JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Corporate Policy Requirements

VULNERABILITY MANAGEMENT

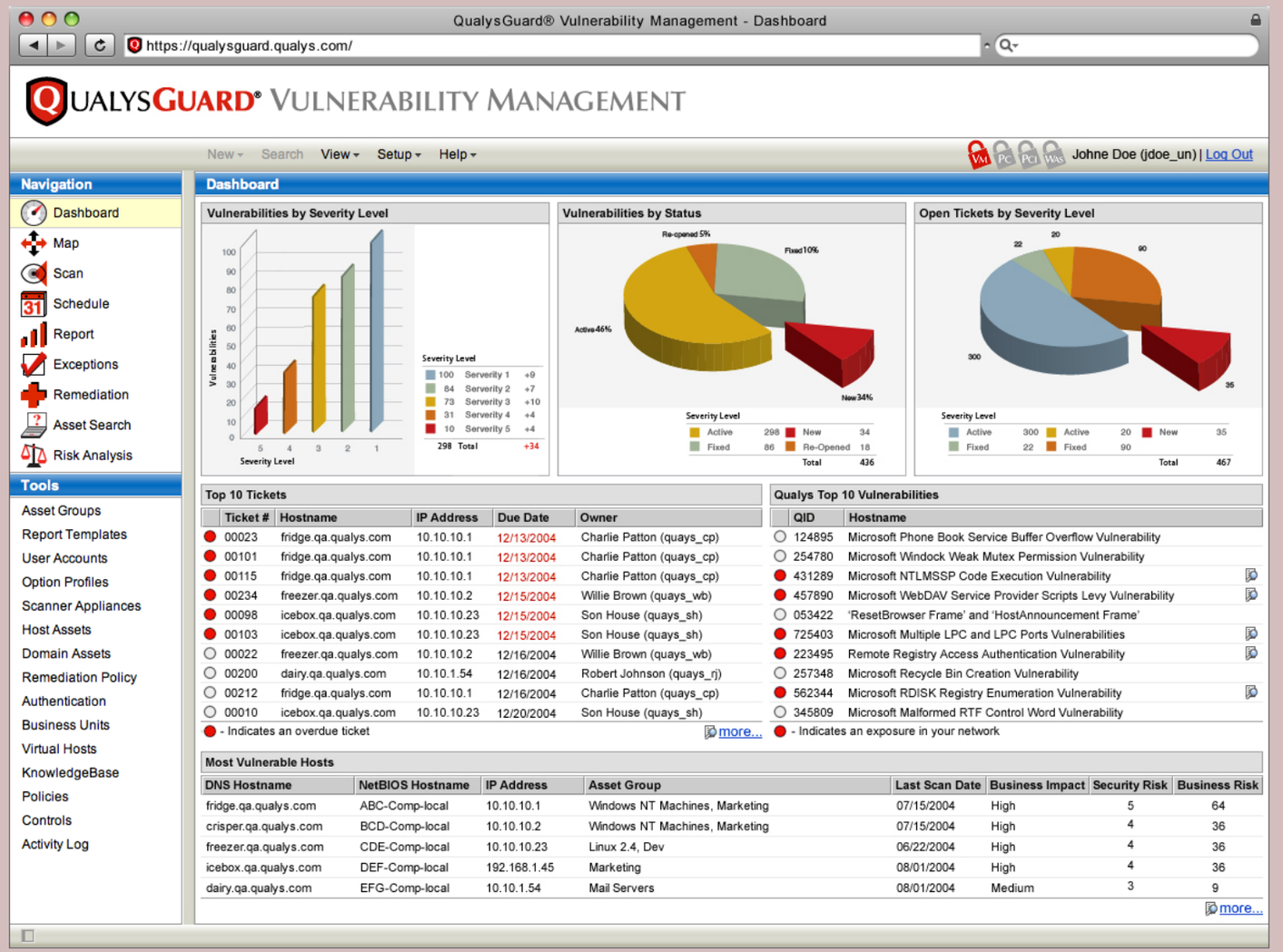
Corporate Policy Requirements

- Laws and regulations that require vulnerability management programs (like PCI DSS, and FISMA) don't apply to all companies
- But…vulnerability management is still very important to them as a key component to security
- Therefore…organizations can (and do) require scanning under their own corporate policies

Scan Targets

- What systems do you want to be covered by your scans?
- Do you scan all systems or just *critical* assets?
- Scanning tools like *QualysGuard* can be used to build your asset inventory automatically
- Admins then take that information and classify the systems as critical or non-critical

