JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

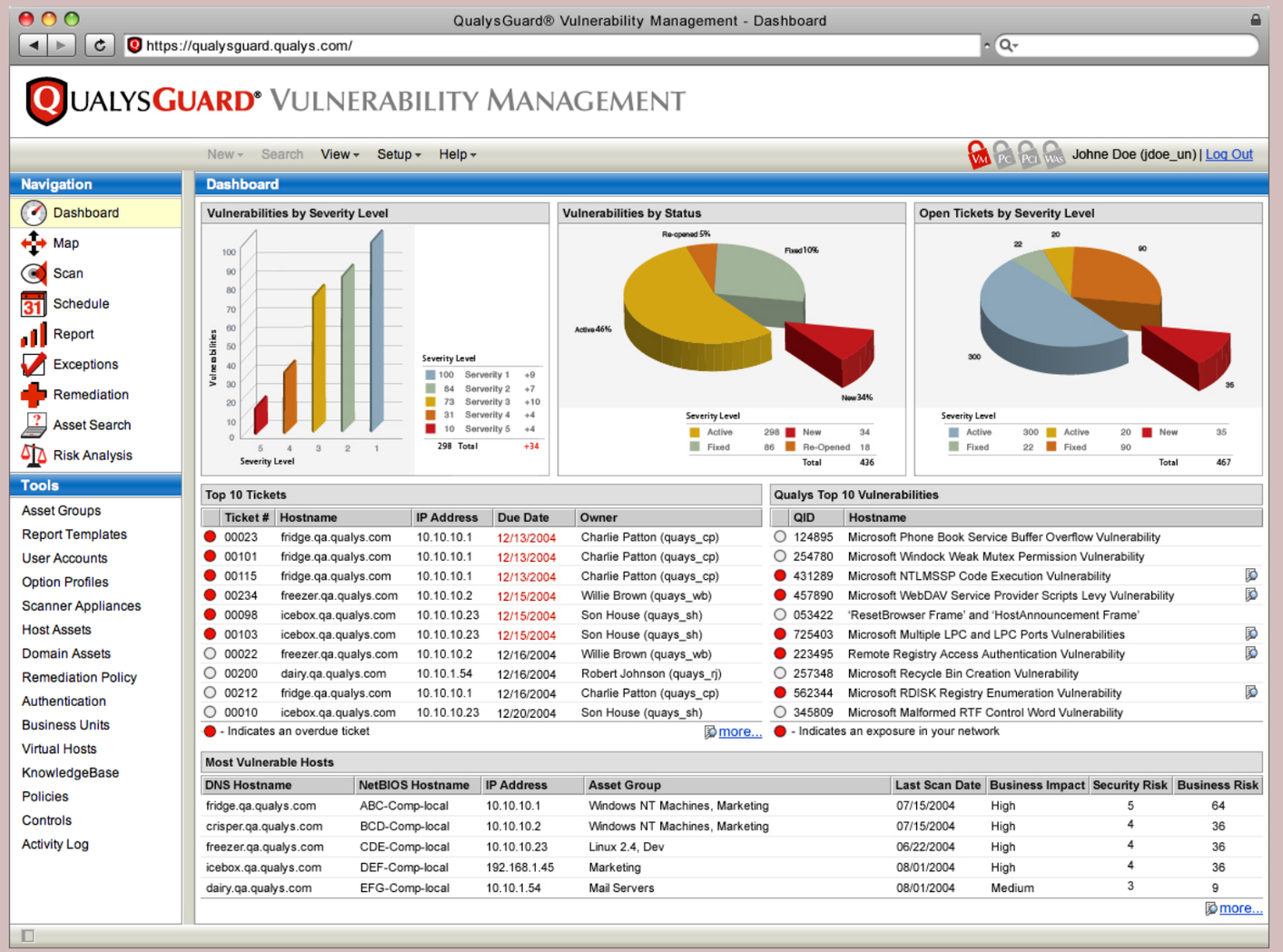
Scanning Tools

VULNERABILITY MANAGEMENT

Vulnerability Scanning Tools

