karte einfügen
- Klick auf "Kismet" im Menü



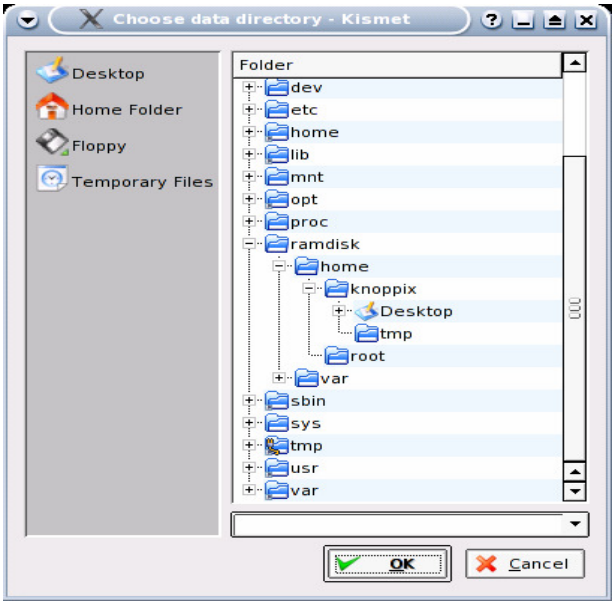
Beispiel: Kismet mit verschiedenen Karten

– Interface Auswählen im Menü (nicht immer notwendig)



Beispiel: Kismet mit verschiedenen Karten

– Logfile Ablage wählen

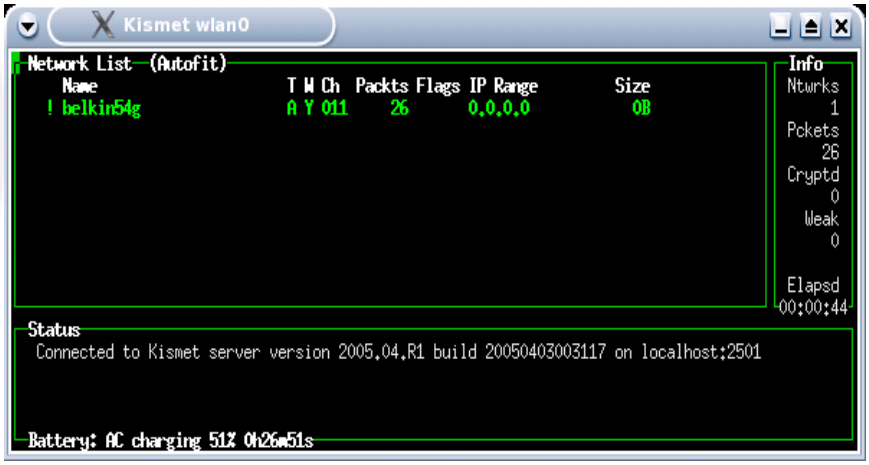


Beispiel: Kismet mit verschiedenen Karten

– Logfile Präfix auswählen

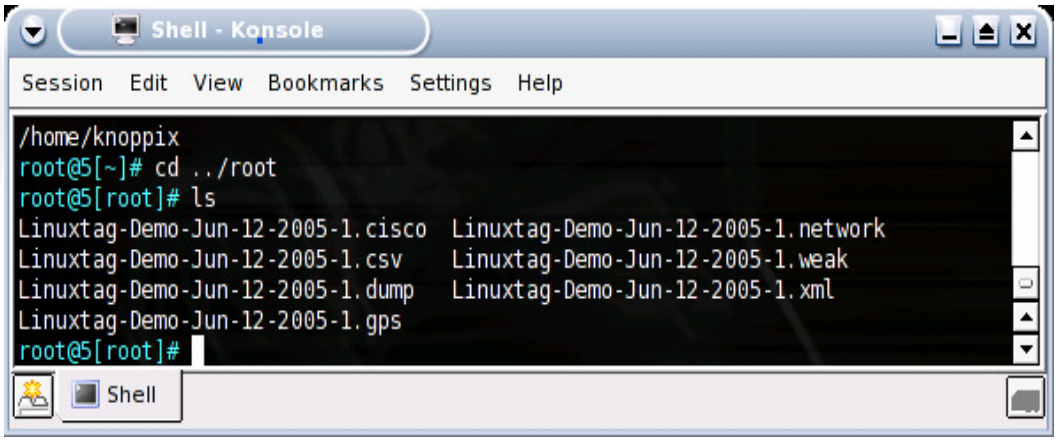
Beispiel: Kismet mit verschiedenen Karten

