Intrusion Prevention from the Inside Out

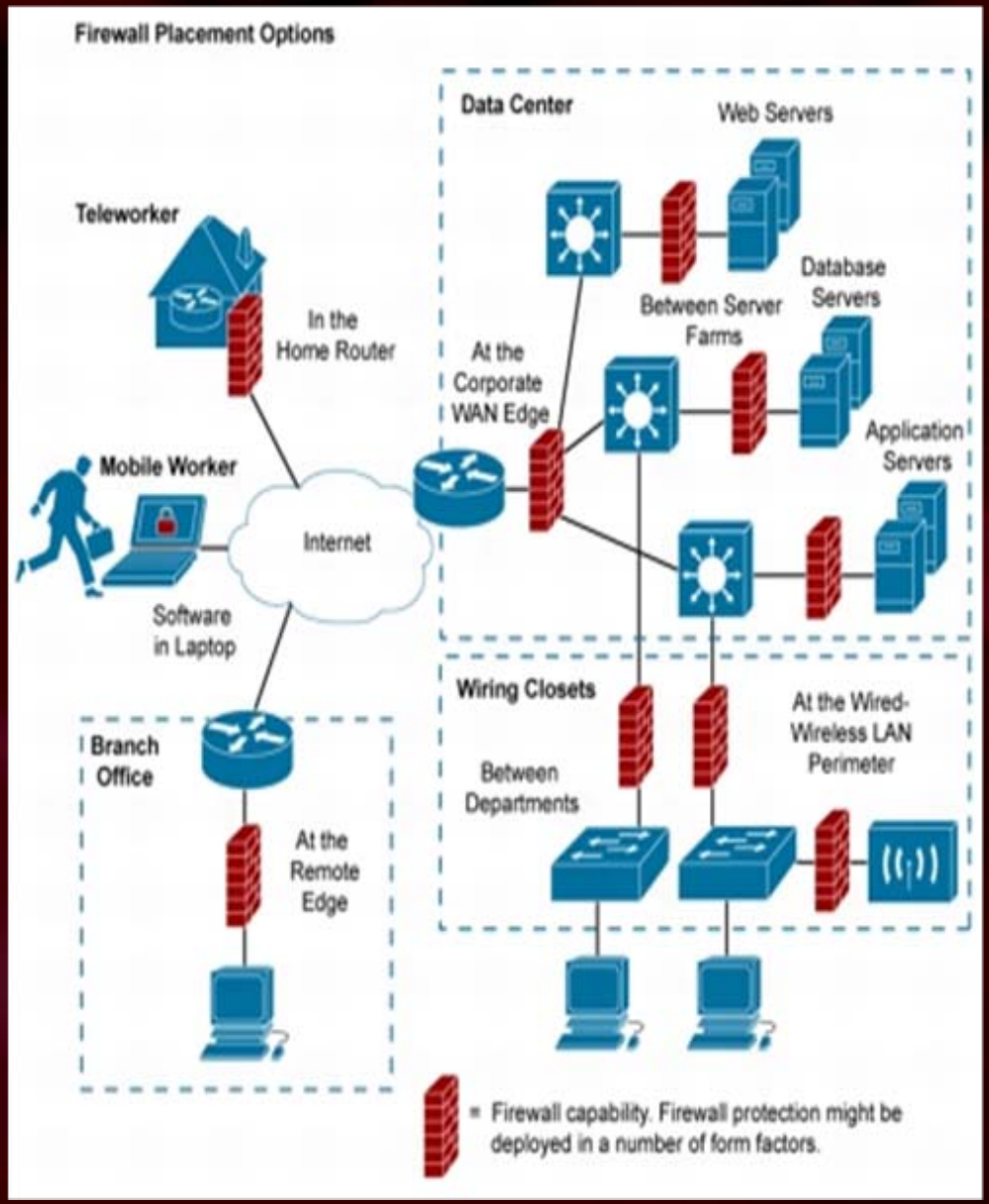
Ernest Staats
Director of Technology and Network Services at GCA
MS Information Assurance, CISSP, CEH, MCSE, CNA, CWNA, Security+, I-Net+, Network+, Server+, A+
Resources available @ http://es-es.net

Topics to be Covered

- Anatomy of a typical network
- Can’t defend what you don’t know
- The new perimeter and how to defend it?
- The insider
- Control access to Data
- Encryption
- Passwords the dirty little secret
- Open source or “free” Tools I use
- Microsoft Security Tools
- VM Security Issues
- Not covered -- Wireless

Anatomy of a typical network

- The illusion of external and internal needs to change
- Where is “the” firewall?
- Web 2.0 pushes this out to the cloud