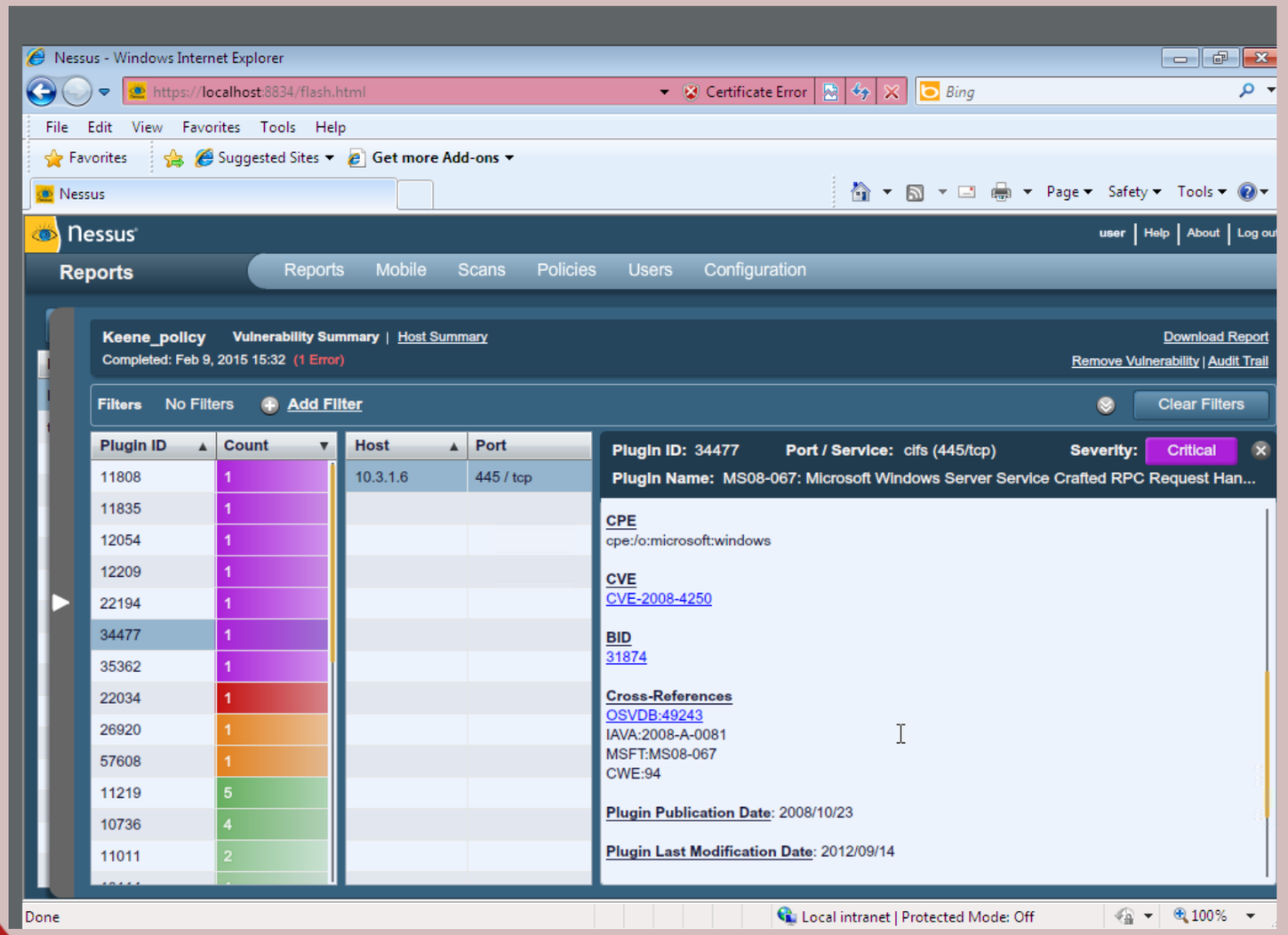
- QualysGuard
- Tenable's Nessus
- Rapid7's Nexpose
- OpenVAS
- Nikto Web Application scanner
- Microsoft Baseline Security Analyzer