QualysGuard Vulnerability Scanner

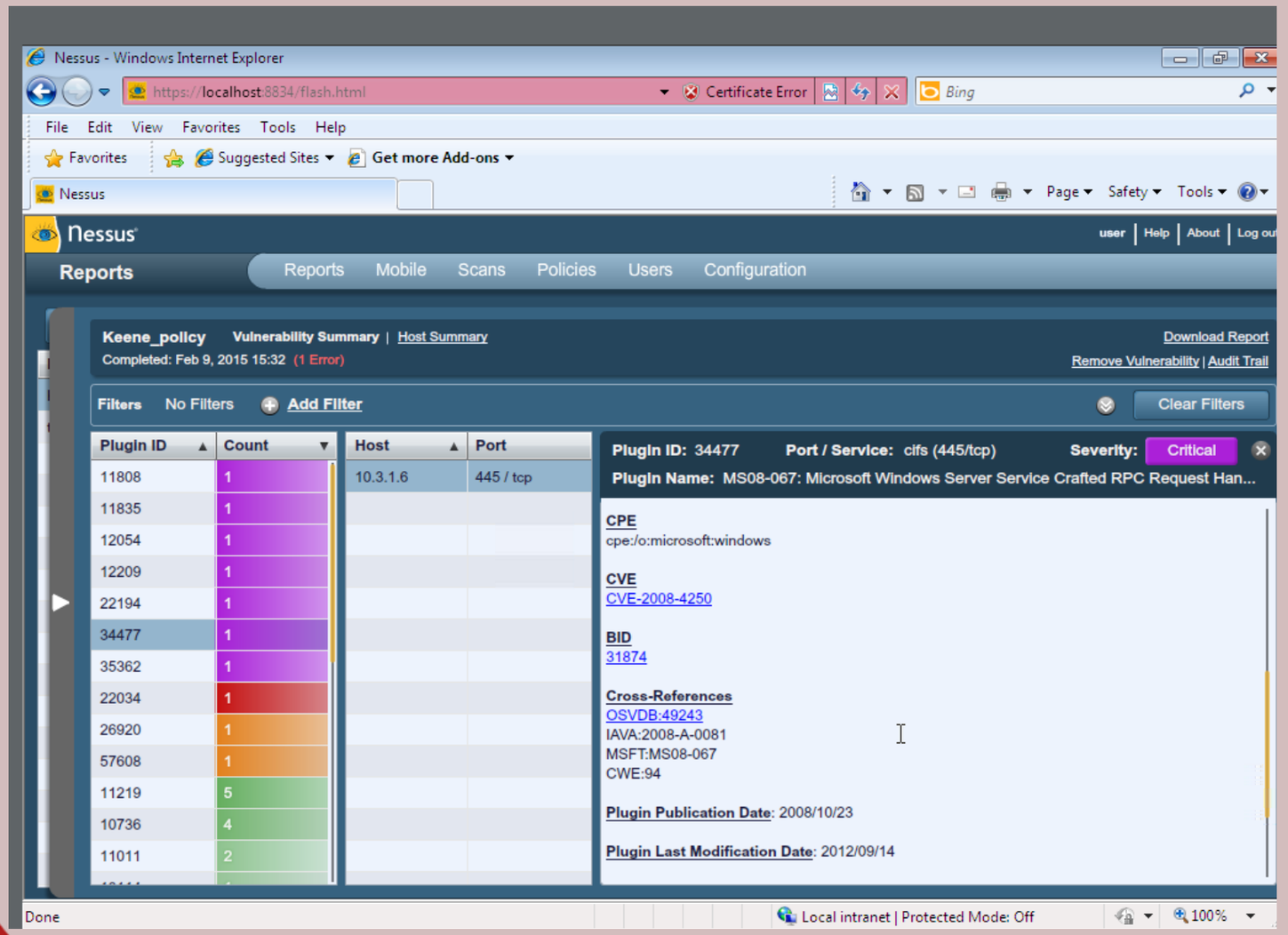


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Scan Frequency

- How often do we scan the systems?
- Schedule determined by your goals to meet security, compliance, or other business requirements
- Automated email reports or alerts can be configured, as well
- For example, the Nessus scanner allows you to setup daily, weekly, monthly, or other scheduled scans by date/time

Tenable's Nessus Vulnerability Scanner



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Scan Frequency Considerations

- Organizational risk appetite
  - How much time between a new threat and a scan?
- Regulatory requirements
  - Do you fall under FISMA or PCI DSS?
- Technical constraints
  - Network may not support scanning everything
- Business constraints
  - Do you have to avoid high business activity times?
- Licensing limitations
  - Scanners can control how many concurrent scans can be performed through licensing

Best Practices For a New Program

- Start small
  - Start with a small section of the network's assets
- Expand slowly
  - Gradually add more scope to your scans
- Prevent overwhelming the enterprise systems and your system administration team