Audit Like a Hacker

August 23, 2011

ISACA Geek Week

Robert Morella

MBA, CISA, CGEIT, CISSP

Robo_geek@bellsouth.net

About Me

- Been there done that:
- IT Systems
- IT Architecture / Governance
- IT Security
- Cybercrime Investigator
- IT Auditor
- ISACA QAT
- Geek
  - Ham Radio/Electronics/Car Stuff/Etc, Etc.

Career Check: IT Audit

- Food For thought:
  - Define what we do?
  - Redefine what we do?
  - Explain what we do?
  - Future IT Auditors?
    - More hackers or more auditors?
    - Pure Security vs Governance vs both?
    - How we got here?

Why Audit like a Hacker?

- Add Value
- Get Risks Right
- Prove Worth
- Think
- Challenge / Enjoyment

Target Audience

- Internal Auditor
- Security Consultant
- Security Professional

Cyber Threats

- (Insert Standard Cybercrime slide here)
- We already know this
- Exciting Times / Scary times
- Are IT Auditors taking the right steps to properly assess security controls?
- Auditing vs. Penetration Testing vs. Hacking

Time to Redefine what we do?

- Auditor + Hacker =
  - Hackitor™
- Mindset
- Skills
- Imagination

Conventional Audit Approach

- Identify and Rank Risks
- Plan and Establish scope
- Request Information
- Perform testing
- Write it up

Hacker/Attacker approach

- Identify target (and value)
- Evaluate risk of arrest (maybe)
- Testing (lots)
- Define Scope? (unlimited)
- Planning?
- Write it up? (not so gr8)

Big Difference: Scope

- Hacker scope is simple: highest value first
- Everything is in play
- Time: not defined
- Available skills: may vary
- Resources: automation, programming skillz

Nothing is ‘out of scope’ for an attacker

- How to get it right (in 200 hours or less)
  - Forgiveness vs Permission
  - Good findings buys you ‘scope credits’
  - Automation and tools buys you time

Is all hope lost?

- How do you ‘widen scope’
- Old cliché time:
  - Think outside the box
  - Work smarter not harder
- Find Risks nobody else finds
- Find High Risks before anybody else

Failure of imagination

- It's so stupid it just might work vs
  if it works, maybe it was not so stupid
- Translation: An extra hour of brainstorming real vulnerabilities and risks is worth ten hours of compliance testing.
- Attackers spend their ‘every waking hour’ doing this; we need to do more.

Failure of imagination

- Many great failures or tragedies in human history were things people ‘never imagined’.
- Example: Deploy Bulletproof Enterprise Firewall
- Attacker emails malware to CFO
  - Never imagined that!
- Never stop learning; know what’s possible.

How to ‘audit like a hacker’?

- Mindset, scope, approach, imagination
- Some real world ideas?

Lesson One: Computers which don't look like computers

- Hidden computers
- Hidden OS
- Hidden Vulnerabilties
- Hidden Risks

Question: What is this?

Answer: Unix Server

- PowerPC workstation running Linux OS
- Web Server, FTP Server, NFS Server
  - What ports are open?
  - Is the OS fully patched?
  - Are there default passwords set?

Even Better

- Does the device write every scanned document to a hard drive?
- Is it configured to over-write that data?
- Do you have a policy to wipe that drive?

More Boxes Auditors forget about: Phone systems

- Shrouded in mystery
- Owned by separate ‘shadow IT department’
- Hidden in phone room

Phones

- Got voice mail?

- Easy to Spot

Stealth

Phones

- PBX = Server
- Voicemail = Server
- Call Routing = Server
- Call Recording = Server
- Servers
  - Drives
  - OS
  - Vulnerabilities

Phones

- Newer PBX, voicemail servers run Windows
- Older units run Unix
  - What ports are open?
  - Is the OS fully patched?
  - Are there default passwords set?

Phones

- Availability risks vs. security:
- Single spinning hard drives
- Proper power protection / environmental
- Backup/recovery sometimes hit or miss
- Where does dial tone come from?
- Often not well integrated into DR plan

Phones

- Pure security risks:
  - Modems
  - Maybe hackers don’t have these anymore?
  - Service companies have service passwords
  - Do you have a policy to wipe that drive?

VoIP: Better Still

- Whole system runs on Windows server
  - What ports are open?
  - Is the OS fully patched?
  - Are there default passwords set?
- Lots of ‘mad toolz’
  - Voice packets make a sniffer a recorder
  - Insider threat is very real
  - Lots of tools to allow VLAN traversal

More Boxes Auditors forget about: SCADA systems

- Backup power systems
- Also common in manufacturing, nuclear power industry, even onboard ships
- Connectivity?
  - Legacy: Serial (RS-422, RS-232)
  - Modern stuff: Ethernet
- OS:
  - Used to be: UNIX and other RTOS
  - Nowadays: Windows

SCADA: what risk?

- Deepwater Horizon Offshore Oil Platform:
  - Used SCADA to monitor well pressure, gas content
  - Survivor testified that Windows based monitoring system screen would 'go blue‘
  - Monitoring system disabled and ignored due to false alarms

SCADA: what risk?

- Iranian scientists use SCADA to control/monitor enrichment centrifuges
- Stuxnet malware caused 'issues' with both control and monitoring
- Rumored to have delayed Iranian enrichment by 3+ years
- Rumored to have been infected by contractors with USB jump drives

SCADA: Perfect Storm Brewing?

- Typically off-the-shelf Windows hardware
- Ethernet Switches ‘in there somewhere’
- LAN connection to office network
- Remote connection for vendor troubleshooting
- Limited IT or Audit involvement
- Limited IT knowledge, oversight
- Vendors apply updates via USB
- Controls power, heat, cooling and more

Even More Boxes Auditors forget about?

- But Wait, there's more:
- Video Surveillance Systems:
  - Ethernet, Windows PC
- Badge Entry System:
  - Ethernet, Windows PC runs database
  - Access controllers are computers
- Systems Vendors and IT sneaks in
  - Mail room systems
  - Executive 'demo units'

Takeaway: Think about Boxes

- Hidden computers
- Hidden OS
- Hidden Vulnerabilities
- Hidden Risks
- Computers which don't look like computers

Lesson Two: Risk Snooping
AKA: Hacking by walking around

- Get Some Exercise:
- Walk around and look
- Think about risks from roof to basement
- Carry WLAN sniffer: Multi-task!

Hacking by walking around

- Physical Security: got any?
- Open every wiring closet, phone room, equipment room
- Look in the dumpster! (Seriously)
- Where could an intruder plug into your LAN

Takeaway: Hacking by walking around

- Not all security risks come through firewall
- Some have feet, hands, and even guns
- Many IT security risks stem from physical security weaknesses

Lesson Three: Liars, cheats, and your friends in IT

- Full disclosure, I used to be one of them
- What do hackers look like?

Hackers on your payroll?

- Inexperienced System Administrator
- Bored Programmer
- Disgruntled employee
- Even perfect employees make mistakes

True Story: repeated server backup failures

- Unexplained file server backup failures
- Backup jobs would start, then fail
- Logs revealed nothing
- Backup test was performed, and it worked
- Culprit: Computer operations
  - Had reports of slow server performance at certain times of day
  - Were rebooting server to ‘clear’ performance issue (which was the backup running)

IT Mistakes are as bad as hacks

- Same controls that prevent hacks also prevent mistakes
- Often internal systems are judged 'risk free' on private network
- Segregation of duties can help, obviously
  - Often challenging to implement
  - Archive Logs to server controlled by IT Security
  - Review post-incident reports

Case Study: Firewall Hack

- Very well hardened firewall
- eCommerce system
- Simple obvious hack happened
- Spam relayed through an internal host
- Then it stopped

Firewall Hack: Big mystery

- No trace of anything wrong at firewall
- No trace of exploit or even hack attempts
- All controls appeared intact
- One clue: firewall logs were corrupt

Firewall Hack: Mystery solved:

- Firewall Admin made a mistake
- Pushed faulty rule set
- Bot came in, hacked a server
- (former) Admin fixed mistake
- Tried to cover tracks (corrupted logs)

Lesson learned:

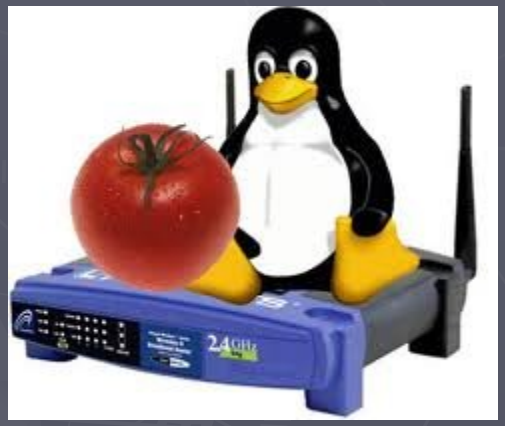
- IT mistakes are just as bad as ‘Hacks’
- Same controls that prevent and detect hacks also prevent and detect IT mistakes
- IT folks are great at hiding their mistakes

Case Study: Big change to big iron

- A certain company is proud of their ability to install Linux on Mainframe VMs (LPARS)
- So proud that they do it for free for their customers
- Big outage to a mission critical mainframe app
- Because Linux OS installed a tiny little software component
  On a test LPAR, on a test system, on a production network.....

Case Study: Big change to big iron

- Software Router



Case Study: Big change to big iron

- Routed ALL traffic from working production app, to a test Linux OS instance
- Vendor did more damage than hacker could
- Again: IT mistakes are as bad as hacks

Some Words of Caution

- How does an attacker exploit a system:
  - Reconnaissance
  - Google for vulnerability discovery
  - Exploit location/creation
  - Execute exploit
  - Take the money (or data) and run
  - Or break things

IT Auditor Approach

- How does an auditor test a system:
  - Recon
  - Google
  - Vulnerability discovery
  - Exploit location/creation (maybe)
  - Execute exploit (No)
  - Take the money (or data) and run (No)
  - Or break things (No)

Those Pesky CLEs

- CLEs
- Career Limiting Events
  - Introducing Malware
  - Breaking production stuff
  - Noisy scripts/Noisy scans
  - Policy

Lesson Four: Poking at the edges

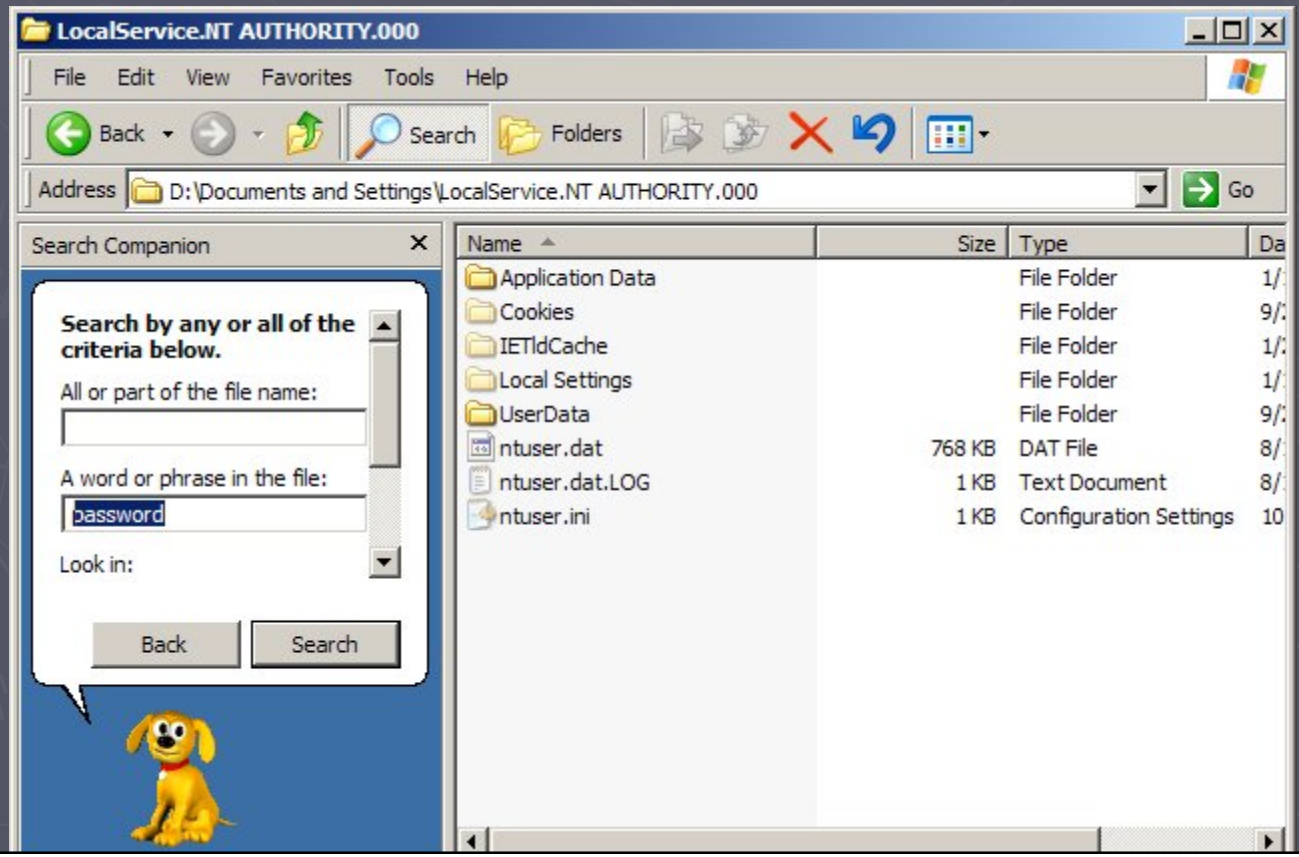
Keys under the mat:

- Windows Shares are information gold
- Searching for passwords
- Searching within files for strings
- Searching for stuff in test/dev scripts
- NFS, FTP, Wiki, SharePoint servers too
- Findings just waiting for you to pick up

Lesson Four: Poking at the edges

Windows search can search within files

Google Desktop allows Google Hacking



Lesson Four: Poking at the edges

Google Hacking is not new :

- But consider what an attacker could do
- Configuration files with passwords
- XML files with connection strings
- HR Data, personal data

- GoogleDork:
  - Someone who leaves data unsecured
- GHDB: Google Hacking DataBase
  - Resource for search strings
  - *www.hackersforcharity.org/ghdb*

Never assume the list is the list

- Always assume *there's another server* that:
  - Is used for test
  - Is used for a vendor app not supported by IT
  - Is being used just to 'play with'
- Sometimes accidental, sometimes not
  - Virtualization makes this herculean feat

Lesson Five: Don’t try this at home?

- No, DO try this at home
  - Build your own IT systems at home
  - Test ideas you don’t have time to test
  - Test real exploits on real servers (yours)
  - Experiment and break stuff
  - Try stupid stuff that just might work.
  - Learn, keep skills sharp
  - eBay is your friend, VMware too

Lesson Six: Making time to do this stuff?

- How do hackers do it?
  Scripts, automated exploits, programs that do the grunt work for them
- How should you do this?
  Scripts, automated audit testing tools, programs that do the grunt work for you
- Understand Limits of automation, but also understand the benefits

Top Hackitor Tool: Scripting

- Unix auditing scripts
  - http://boran.com/audit
- Firewall auditing scripts
- Database Auditing: scripts, tools, etc
- 'Toolz' too, but with caution

Top Hackitor Tool: Scripting

- Example:
- Simple batch file for SQL server to test for blank admin password
- Uses OSQL.exe DOS shell uitility
  - osql –L <<lists all servers on network
  - osql -S server1 -U sa –P
  - osql -S server2 -U sa –P
  - osql -S server3 -U sa –P

More automation means more time

- More Time to:
  - Think outside the box.
  - Think about boxes you forgot about
  - Think about risks you never imagined
  - Walk around and look for risks

Summary:

- Insider threats:
  Key Takeaways:
  - Dig deeper, poke around the edges of a system: audit like a hacker
  - Question your assumptions, and trust, yet verify what IT tells you
  - IT Mistakes are Just as Bad as Hacks, and Often worse, and harder to spot
  - Automation gives you the time to do more value-added manual work

Questions

- ?

Thanks!

Audit Like a Hacker

August 23, 2011

ISACA Geek Week

Robert Morella

MBA, CISA, CGEIT, CISSP

Robo_geek@bellsouth.net