QualysGuard Vulnerability Scanner



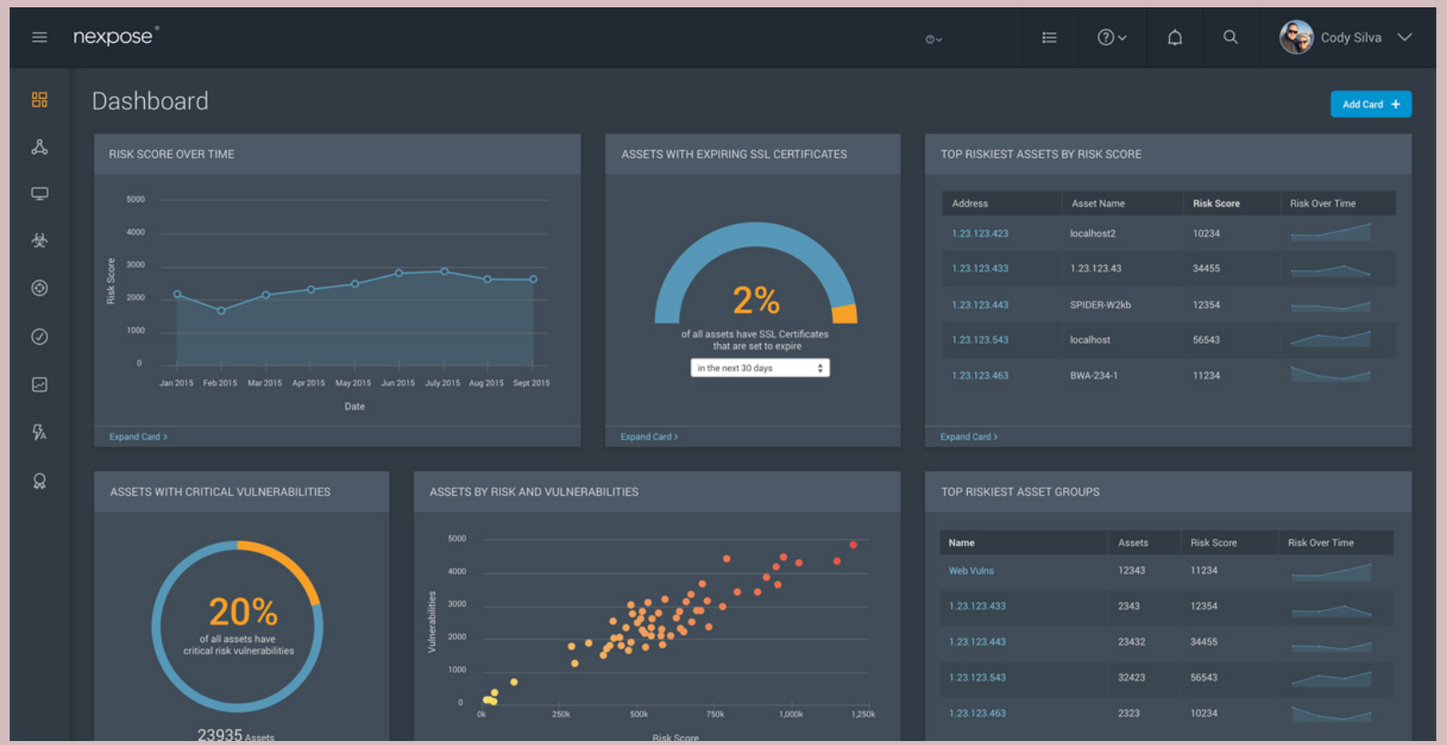
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Tenable's Nessus Vulnerability Scanner



