

# Scanning for Dollar\$

Scanning for fun and profit

**Bill Hayes**  
**Omaha World-Herald Company**

# Ethical scanning



- Scan only for legitimate purposes
- Written permission
- Auditable process

# Scanning uses

- Network Discovery
- OS Fingerprinting
- Vulnerability Assessment
- Penetration Testing
- Remediation
- Certification
- Change Control



# Scanning Platform Considerations



- Many scanning tools originally developed for Unix/Open source
- Ports to other OSes may not be available or have the same functionality
- Moral: Learn to love Penguins

# Network Discovery

- Identify network hosts and devices
- Port Scanners predominate
- Nmap  
(Unix/Linux/Windows)
- SuperScan (Windows)
- NetworkView (Windows)



# OS Fingerprinting



- Identifies Operating Systems through unique TCP packet characteristics
- See Fydor's OS Fingerprinting papers at <http://insecure.org/>

# Service Identification

- Services can be identified from open ports and banners
- Some scanners are used to recon/exploit open services like THC-Amap
- Open share scanners like Legion and Systemals ShareEnum
- FTP scanners used by Warez script kiddies



# Service Banners

- Service Banners identify service and frequently operating system
- Example: “220 unknown FTP server (SunOS 5.8) ready”
- Can be misleading -- patches do not always update a service.
- Numerous banner grabbing scripts.



# Vulnerability Scanners

- Examine hosts and network devices to determine flaws
- incorrect configurations
- unpatched services
- Nessus premier scanner
- SATAN derivatives (SARA, SAINT)
- Core-Impact, Retina, ISS-Scanner, etc.



# Banner Reading

- In “Safe mode” many vulnerability scanners use data returned from service banners to determine a vulnerability
- Problematic because service banners can be inaccurate. Patches may not update banners.

# Service Testing

- Vulnerability scanners may test services to fingerprint service or identify a vulnerability.
- Testing for a vulnerability or fingerprinting it may cause the service to lock up. Microsoft Clustering Service often dies.

# “Safe” vs “UnSafe”

- Safe tests do not actually test for a specific vulnerability. Performs indirect tests such as banner grabbing.
- UnSafe tests actually run an exploit against a service. This could cause the service to fail or leave the system in an unstable condition.

# Application Scanners

- Test application security
- Http and SQL scanners
- WebInspect (SPI Dynamics)
- AppScan (Scantum)
- Nikto (Open Source)
- NGS SQLscan



# Penetration Scanners

- Canvas
- Core Impact
- Metasploit



# Remediation

- Scanning used for patch remediation
- HFNetChk Pro
- Retina
- Nessus/Thunderbolt

# General References

- <http://sectools.org/>
- <http://www.hackingexposed.com/tools/tools.html>
- <http://www.sysinternals.com/NetworkingUtilities.html>
- <http://insecure.org/nmap/nmap-fingerprinting-old.html> and  
<http://insecure.org/nmap/osdetect/>



# References (Port Scanners)

- **Angry Scanner (Freeware Windows) -**  
<http://www.angryziber.com/ipscan/>
- **Foundstone SuperScan (Freeware Windows) -**  
<http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/dsscan.htm>
- **Nmap (Open Source - UNIX/Linux/Windows) -**  
<http://www.insecure.org/nmap>
- **NetworkView (Shareware Windows - Network Discovery/Admin) -**  
<http://www.networkview.com>

# References (Vulnerability Scanners)

- **Nessus (Freeware/subscription) - <http://www.nessus.org>**
- **Retina (Commerical \$\$\$)-  
<http://www.eeye.com/html/Products/Retina/index.html>**
- **MBSA (Microsoft Windows only) -  
<http://www.microsoft.com/technet/security/tools/mbsahome.msp>  
x**
- **Axman (Open Source) ActiveX fuzzer -  
<http://www.metasploit.org/users/hdm/tools/axman/>**

# References (Application Scanners)

- **AppScan (Web Commercial \$\$\$) -**  
<http://www.watchfire.com/products/appscan/default.aspx>
- **Nikto (Web Open Source) -**<http://www.cirt.net/code/nikto.shtml>
- **WebInspect ( Web Commercial \$\$\$) -**  
<http://www.spidynamics.com/products/webinspect/>
- **NGSSQuirrel ( SQL Commercial \$\$\$) -**  
<http://www.nextgenss.com>
- **THC-AMAP (Open Source UNIX/Linux) -**  
<http://thc.segfault.net/thc-amap/>

# Scanners (Open Shares)

- Legion Scanner -<ftp://ftp.technotronic.com/rhino9-products/legion.zip>
- Systemal ShareEnum -  
<http://www.sysinternals.com/Utilities/ShareEnum.html>