– Kismet benutzen



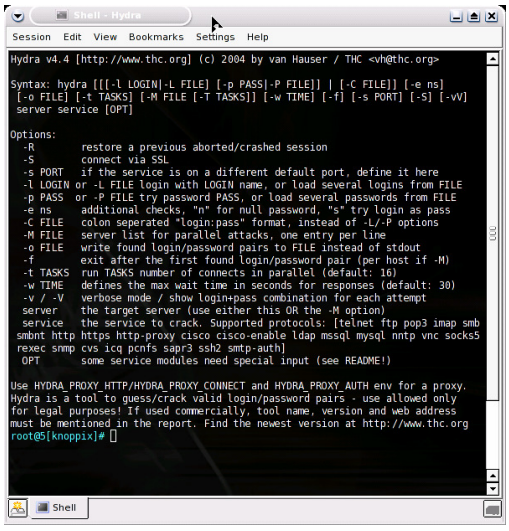
Beispiel: Kismet mit verschiedenen Karten

– Kismet Logfiles



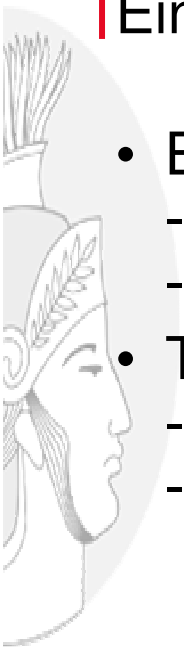
Und wenn keine Autokonfiguration vorhanden ist?

Nicht alle Tools besitzen eine Autokonfiguration. Diese werden dann in einem shell window, und wenn vorhanden, mit der Help Option aufgerufen.



Beispiel hydra:

Hier macht es keinen Sinn, grafische Abfragen zu machen.



Einige Tools im Einsatz:

- Bluetooth Bluesnarfer
  - Tool auf der CD
  - selbstgestrickte Erweiterung
- Tcpdump
  - Tools auf der CD
  - Filtersammlung / Scripts?

Bluetooth Bluesnarfer:

Bluesnarfer ist fertig zum Einsatz als Command Linetool, aber kein fertiges Hackertool.
Auditor Teil: Anpassung

```
*** bluesnarfer.h.orig         Wed Jan 12 17:54:41 2005
--- bluesnarfer.h              Wed Jan 12 17:55:00 2005
***************
*** 8,14 ****
  #define DDIAL               0x6
  #define INFO                0x7

! #define RFCOMMDEV           "/dev/bluetooth/rfcomm/"
  #define DEFAULTPB           "AT+CPBS=\"ME\"\r\n"

  struct opt {
--- 8,14 ----
  #define DDIAL               0x6
  #define INFO                0x7

! #define RFCOMMDEV           "/dev/rfcomm"
  #define DEFAULTPB           "AT+CPBS=\"ME\"\r\n"

  struct opt {
```

Bluetooth Bluesnarfer:

```
root@sniffi[blue]# bluesnarfer -r 1-100  -b 00:0e:6d:XX:XX:XX
device name: Nokia 6310i
+   1 - Beat : +4176383XXXX
+   4 - Rene : 079604XXXX
+   7 - Barb : 079755XXXX
+   10 - Andi P. Natel : 004179280XXXX
+   13 - Peti : 004179516XXXX
+   16 - Mse : +4178789XXXX
+   19 - Speli Natel : 004176325XXXX
+   22 - Aziz : 06050XXXX
+   25 - Rene Deutsch : 0359522XXXX
+   26 - Tschanz : 078610XXXX
+   27 - Erni : 05231XXXX
bluesnarfer: release rfcomm ok
```