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Rapid7's Nexpose



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

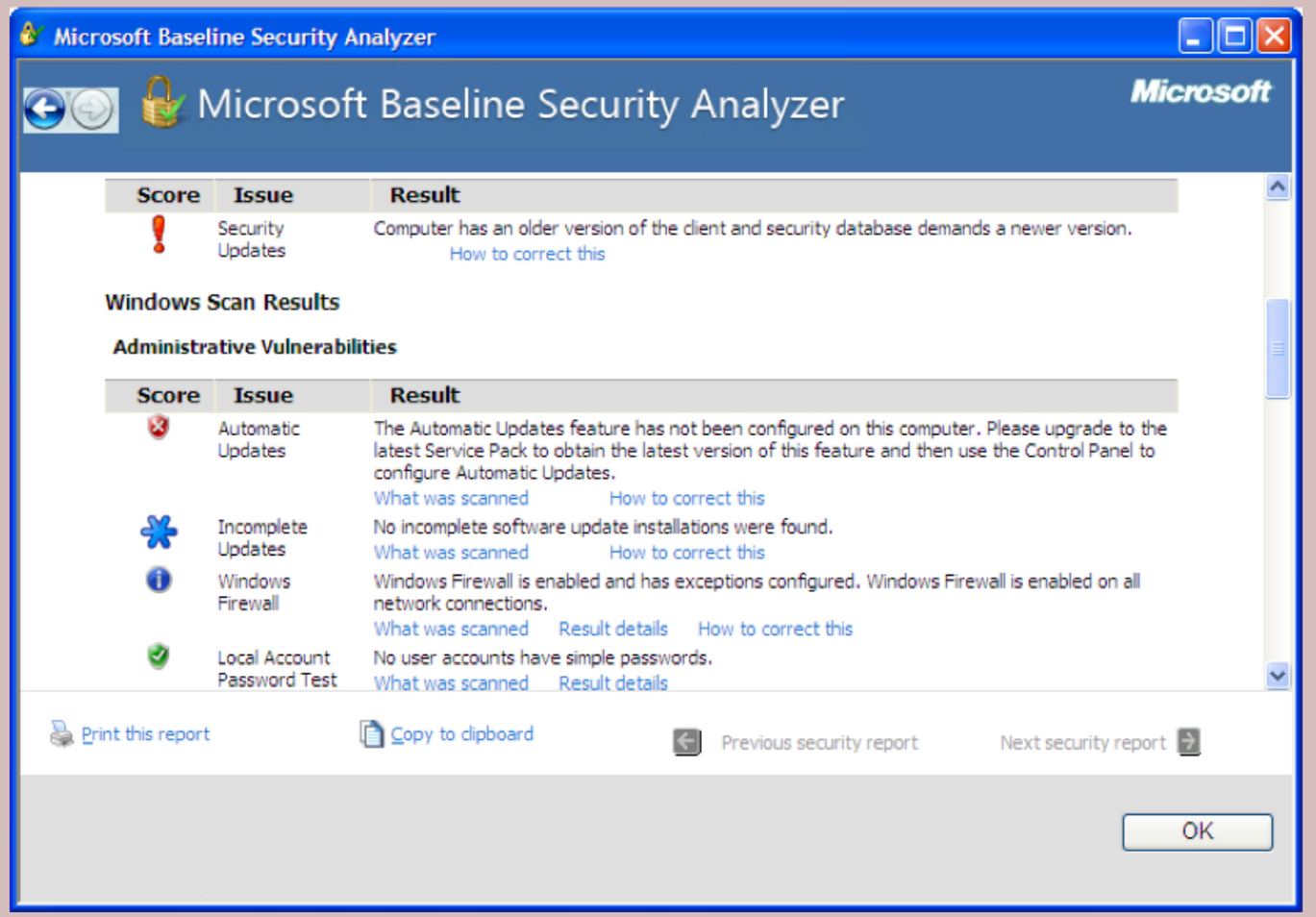
OpenVAS (Open-source Scanner)

Nikto
(Web Application Scanner)

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          87.229.144.34
+ Target Hostname:    google.ru
+ Target Port:        80
+ Start Time:         2015-02-26 14:51:38 (GMT6)
---------------------------------------------------------------------------
+ Server: gws
+ Uncommon header 'alternate-protocol' found, with contents: 80:quic,p=0.08
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://www.google.ru/
+ Server banner has changed from 'gws' to 'sffe' which may suggest a WAF, load b
alancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-5737: WebLogic may reveal its internal IP or hostname in the Location he
ader. The value is "http://87.229.144.34/".
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Microsoft's Baseline Security Analyzer



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE