

# Security Forum

## Practical Intrusion Detection Tips

and

## What Hackers Have Up Their Sleeves Now

Brad C. Johnson SystemExperts  
Corporation

## Agenda

---

- Quick assessment of the state of intrusion detection (ID)
- Overview of why intrusions are successful despite ID systems and the relationship to hacker efforts
- Cover primary intrusion areas, tools, and techniques hackers use
  - Web servers
  - Web applications
  - Wireless 802.11b (access points)
  - Modems

## Intrusion undetection

- Typical ID issues for host and network intrusions
  - Monitor system and application log files and events
    - ManTrap, ManHunt, Cisco IDS, RealSecure, NFR, Tripwire, StormWatch, Snort, Intruder Alert, Shadow, Dragon, etc.
    - ■ Use one!
  - Alarm and event generation
    - e.g., email, page, voicemail, carrier pigeon, etc.
  - Firewall filters and router configurations
    - SurfControl, Cisco PIX, CyberArmor, McAfee, StormWatch, CheckPoint, Netscreen, SecurellS, StoneGate, WatchGuard, ZoneAlarm, etc.
    - ■ Use One!

## Intrusion awareness

- There are dozens of intrusion detection tools to choose from
- Virtually none of them will help you with anything but generic problems (e.g., port scans, block ports/services)
- There are many tools, sites, conferences, and educational classes dedicated to intrusion detection and yet
  - a) most sites have little to no functional ID services
  - b) many intrusions are successful and most are not detected....WHY?
- Site specific intrusion detection systems require significant:
  - Hands-on configuration
  - Development
  - Expertise
  - Iterations of testing to figure out
    - a) what's normal
    - b) reasonable thresholds

## What does the hacker know?

---

- Most sites are not instrumented for anything but obvious intrusion fingerprints
- There are dozens of very easy to use tools that give accurate profiles of potential and existing vulnerabilities
  - Many of these tools have intrusion detection avoidance mechanisms built into them: e.g., URL encoding, packet fragmentation, protocol tunneling
- Most organizations are not in touch with public domain tools, techniques, and initiatives
  - They don't realize how easy many intrusions are

## Being in touch with hacker news

---

- How many have heard of rootkits?
  - Can you think of one file on any distribution? What does it do?
- How many have a web site?
  - Tell me what Whisker does. How does it work?
- How many have an 802.11b access point?
  - Tell me what MiniStumbler is. How does it work?
- How many have any modems?
  - Tell me what THC-Scan is. What are its good and bad points?

## Being in touch with hacker news answers

---

- Name one exact file on any distribution
  - \_root\_040.zip: NT: deploy.exe, \_root\_.sys
  - rootkitLinux.gz: Linux: netstat (hides activities )
  - rootkitSunOS.tgz: SunOS: fix.c (change checksums)
  - rootkit.zip: UNIX: es (ethernet sniffer), z2 (remove log entries)
  - fbrk1-imps.tar.gz: FreeBSD: sizer (change file size)
  - sol24.zip: Solaris: psrace.c: set UID to 0
- Tell me what Whisker does. How does it work?
  - Looks for well-known Web server distribution exploits and simply makes a series of GET requests for specific file names

## Being in touch with hacker news answers

---

- Tell me what MiniStumbler is. How does it work?
  - Program to find 802.11b access points and it runs on a handheld PocketPC
    - other programs include Kismet, Wellenreiter, THC-WarDrive
  - It sends out probe-request packets (management packet type 00 sub-type 0100) and logs the response
- Tell me what THC-Scan is. What's good and bad?
  - The Hacker's Choice (phone) Scanner: i.e., phone phreaking, model dialer: other programs include Toneloc and SandStorm
  - Does a great job against very large sets of numbers, doesn't try to be too smart, but has a limited number of target devices that it can automatically detect

## Common intrusion detection mistakes

- Trying to get from having nothing to being done in one step
- Assuming you know what's normal
- Attempting to solve everything instead of the obvious (e.g., low hanging fruit)
- Reading endless publications or attending your umpteenth class on intrusions and yet
  - Still having the same types of intrusion problems
  - Still having very little intrusion detection capabilities
  - Really not having any idea what's in the public domain for your use and education

## Where do successful intrusions happen?

- Web Servers
- Web Applications
- Wireless Infrastructure
- Modems
  - This is where it all started
  - The tenet of most hacking efforts are
    - a) getting something for free
    - b) showing off and embarrassing somebody else
- Email (trojans, worms, etc.)
  - I'm not going to talk about this ☹️
    - ■ but install a virus detector on EVERY system!

## Thinking about intrusions

- **Intrusion Area**
  - Each area has it's own issues relating to detection, owners, configurations, best practices
    - e.g., Web server is separate from FTP/TELNET which is separate from firewalls which is separate from routers, etc.
    - ■ put major services on their own system
- **Typical Problems**
  - A small amount of research will reveal common problems that everybody is dealing with
- **Methodology**
  - Figure out how to detect a problem and then recreate it in your environment: automate this if you can
- **Practical Tips**
  - Apply Occam's razor: the simplest approach or observation is likely to be the best one (i.e., conquer and move on)

## Web servers

- **Intrusion Area**
  - Server deployment: every Web server comes with its own set of configuration, deployment, setup, security, and problems!
- **Typical Problems**
  - Insecure package contents
  - Insecure default options/settings
    - ■ check every possible configuration setting!
- **Methodology**
  - Very easy: cut/paste a well-known URL
- **Practical Tips**
  - ■ Use "CGI" scanning tools: e.g., whisker or Nessus web tests
  - ■ Check your Web server logs for well-known problematic server-side files and programs

## Whisker: CGI scanner

---

- Scans for well-known exploitable files
- Uses the server type to be selective
- Can determine the OS type to be more selective
- Options to by-pass IDS using URL encoding
  - `/cgi-%62in/ph%66` instead of `/cgi-bin/phf`
- Looks for files in many different directories
  - Let's take a closer look at how robust this tool is

## Whisker cont.

---

- Directories searched (125)
  - `/cgi-bin`, `/cgi-local`, `/htbin`, `/cgibin`, `/cgis`, `/cgi`, `/wwwthreads`, `/scripts`, `/app*`, `/backup*`, and other common root directories
- Log directories searched (85)
  - `/cache-stats`, `/log*`, `/scripts/weblog`, `/stat`, `/wwwstatus`, `/server_stats`, `/wusage` and other common log directories
- Files searched (there are hundreds)
  - `iissamples/exair/howitworks/Codebrws.asp`
  - `iissamples/query.asp`, `iisadmpwd/aexp4b.htr`
  - `tools/newdsn.exe`, `cgi-win/uploader.exe`
  - `testcgi.exe`, `cgitest.exe`, `webdist.cgi`, `pfdisplay.cgi`
  - `php.cgi`,

## Web applications

- **Intrusion Area**
  - Internet applications: most programs have not been either developed or tested for the insecure, untrustworthy, anonymous network world
- **Typical Problems**
  - Server doesn't validate incoming data
    - ■ Code should validate any incoming parameter data (even if it's coming from another "safe" function!)
  - Design assumes client won't change data
  - 1-time authentication and authentication implies authorization
- **Methodology**
  - Moderately difficult: Change data on the client and send it back: e.g., cookie, URLs, environment variables, forms, IDs
    - let's talk about this...
- **Practical Tips**
  - ■ Understand and/or use tools designed to find these types of problems: e.g., WebSleuth
  - ■ Scan Web application logs for "unexpected" errors: e.g., references to odd locations in the file system, invalid data, special characters

## Wireless infrastructure

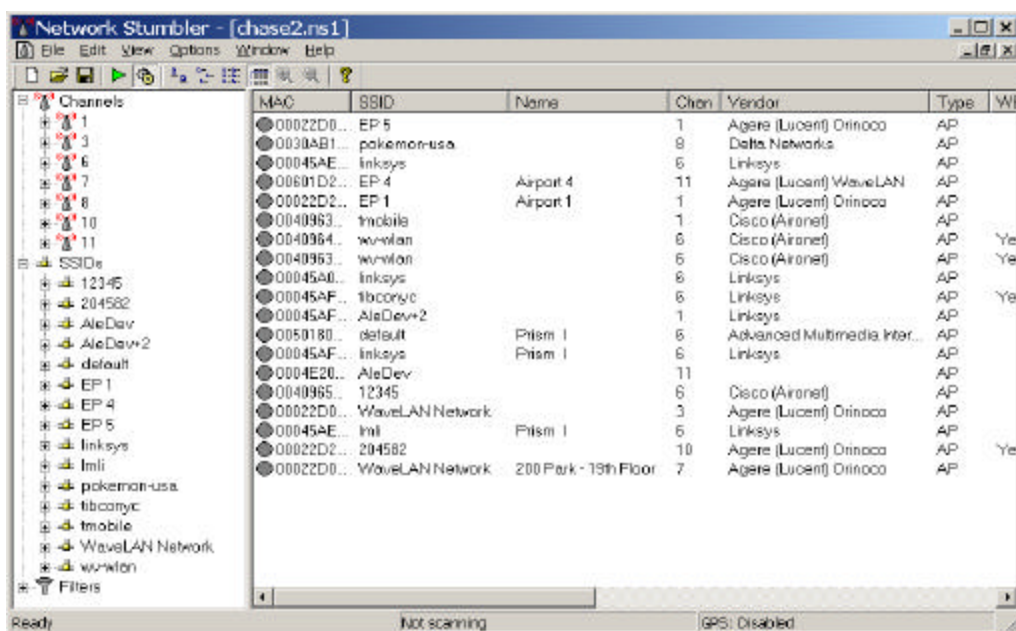
- **Intrusion Area**
  - 802.11b: wireless technology is often not installed by the IT/Security team, it's difficult to chart where the radiation pattern goes, and almost all access points come configured in their least secure setup
- **Typical Problems**
  - The access point is accessible from unwanted places
  - Default configurations allow access to your internal network
- **Methodology**
  - Moderately easy: Install and use "war driving" programs and mapping software
- **Practical Tips**
  - ■ Install and use "war driving" programs and mapping software: e.g., NetStumbler or MiniStumbler (free), Network Sniffer (more than \$10K), AiroPeek (a few \$K)

## NetStumbler: access point finder

- Windows utility for “war driving” – that is, finding Access Points (AP)
- Gives critical AP information including
  - MAC address, SSID, network name, broadcast channel, vendor, WEP flag, GPS coordinates (if attached to the serial port), and all sort of other stuff...
- MiniStumbler available for handhelds!

## NetStumbler cont.

60 seconds on one corner in a major city



# NetStumber cont.

## ■ MiniStumber for handhelds

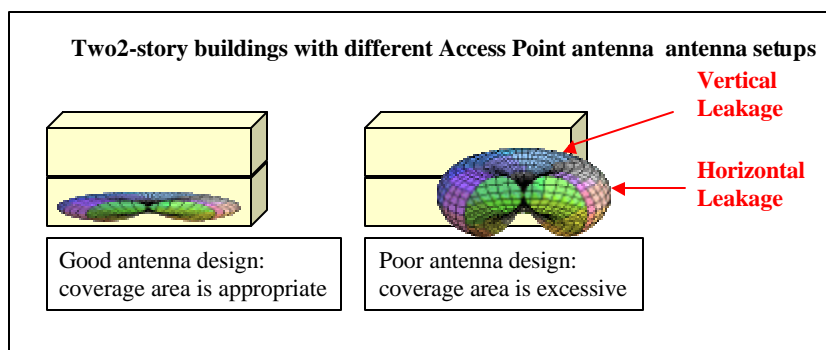
MAC	Chan	SSID	SNR
0090D100BF6C	11	WLAN	5
0090D100B93B	11	WLAN	
0090D100CC6F	11+	WLAN	10
0090D100BEC5	6	WLAN	
004033AFC3D1	10	Wireless	
0090D100CAA5	11	WLAN	17
0090D100BE02	1	WLAN	



# NetStumbler cont.

## ■ Why is NetStumbler successful?

- Poor antenna selection
- Access point is in broadcast mode and responds to probe-request packets



Antenna Design Considerations

## Other wireless tips

- ■ Make sure your policies have 802.11b specific requirements
- ■ Create a short “Things To Do” list for setting up an AP
- ■ Use WEP
- ■ Change the SNMP community string
- ■ Change the SSID (network name)
- ■ Change the default admin password
- ■ Disable broadcast SSID
- ■ Consider disabling DHCP
- ■ MAC stuff
  - use it
  - have a cron job to dump the arp cache and look for vendor MAC addresses that aren't yours!

## Modems

- **Intrusion Area**
  - Modems: phone based services exist for many different types of devices and programs and are the least tested aspect of almost every company
  - ■ inventory all of your modems
- **Typical Problems**
  - Bypass almost all other security mechanisms
  - Phones are usually not part of intrusion detection, event management, SNMP, or audit services
  - Phone based testing programs are incomplete and generate false positives and negatives

## Modems cont.

---

### ■ Methodology

- Very easy: insert phone list or range into program: when it finds a connection, most are fairly easy to just use (e.g., router, printer)
- Very hard: if you want fine grained accurate data, you have to monitor (baby-sit) the process and inject data, common sense, and expertise
  - let's talk about this...

### ■ Practical Tips

- ■ Use war dialing software to survey your phone space: e.g., The Hacker's Choice (THC-Scan – free), SandStorm PhoneSweep (many \$K to tens of \$K)

## Closing thoughts

---

- ■ Investigate the common problem areas first
  - Web applications, modems, web servers, wireless 802.11b, and email based virus and trojans
- ■ Add periodic assessments of these key areas
- ■ Analyze your environment to figure out what's normal
  - This is the first thing you HAVE to do, it's the hardest part but generates the most practical issues and questions you'll need to understand
- ■ Use ID tools to monitor the system that connect to ISPs and partners
- ■ Build burglar alarms for events you're specifically concerned with or have been the target of
- ■ If you're ever interested in prosecuting, you need to contact agencies BEFORE it happens so you know what you're actually supposed to do and collect
  - Remember that ID and incident response are really two different things: try and handle them separately but cooperatively AND that no matter what you do, some intrusion will be successful anyway

## References

---

- White papers

- <http://www.systemexperts.com/literature.html>

“Wireless 802.11 LAN Security:  
Understanding the Key Issues”

“Internet Penetration Testing:  
A Seasoned Perspective”



**Brad C. Johnson**  
**Vice President**

**[Brad.Johnson@SystemExperts.com](mailto:Brad.Johnson@SystemExperts.com)**

**401-348-3099 direct**

**401-348-3078 fax**

**978-440-9388 main**

**[www.SystemExperts.com](http://www.SystemExperts.com)**