Bluetooth Bluesnarfer:

Und was man damit machen kann.

```
do forever
{
scan for devices()
    for each devices found do
       {
       test if i can connect to the Bluetooth Device with bluesnarfer
       if (yes)
         {
         get phone type
         get phone liste
         write infos to a list
         and if you will make money, call my 0900..... Number
                                    (50.- per call)
         }
       }
}
```

(nicht optimaler Code, aber Managertauglich)

tcpdump + ethereal + tethereal

- Kennt jeder Netzwerktechniker
  - Was wird geliefert:
    lauffertige Version
  - Was wird nicht geliefert:
    fertige ethereal Filter-Files
    Interpretation der Dump Files

tcpdump + ethereal + tethereal

- Auszug aus einem Script

```
split_dumpfile() {
    echo -e "\n#########################################################################"
    echo -e "### write tcpdump files (binary)"
    echo -e "arp file..."
    $tcpdump_path -r $tcpdumpfile -nn arp -w $tmpdir/tcpdump_arp > /dev/null 2>&1
    ls -lh $tmpdir/tcpdump_arp | awk {'print $9" "$5'}
    echo -e "icmp files..."
    $tcpdump_path -r $tcpdumpfile -nn icmp -w $tmpdir/tcpdump_icmp > /dev/null 2>&1
    ls -lh $tmpdir/tcpdump_icmp | awk {'print $9" "$5'}
```

Diese Arbeit muss jeder selber machen!

Zusammenfassung:

- Auditor besitzt eine grosse Auswahl an aktuellen Tools, integriert in ein strukturiertes Benutzermenü und wenn möglich Autokonfiguration.

Und was ist der Nutzen?

- Grundlegendes Arbeitsumfeld
  - Perfekt für Schulung und Support
- Unabhängig von bereits installierter HW + SW
  - Keine Installation notwendig
- Vorbereitungszeit kann reduziert werden
  - Alle Tools sind konfiguriert und einsatzbereit
- Schützt vor Vergesslichkeit
  - Man darf nur nicht die CD vergessen…
- Anpassungsfähig
  - Beispiel: Als Marketing “Giveaway”
  - Beispiel: Interne "more harmless" Version

Was kann es nicht?

- Automatische Audits
  - Es liefert keine automatischen, kompletten Audit-Reports. Security-Kenntnisse sind weiterhin nötig.

  Automatische Hacks
  - Es ist kein Hackertool, sondern ein Auditing-Tool, aber was man damit macht, muss jeder für sich selber entscheiden!
- RTFM
  - Man muss immer noch selber herausfinden, was genau welches Tool macht, und wie man es am besten einsetzt!
- Sonstiges
  - Kaffeekochen (noch nicht, aber geplant)

Was ist Neu in dieser Version?

- Bessere USB-Unterstützung
  - USB CD Laufwerke
  - USB Memory Sticks
- Kernel Hardening
  - IP-Stack Hardening teilweise umgesetzt

Was ist Neu in dieser Version?

- 2 verschiedene ISO Images: Wegen Treiberproblemen in der Autoerkennung
- auditor-200605-02-ipw2100.iso für Karten mit ipw2100 Chip
- auditor-200605-02-no-ipw2100.iso für Karten mit ipw2200 Chip

Was ist Neu in dieser Version?

- proxychains 1-8-1 (for example scanning over proxy more easy)
- kismet-logfile-viewer klv.pl and klc.pl
- ntp fingerprinting tool
- tftp bruteforce tool
- cisco torch 0.4b
- unicornscan 0.4.2
- packit
- sendip
- nasl 2.2.4
- tcpick
- cryptcat
- amap version 4.8
- tcpsplit
- Ethereal version 10.11
- ettercap-ng-0.72 and modified the etter.conf
- replaced tinysnmp with snmp tools
- vnc2swf /usr/X11R6/bin/recordwin and vnc2swf
- wpa-supplicatiant 0.3.8
- hostapd-utils 0.3.7
- ssldump
- fragrouter
- Metasploit 2.4 including all known updates
- airsnarf, but no menu at moment
- fakeap to /opt/auditor but no menu entry at moment, need to write a shell script
- dsniff 2.4b1-10
- nessus plugins updated
- Snort 2.3.2-5
- Bleeding-edge rules for snort

.....

