CERIAS

the center for education and research in information assurance and security

Risk Assessment Applied

A Living Lab Project

Lindsay Friddle | John Wikman, Purdue School of Engineering and Technology, IUPUI Mentor: Connie Justice, Purdue School of Engineering and Technology, IUPUI

WHAT

- •Risk assessment is the first step in risk management, a structured approach to risk mitigation
- Strategies
 - Transfer the risk

2008 - EBB-A4C - Risk Assessment: A Living Lab Project - Connie Justice - RMPL

- Avoid the risk
- Reduce negative impact of riskevents
- Accepting consequences of risk
- •Applied to a computer network, risk assessment entails the building of a network map, including a list of all resources attached to the network
- •From that map, risks (such as open ports, gaps in the firewall, etc.) can be found and managed

WHY

- Accurate risk-assessment is first step toward safeguarding the network
- Also provides current machine inventory
 - OS version
 - Patch levels
 - Software
 - Open ports by machine
 - Running services



- Use dedicated assessment machine (usually laptop for portability)
- Software tools
 - •GFI Languard
 - Nessus
 - •iInventory
- •All scans are safe-scans--no vulnerabilities are exploited

) 😅 🥔 🔃 🔍 , · My network scan (13:14 29 Feb) ilnventory **LANauditor®** 192.168.3.13 General 192.168.3.100 Scan network IN-CIT-RAL-01 44 Computer records (4) ■ Windows PC (4) Registered User Audit network assets Operating System OS Serial Number 76487-641-2994605-23948 Agent builder wizard Latitude D530 PC Serial Number Import audit data Intel(R) Core(TM)2 Duo CPU T7250 @ 2.00GH. CPU 1 Serial Number GenuineInte Resolve software Standard CPU 1 Speed 1994 MHz CPU 1 Class Model 15, Stepping 13 General Show agent config CPU 2 Type Mac CPU 2 Serial Number ■ Windows CPU 2 Vendor GenuineInte CPU 2 Speed CPU 2 Class Model 15, Stepping 13 Win32 logins Total Hard Disk Space 75.53 Gbytes Win32 modem IN-CIT-RAL-01 Database (JET) Example

WHEN

- Each company should develop a policy
 - •Time-based (i.e. once per year, every six months, etc.)
 - •Event-based (i.e. adding new server, add new desktop machine)











