



O-ISC '07
Ohio Information Security Conference

Exploits

Analysis and Assessment

Deral Heiland
Layered Defense Research

Layered Defense ResearchSM

Speaker Biography



Deral Heiland

Employed as Senior Information Security Analyst by a fortune 500
Global IT outsourcing company,

Founder of Layered Defense Research

&

Director of Ohio Information Security Forum

- Threat ,Vulnerability & Risk specialist
- I have a passion for security
- I Love sharing security with others
- Believe the greatest weapon in the hands of security professional is knowledge

Layered Defense ResearchSM

Why This Subject

- Prevent being caught blind
- Over or under reaction is very costly
\$\$\$\$\$\$
- Technology can be a great tool, but it is not the silver bullet
- Security teams are not evaluating exploits until its to late
- Encourage you to go further and to look deeper

- Insight into the world of exploitation
- Knowledge gathering
- Assessment from identification to mitigation



O-ISC '07
Ohio Information Security Conference

Exploits

Layered Defense ResearchSM

■ Buffer overflows

- CVE (Common Vulnerabilities and Exposures database) count 2006: 584
- Heap overflows
- Stack smashing

■ Format string

- CVE count 2006: 65
- Not normally seen in exploits(viruses, worms & malware)
- Rare ?

■ Integer overflows

- CVE count 2006: 96
- Commonly related to buffer and heap overflows

■ Off by one

- CVE count 2006: 14
- Generate DOS (denial of services) condition

Some More Exploit Types

- SQL injection
- Cross site scripting
- Directory traversal
- Information leakage

Exploit vectors

- Network system
- Protocol
- O/S
- Web systems
- 3rd party application

- Who is creating them ?
 - Criminals
 - Researchers
 - Hackers

- What are their goals & motivation ?
 - Knowledge / Learning
 - Fame
 - Financial
 - Criminal activity (Organized Crime)
 - white hat (Pay for exploits)
 - Remember a remote exploit without user intervention is the holy grail



O-ISC '07
Ohio Information Security Conference

Researching Information

Layered Defense ResearchSM

■ Internet

- Blogs
- Research white papers
- BugTraq
- Hacker sites (Not from your corporate network)

“If you want to know whats going on in HELL, sometimes you need to dance with the Devil”

-Anonymous

■ Conferences

- Professional
- Hacker (Insight into cutting edge security research)
 - Blackhat - Las Vegas
 - Defcon - Las Vegas
 - Shmoocon - Washington DC
 - CCC 23C3 - Germany
- If you cannot attend, obtain the presentations on-line and read them.

Web Sites

- www.securityfocus.com/archive/1
- seclists.org/fulldisclosure/
- seclists.org/dailydave/
- www.frsirt.com/english/
- secunia.com/
- cve.mitre.org

Web Sites

- Phrack magazine (For the hard Core)
- www.nologin.org/
- www.milw0rm.com
- doc.bughunter.net/
- www.metasploit.com
- elsenot.com/index.php?title=Windows_ElseNot_List?
- www.offensivecomputing.net/



Determining Risk & Scaling Reaction

- A very focused form of risk assessment but follows the same principles of risk assessment.
- Focus on a specific threat and a specific target and follow it through from identification to mitigation

■ Threat Identification

- Vendor
- Hacker talk
- You may discover it yourself

■ Asset Identification

- Details are normally lacking
- Identify systems that could be impacted by the threat
- Perfect detail is not always required
 - What is percentage of the foot print that could be impacted ?
 - What makes up our Tier one systems ?

■ Probability

- Requires close analysis of the threat
- This is a moving target always changing
- This is the fun stuff

■ Impact

- Low, Medium & High
- Determine the impact to the asset if the threat under review would occur

■ Mitigation

- Cost
- Impact
- Vendor patches
- Network filters / firewall changes
- Disable vulnerable features and services
- 3rd party patches “ NO”



Case scenarios

A Look at Worm History

Case 1 MS03-039 Blaster 2003



- Heap Overflow Vulnerability
- I think everything is compared to BLASTER now
- How were we each affected ?
- Why were we caught off guard ?
 - Blaster was not a surprise
 - Source code was available for several weeks prior to the outbreak
 - The exploit code was demonstrated to various IT departments within my company, but only a few took it as a serious threat

Case 2 MS04-011 SASSER



- Buffer overflow vulnerability
- W2K XP
- Proof of concept code was also available before the worm hit
- I demonstrated this code also “ They took me more serious this time”
- Sasser built in FTPD was vulnerable to a stack based buffer overflow

Case 3 MS05-039 ZOTAB



- Buffer overflow vulnerability
- Only W2K was remotely exploitable
- Proof of concept code was also available before the worm hit
- At this point there was no need to demonstrate code

Case 4 MS06-040

- Stack based buffer overflow
- W2K & WINNT was remotely exploitable
- Proof of concept code was also available
- Microsoft did say that targeted exploits were being used prior to exploit code being publicly available



O-ISC '07
Ohio Information Security Conference

Conclusion

Layered Defense ResearchSM

Conclusion

- All reported/discovered vulnerabilities need to be tracked and assessed from discovery to mitigation
- Over reaction or under reaction can be costly “knowledge prevents this”
- A good patch management team is vital to a healthy company
- A good exploit/vulnerability assessment team will reduce risk and cost
- So dive in !

Questions & Answers

Contact info
dh@layereddefense.com