→ für mehr infos, lies die Release Info

BUGS in dieser Version?

- Teilweise Probleme mit Kismet
  → Problem vom Kismet
- Und viele uns noch nicht bekannte....

Blick in die nahe Zukunft

- Noch bessere Kartenunterstützung / Kartenerkennung div. Anbieter
- USB Wireless Adapter
- OS Hardening
- Weitere Integration von Tools mit Userführung
- Neue Netzwerktools
- Integration von „missing“ Tools

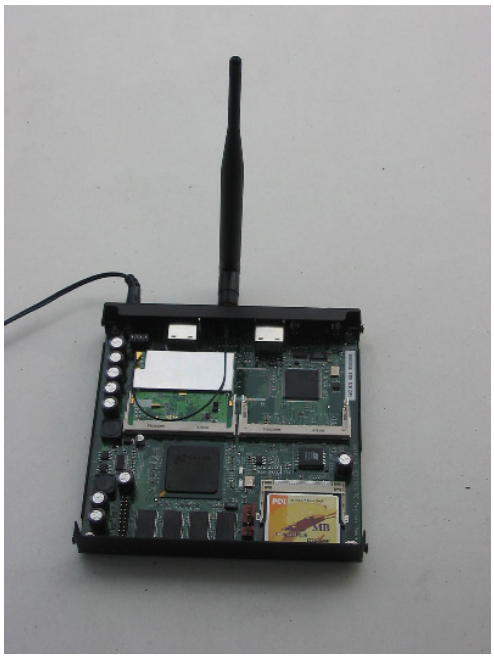
Blick in die ferne Zukunft

- RFID Integration....
- Infrarot Tools...
- Audit Reporting Tools...
- DVD Version mit noch mehr Tools (+ Rainbow Files)...

...an Ideen mangelt es uns nicht, nur an Zeit und Geld.....

Blick in die ferne Zukunft (2)

- Auditor auf einer Appliance als Server...



Final stuff

- Wo kriegt man das Ding?
  FTP Server Liste auf:
  - http://www.remote-exploit.org
- Was kostet es?
  - Es finanziert sich aus Spenden.
    (Geld + Hardware)
- Sind individuelle Anpassungen möglich?
  - Ja, Preis ist Verhandlungssache.

Unterstützte Hardware

- Ist XYZ unterstützt?
  - Es existiert eine Wiki Dokumentation und ein Forum auf
    http://www.remote-exploit.org

```
[-=] PCMCIA wireless adapters known to work [=-]
```

Vendor	Model	Status	Comment	Chipset
3-Com	CRWE737A	OK	-	Spectrum24
Belkin	802.11b Belkin Prism2	OK	-	Prism 2
Buffalo	WLI-PCM-L11GP	OK	-	-
Cisco	Aironet CB21AG-A-K9	OK	-	Atheros
Cisco	Aironet PCM-352	OK	-	Cisco
Cisco	Aironet LMC-352	OK	-	Cisco
Cisco	Aironet AIR-PCM340	OK	-	Cisco
Cisco	Aironet AIR-01(352)	OK	-	Cisco
Dell	TrueMobile? 1150 (802.11b)	OK	-	Hermes/Orinoco?

Bug Reporting

- Fehler!
  - Da Niemand und nichts Fehlerfrei ist, gibt es auch Bugs auf der CD.
- Auditor Bugs?
  - Mitteilung an uns, was, wie, mit welcher Hardware nicht geht. BITTE: Detailliert!!!!
- Allgemeine Software Bugs?
  - Bitte direkt an Entwickler, allenfalls Kopie an uns.

Q & A

Christoph Weber
http://www.wardriving.ch
wardriver@wardriving.ch

Max Moser
http://www.remote-exploit.org
mmo@remote-exploit.org