Can’t defend what you don’t know

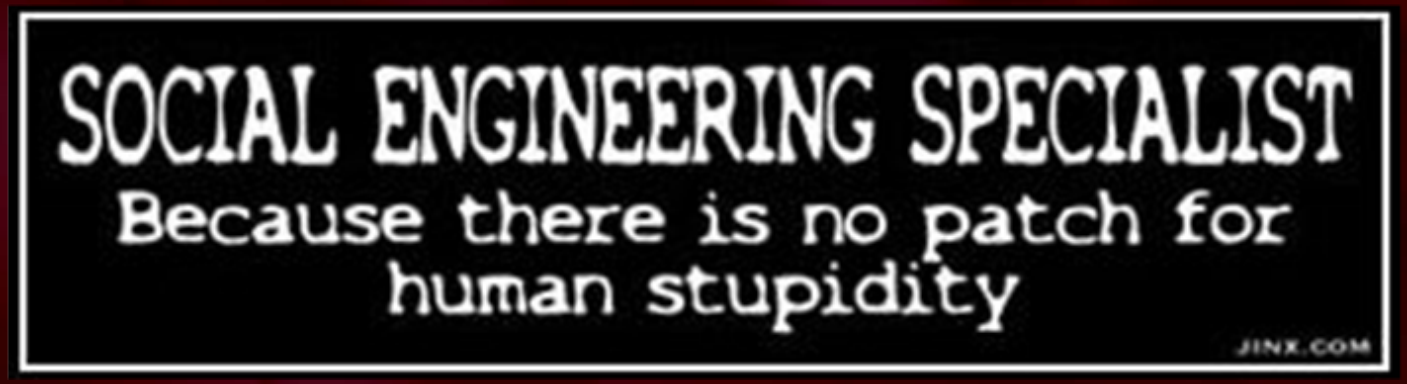
- “Know your enemies & know yourself” <Sun Tzu>
- Map your network regularly “The Dude”
  “Engineers Tool Set”
- Sniff and Baseline your network know what type of data needs to be going across your system
- Know what types of paths are open to your data
- Web 2.0
- Mobile device access
- DLP- Data leakage prevention recognizes sensitive data during content inspection on a network appliance and endpoint software.
- RMS - Rights management restricts end-user actions:
  - printing and copy/paste
- Device control aims to prevent confidential data from walking out the door

The New Perimeter & How to Defend It

- What keeps me up at night?
- USB Blocking
  - Windows GP
  - Netwrix http://www.netwrix.com/usb_blocker.html
- WIFI and mobile devices
- Outside email
- VPN –Remote Access of data
- Web 2.0 / Social Networking sites
- Users
- GFI end point security
- **Guardian Edge smart phone**

The Users: “They Are All Witches”

- Users are witches even if it is because we have made them that way by not communicating. Thus forcing them to come up with their own solutions!



- Education and training can lower the impact and success of Social Engineering

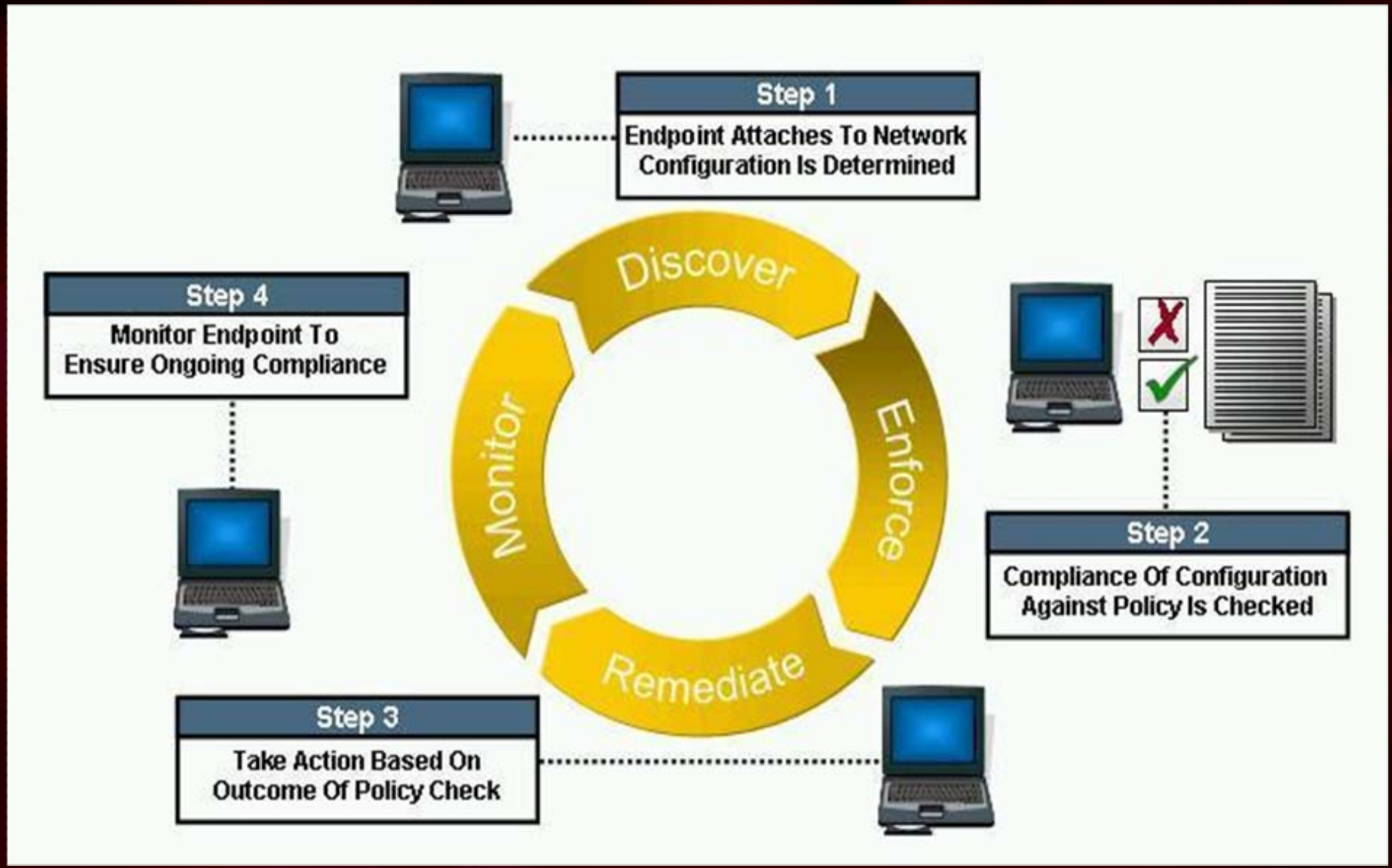
Control Access to Data (NAC)

- What is a NAC? Control who and what gains access to a network to ensure they meet a set standard, and continually monitoring to ensure the devices remain compliant
- The promise
  - "Clean up your network and solve all your security problems."
- The Reality
  - Adds a layer of complexity (policy vs. action enforcement)
  - Proper switch configuration
    - VLAN configuration is critical (management VLAN)
    - SNMP and NTP can become issues
    - L2 vs L3 switches (capable vs. enabled)
    - What is holding your ARP information– Is DNS working?

Types of NAC

- Hardware-based: “appliances” -- some replace switches, others operate between the access layer and network switches
- Software-based: software “Agent” must be installed on each end device “PC”
- Inline: become a single point of failure
- Out-of-band: often require a high level of network and server configuration change and ports to track
- Agent : -- higher level of security can be conducted and can generate less network traffic, but… software deployment and maintenance become issues
- Agentless: vulnerability or policy assessment scans (or both) on endpoints before they're permitted to access the network fully (typically more network traffic)

The Typical NAC Process



Hardware Vendors

- **Bradford**
- **Fore Scout**
- **CISCO**
- **Mirage Networks**
- **Blue Coat**
- **CyberGatekeeper**
- **Trend Micro**
- Several hardware vendors are merging NAC with IDS/IPS

Software Vendors

- Sophos
- Packet Fence (“Free” lots of options) http://www.packetfence.org/downloads.html
- Symantec
- Dynamic NAC Suite
- NuFW IP based access (Free) http://www.nufw.org/
- Microsoft NAP Network Access Protection Server 08

Encryption Software

- Hard drive or Jump Drives
  - CE Infosys http://tinyurl.com/33aa66
  - True Crypt for cross platform encryption with lots of options
    - http://www.truecrypt.org/downloads.php
  - Dekart its free version is very simple to use paid version has more options
    - http://www.dekart.com/free_download/
      - http://www.dekart.com/
- Email or messaging
  - PGP for encrypting email
    - http://www.pgp.com/downloads/index.html

Passwords: Length Matters

- The secret: If you password is long enough, it doesn't need to be complex. Long passwords defeat common password crackers
- How long should your passwords be?
  - Passwords should be a minimum of 10- 15 characters to be considered non-trivial.
- A password of 15 characters or longer is considered secure for most general-purpose business applications. i.e. a "pass phrase"
- Disable the storage of weak cached LM password hashes in Windows, they are simple to break

Good example: Denverbroncosrulethenhl

Password Recovery Tools:

- Fgdump (Mass password auditing for Windows)
  - http://foofus.net/fizzgig/fgdump
- Cain and Abel (password cracker and so much more….)
  - http://www.oxid.it/cain.htnl
- John The Ripper (password crackers)
  - http://www.openwall.org/john/
- RainbowCrack : An Innovative Password Hash Cracker tool that makes use of a large-scale time-memory trade-off.
  - http://www.rainbowcrack.com/downloads/?PHPSESSID=776fc0bb788953e190cf415e60c781a5

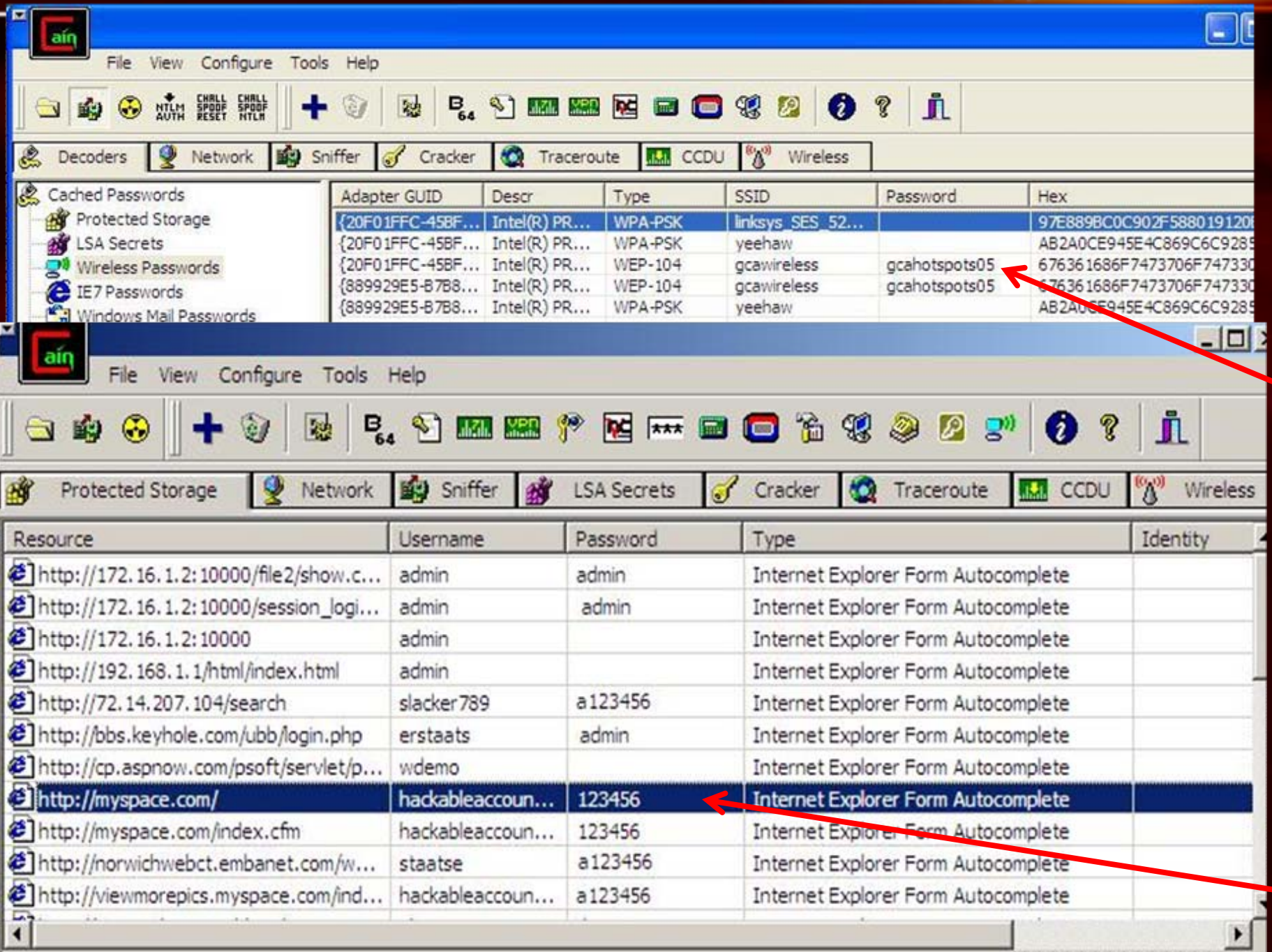
Most Used Tools:

- Google (Get Google Hacking book)
  - The Google Hacking Database (GHDB)
    - http://johnny.ihackstuff.com/modules.php?op=modload&name=Downloads&file=index
- **Default Password List**
  - http://tinyurl.com/39teob
- **Nessus**
  - Great system wide vulnerability scanner http://tinyurl.com/3ydrfu
- Cain and Abel
  - (the Swiss Army knife) Crack passwords crack VOIP and so much more
    - http://www.oxid.it/cain.html
- **Autoruns**
  - shows the programs that run during system boot up or login
  - http://tinyurl.com/3adktf
- **Iron Geek**
  - Step by step security training http://tinyurl.com/bzvwx
- SuperScan 4
  - Network Scanner find open ports (I prefer version 3)
    - http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm
- EventSentry
  - Allows you to consolidate and monitor event logs in real-time, http://tinyurl.com/2g64sy

Most Used Tools:

- **The Dude**
  - Auto network discovery, link monitoring, and notifications supports SNMP, ICMP, DNS and TCP monitoring; http://tinyurl.com/mulky
- **Soft Perfect Network Scanner**
  - A multi-threaded IP, SNMP and NetBIOS scanner. Very easy to use; http://tinyurl.com/2kzpss
- WinSCP
  - wraps a friendly GUI interface around the command-line switches needed to copy files between Windows and Unix/Linux http://tinyurl.com/yvywqu
- Nagios
  - Highly configurable, flexible network resource monitoring tool http://www.nagios.org
- **Open DNS--**
  - Another layer to block proxies and adult sites; http://www.opendns.com/
- **Ccleaner**
  - Removes unused files and other software that slows down your PC; http://www.ccleaner.com/
- **File Shredder**
  - A fast, safe and reliable tool to shred company files; http://www.fileshredder.org/
- **WinAudit**
  - Audits Windows® based computers. Just about every aspect of computer inventory is examined. Also can automate inventory administration at the network level; http://tinyurl.com/27pk6t

Cain and Abel Local Passwords



Nessus Summary

Tenable Nessus Security Report

Start Time: Finish Time:

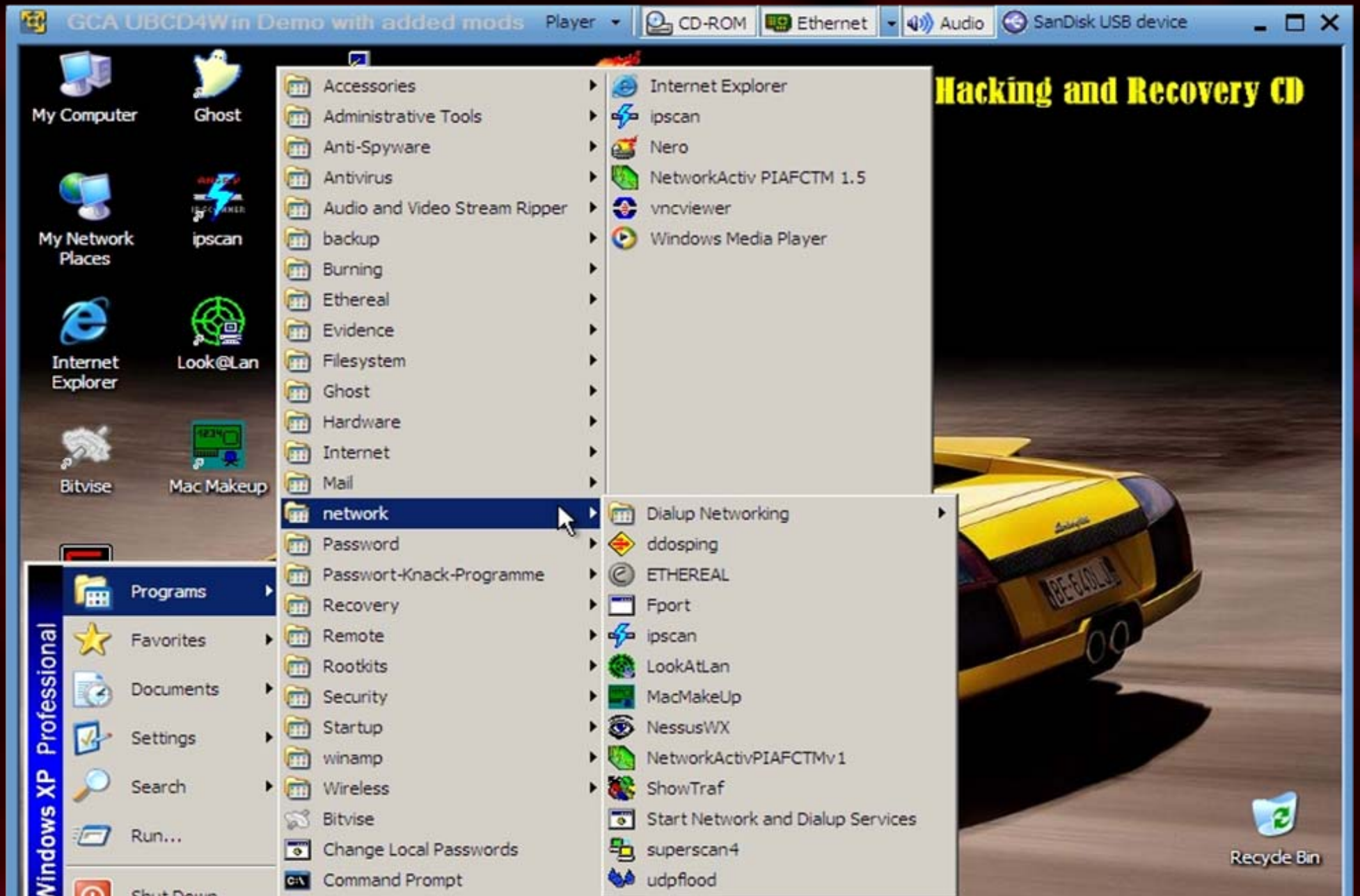
/255.255.255

192.168.22.1	2 Open Ports, 6 Notes, 1 Warnings, 1 Holes.
192.168.22.8	7 Open Ports, 13 Notes, 1 Warnings, 1 Holes.
192.168.22.10	5 Open Ports, 9 Notes, 0 Warnings, 1 Holes.
192.168.22.11	5 Open Ports, 9 Notes, 0 Warnings, 1 Holes.
192.168.22.15	7 Open Ports, 22 Notes, 0 Warnings, 0 Holes.
192.168.22.80	5 Open Ports, 7 Notes, 0 Warnings, 0 Holes.
192.168.22.81	6 Open Ports, 12 Notes, 1 Warnings, 1 Holes.
192.168.22.100	5 Open Ports, 7 Notes, 0 Warnings, 0 Holes.
192.168.22.161	5 Open Ports, 12 Notes, 2 Warnings, 1 Holes.
192.168.22.166	3 Open Ports, 4 Notes, 2 Warnings, 1 Holes.

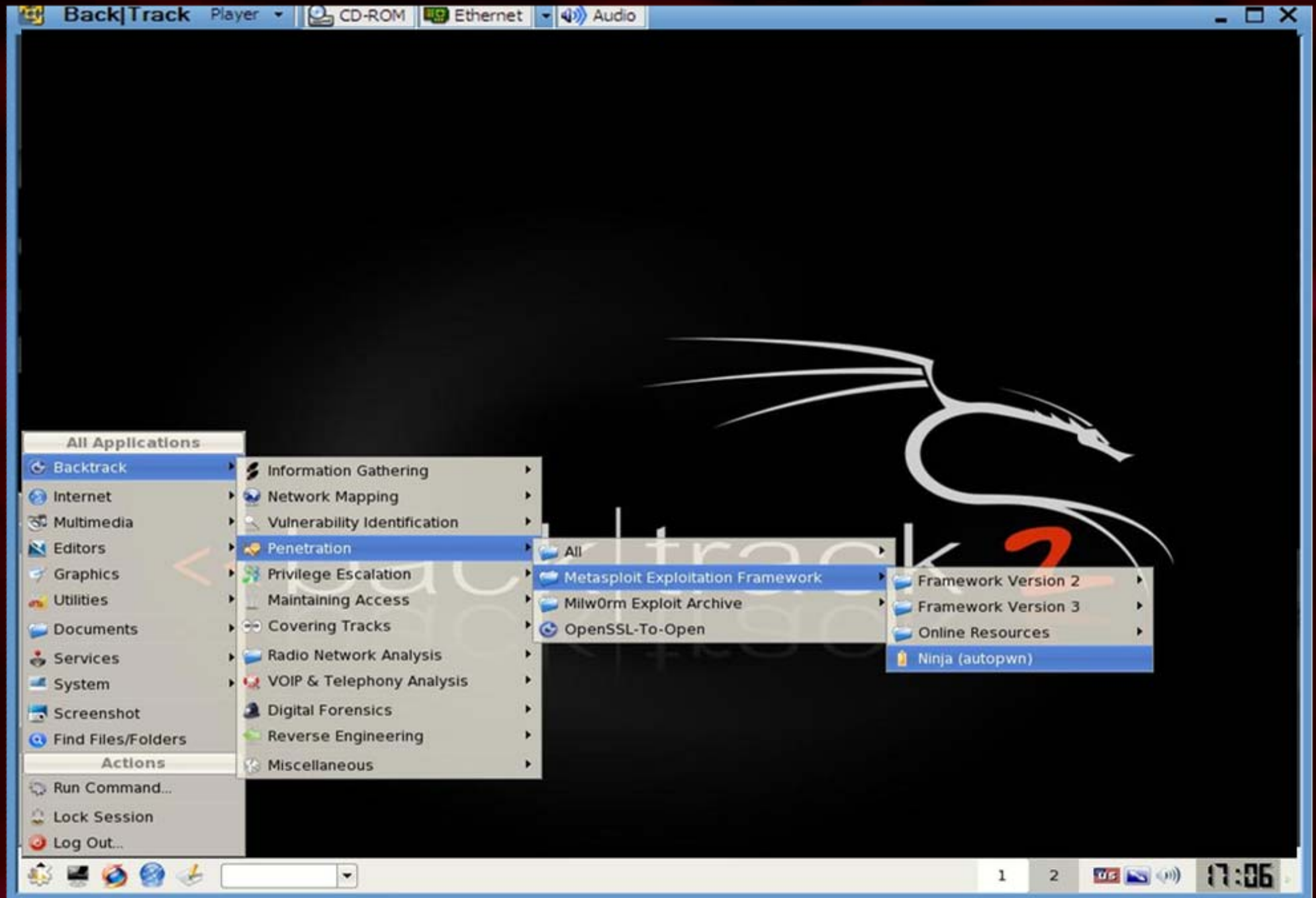
Most Used Tools 2:

- Wireshark
  - Packet sniffer used to find passwords and other important network errors going across network
  - SSL Passwords are often sent in clear text before logging on
  - **http://tinyurl.com/yclvno**
- Metasploit
  - Hacking/networking security made easy
  - http://www.metasploit.com/
- BackTrack or UBCD4WIN Boot CD
  - Cleaning infected PC's or ultimate hacking environment. Will run from USB
  - **http://tinyurl.com/2y2jdj**
  - **http://tinyurl.com/38cgd5**
- Read notify
  - "Registered" email
  - http://www.readnotify.com/
- Virtual Machine
  - For pen testing
  - **http://tinyurl.com/2ghs2e**

UBCD in a VM track that one….



BackTrack in VM U3 Device



Secure Your Perimeter:

- DNS-stuff and DNS-reports
  - http://www.dnsstuff.com http://www.dnsreports.com
  - Test e-mail & html code
  - Web Inspect 15 day http://tinyurl.com/ng6khw
- Shields UP and Leak test
  - https://www.grc.com/x/ne.dll?rh1dkyd2
- Security Space
  - http://tinyurl.com/cbsr
- Other Firewall options
  - Untangle www.untangle.com
  - Smooth Wall www.smoothwall.org
  - IPCop www.ipcop.org

Tools to Assess Vulnerability

- Nessus(vulnerability scanners)
  - http://www.nessus.org
- Snort (IDS - intrusion detection system)
  - http://www.snort.org
- Metasploit Framework (vulnerability exploitation tools) Use with great caution and have permission
  - http://www.metasploit.com/projects/Framework/

Networking Scanning

- MS Baseline Analyzer
  - http://www.microsoft.com/downloads/details.aspx?FamilyId=4B4ABA06-B5F9-4DAD-BE9D-7B51EC2E5AC9&displaylang=en
- The Dude (Mapper and traffic analyzer)
  - http://www.mikrotik.com/thedude.php
- Getif (Network SNMP discovery and exploit tool)
  - http://www.wtcs.org/snmp4tpc/getif.htm
- **SoftPerfect Network Scanner**
  - http://www.softperfect.com/
- HPing2 (Packet assembler/analyzer)
  - http://www.hping.org
- Netcat (TCP/IP Swiss Army Knife)
  - http://netcat.sourceforge.net
- TCPDump (packet sniffers) Linux or Windump for windows
  - http://www.tcpdump.org and http://www.winpcap.org/windump/
- LanSpy (local, Domain, NetBios, and much more)
  - http://www.lantricks.com/

File Rescue and Restoration:

- Zero Assumption Digital Image rescue
- http://www.z-a-recovery.com/digital-image-recovery.htm
- Restoration File recovery
  - http://www.snapfiles.com/get/restoration.html
- Free undelete
  - http://www.pc-facile.com/download/recupero_eliminazione_dati/drive_rescue/
- Effective File Search : Find data inside of files or data bases
  - http://www.sowsoft.com/search.htm

Discover & Delete Important Info

- Windows and Office Key finder/Encrypting
  - Win KeyFinder (also encrypts the keys)
    - http://www.winkeyfinder.tk/
  - ProduKey (also finds SQL server key)
    - http://www.nirsoft.net
- Secure Delete software
  - Secure Delete
    - http://www.objmedia.demon.co.uk/freeSoftware/secureDelete.html
- DUMPSEC — (Dump all of the registry and share permissions)
  - http://www.somarsoft.com/
- Win Finger Print (Scans for Windows shares, enumerates usernames, groups, sids and much more)
  - http://winfingerprint.sourceforge.net

Free Qualys-Style Network Scanner

- Open VAS -- *www.**openvas**.org*
- Get one free check of one public IP address
  - http://www.qualys.com/forms/trials/qualysguard_free_scan/?lsid=7002&leadsource=81053

Application and Data Base Tools

- **AppScan**
  - Web application security testing Security Scanner
  - http://tinyurl.com/mhlqp3
- **WINHTTrack**
  - Website copier
  - **http://tinyurl.com/ypmdq2**
- **SQLRecon**
  - Performs both active and passive scans of your network in order to identify all of the SQL Server/MSDE installations
  - http://tinyurl.com/3bgj44
  - More SQL Tools http://tinyurl.com/3bgj44
- **Absinthe**
  - Tool that automates the process of downloading the schema & contents of a database that is vulnerable to Blind SQL Injection
  - http://tinyurl.com/34catv
- **WebInspect**- SpyDynamics
  - 15 day trial against your web/application servers http://tinyurl.com/ng6khw

Microsoft Tools

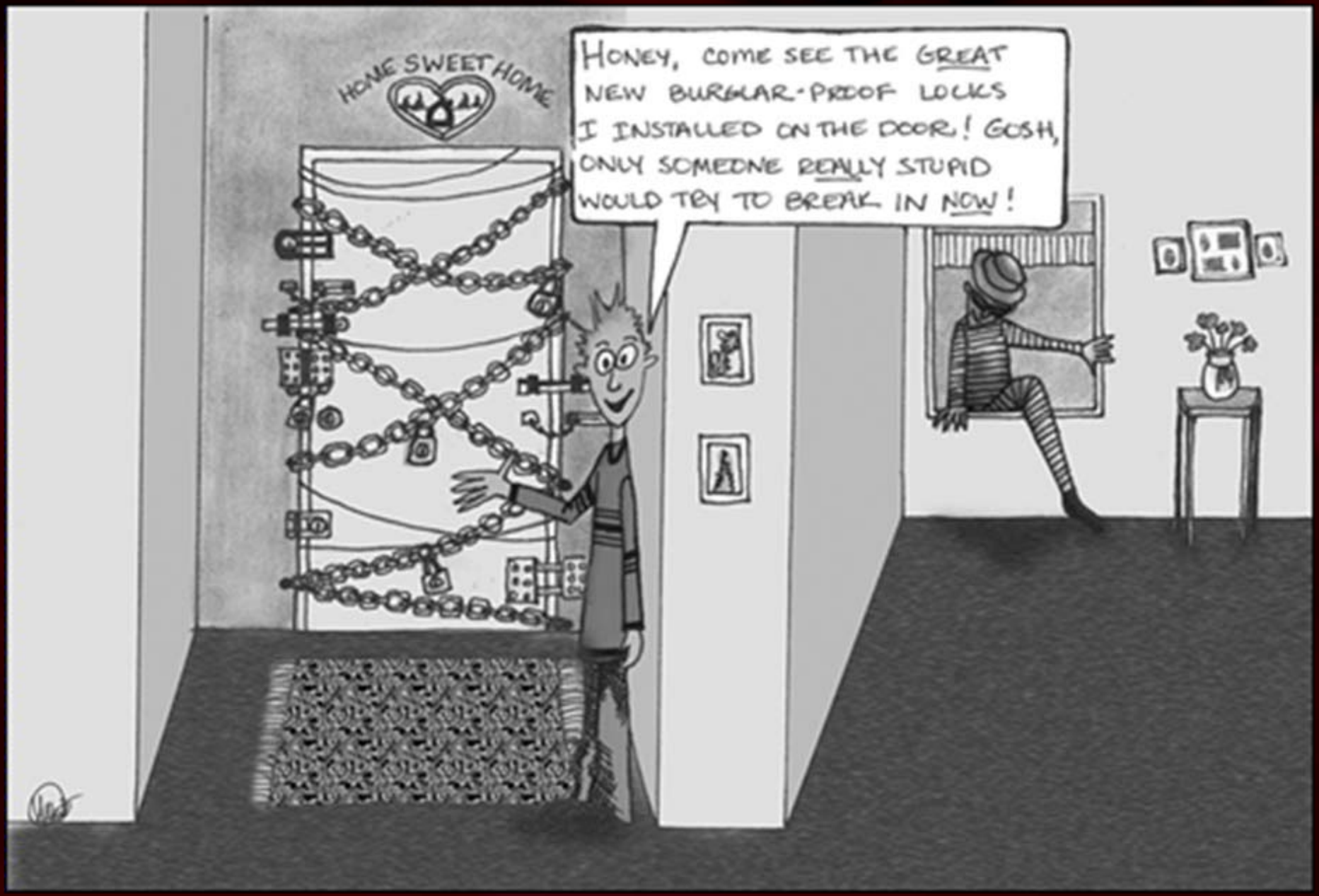
- The GPMC scripts http://tinyurl.com/23xfz3 are made up of a number of individual command-line tools for manipulating GPOs
  - One example cscript.exe "C:\Program Files\Microsoft Group Policy\GPMC
    - Sample Scripts\BackupAllGPOs.wsf" {backupLocation}
- File Server Resource Manager
  - Better reporting capabilities for identifying how storage is being used
  - Define quotas on folders and volumes **http://tinyurl.com/46d4nj**
- Rights Management Services
  - IRM/RMS precise control over the content of documents and helps control unauthorized copies **http://tinyurl.com/rid2**
  - AutoRuns to find what is running on PC
  - NAP to control access to network Need Server 08
  - Steady State
  - ForeFront Paid product but it has been amazing
  - ToySync **http://tinyurl.com/ysc45p**

VM Security

- Hardware-based attestation of hypervisor integrity
- Secure BIOS update mechanisms should be mandatory
- Understand the level at which your hypervisor provider hosts drivers. (Drivers are a weak link in any server security model.)
- Security policies that define the configuration of the hypervisor, access controls, LAN or disk-based sharing, VLAN's
- Policy updates should be tightly controlled
- Restrict the ability to load arbitrary software in security, management, and other critical partitions
- Plan for the single point of failure
- Protect against DoS, no single host OS partition should consume 100% of any resource
- VMs should not share their resources with other hosted VMs
- Inter-VM communication should be configured through tightly controlled, explicit policy

Taken from Gartner's "Secure Hypervisor Hype: Myths, Realities, and Recommendations" (Neil MacDonald, Pub. ID: G00140754, 6 July 2006

What Ports do have Open?



Paid But Recommended Tools

- Spy Dynamics Web Inspect
- QualysGuard
- EtherPeek
- Netscan tools Pro (250.00 full network forensic reporting and incident handling)
- LanGuard Network Scanner
- AppDetective (Data base scanner and security testing software)
- Air Magnet (one of the best WIFI analyzers and rouge blocking)
- RFprotect Mobile
- Core Impact (complete vulnerability scanning and reporting)
- WinHex– (Complete file inspection and recovery even if corrupt) Forensics and data recovery

Shameless Plug

- Presentations on my site located at
  - www.es-es.net
- Check out the presentation given this morning
  - Manage & Secure Your Wireless Connections
  - Also available on my site
- To learn more about GCA (Georgia Cumberland Academy)
  - www.gcasda.org