TENABLE

Network Security®

TENABLE
Network Security®

Unified Security Monitoring

- PCI, SOX & FISMA
- CIS, NIST, CERT
- RIAA, MPAA, NERC
- Real-time Monitoring
- Best-Practices Auditing
- Data Leakage Monitoring
- Software Enumeration
- Accurate Asset Discovery
- Communication Activity

- Nessus 3 Vulnerability Scanner
- Distributed Scanning
- Patch & Configuration Auditing
- Data Leakage Identification
- Passive Network Monitoring
- Network Change Detection
- Role-Based Analysis
- Automatic Asset Discovery
- Security Workflow
- Sophisticated Reporting

- Log Aggregation
- Network Anomaly Detection
- Compromise Detection
- Role-Based Analysis
- Usage Monitoring
- Automatic Asset Learning
- False Positive Reduction
- Forensic Analysis
- Easy to deploy and operate

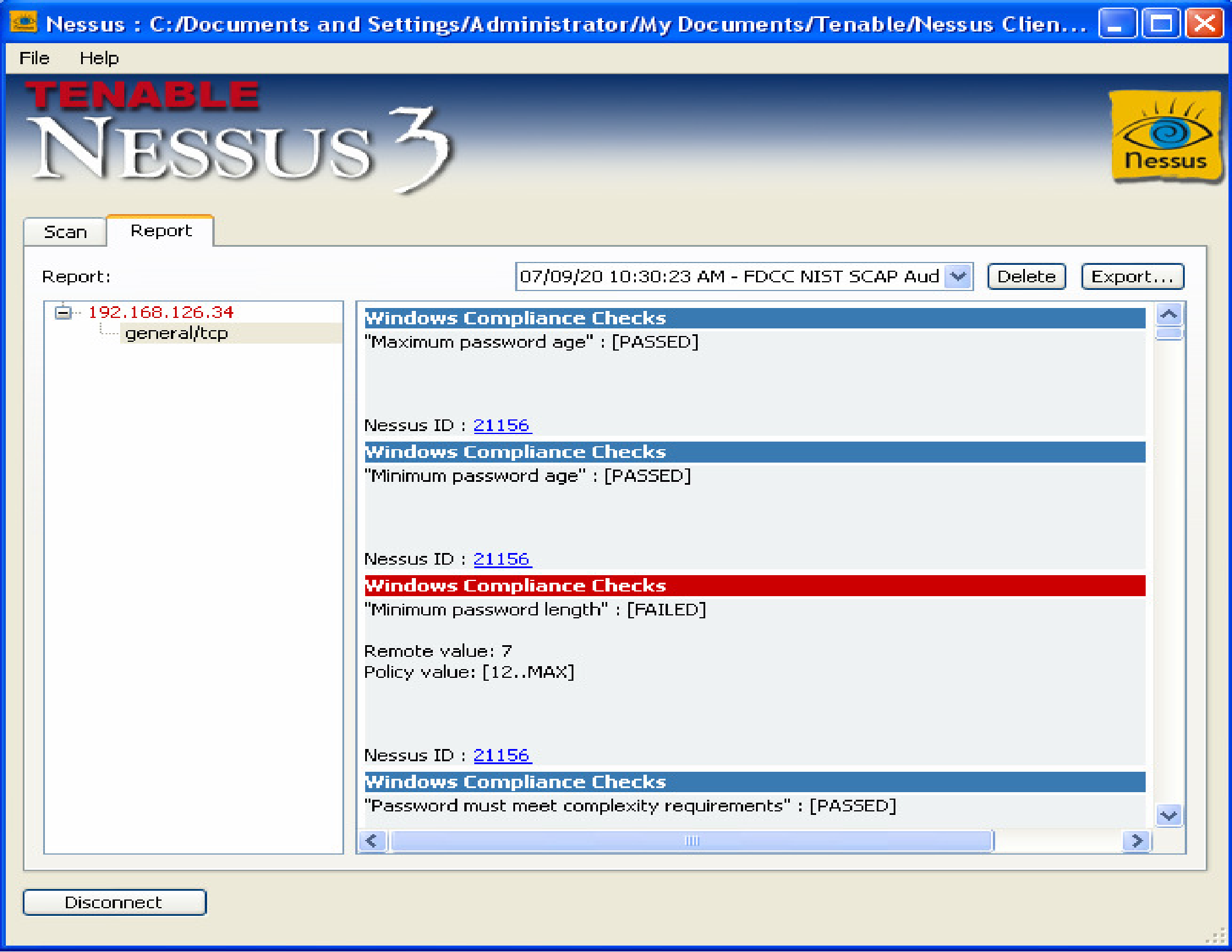
Nessus 3 Vulnerability Scanner

- Scans networks to discover hosts, applications and vulnerabilities
- Downloaded more than **3,000,000** times in last 12 months
- Available for wide variety of **Windows** and **UNIX** platforms
- Audits more than **15,000** different vulnerabilities
  - Free Users audit with older checks
  - Commercial customers can audit configurations and use latest checks
- **CVSSv2** and **CVE**

Agent-less Auditing With Nessus

- **Agencies** audit with **multiple** Nessus Scanners
  - Management and reporting performed by the Security Center
- **Individuals** audit with **single** Nessus Scanners

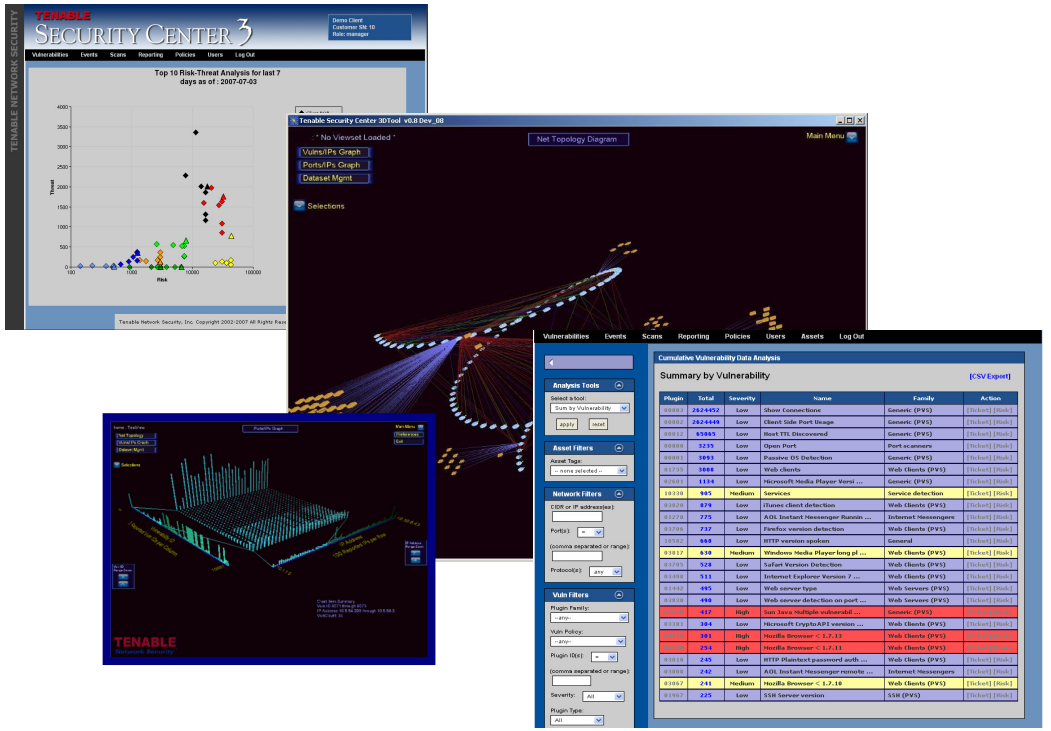
- Vulnerability Audits
- Patch Audit
- Configuration Audits (including S-CAP content)
- Sensitive Data Discovery (credit cards, SSNs, .etc)


Nessus : C:/Documents and Settings/Administrator/My Documents/Tenable/Nessus Clien...
File
Help
TENABLE
NESSUS 3
Nessus
Scan
Report
Report:
07/09/20 10:30:23 AM - FDCC NIST SCAP Aud
Delete
Export...
192.168.126.34
general/tcp
Windows Compliance Checks
"Maximum password age" : [PASSED]
Nessus ID : 21156
Windows Compliance Checks
"Minimum password age" : [PASSED]
Nessus ID : 21156
Windows Compliance Checks
"Minimum password length" : [FAILED]
Remote value: 7
Policy value: [12..MAX]
Nessus ID : 21156
Windows Compliance Checks
"Password must meet complexity requirements" : [PASSED]
Disconnect

Enterprise Agent-less Auditing

- Tenable Security Center
- In use at more than 30 Government agencies
  - Current under Common Criteria evaluation

- Role Based
- Scan Scheduling
- Asset Discovery
- Results Reporting
- Asset Trending
- *… SIM, NBAD & Logs*



TENABLE NETWORK SECURITY

TENABLE SECURITY CENTER 3

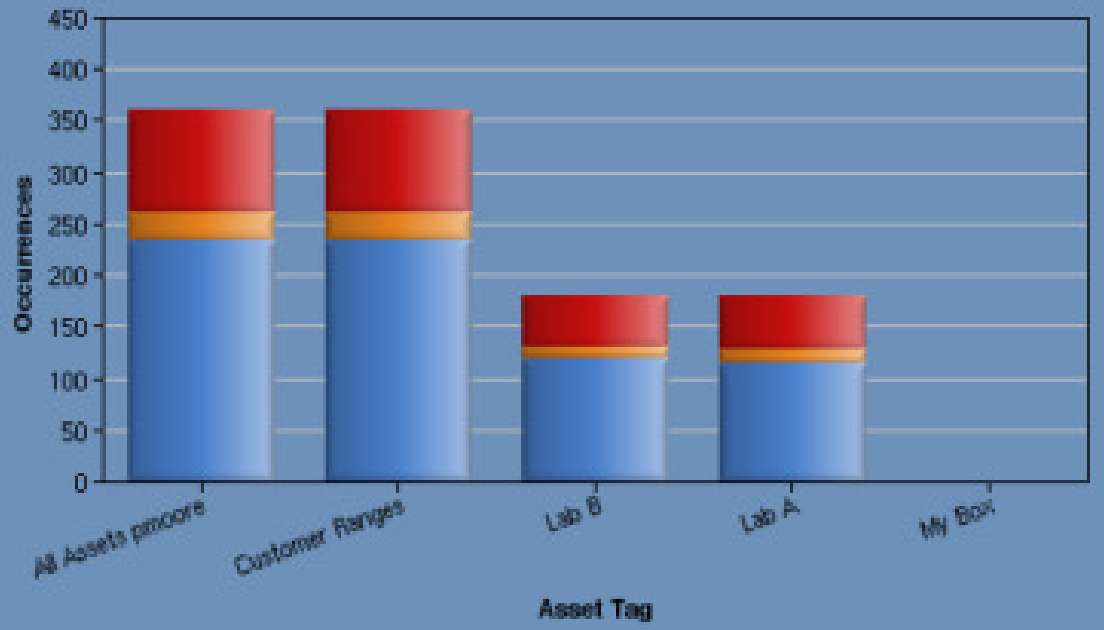
Phil
Customer SN: 20
Role: manager

Home | Vulnerabilities | Events | Scans | Reporting | Policies | Users | Assets | Log Out | System State

- Analysis Tools
- Asset Filters
- Network Filters
- Vuln Filters
- Discovery Filters
- Observed Filters
- Workflow Filters
- Reset Filters
- Export CSV

Summary by Assets

8 records / 1 page



Asset	Total	Critical	High	Medium	Low
Event Asset I	0	0	0	0	0
Event Asset II	0	0	0	0	0
Lab C	0	0	0	0	0
My Box	1	0	0	1	0
Lab B	181	0	50	12	119
Lab A	179	0	50	14	115
All Assets pmoore	361	0	100	27	234
Customer Ranges	361	0	100	27	234

TENABLE NETWORK SECURITY

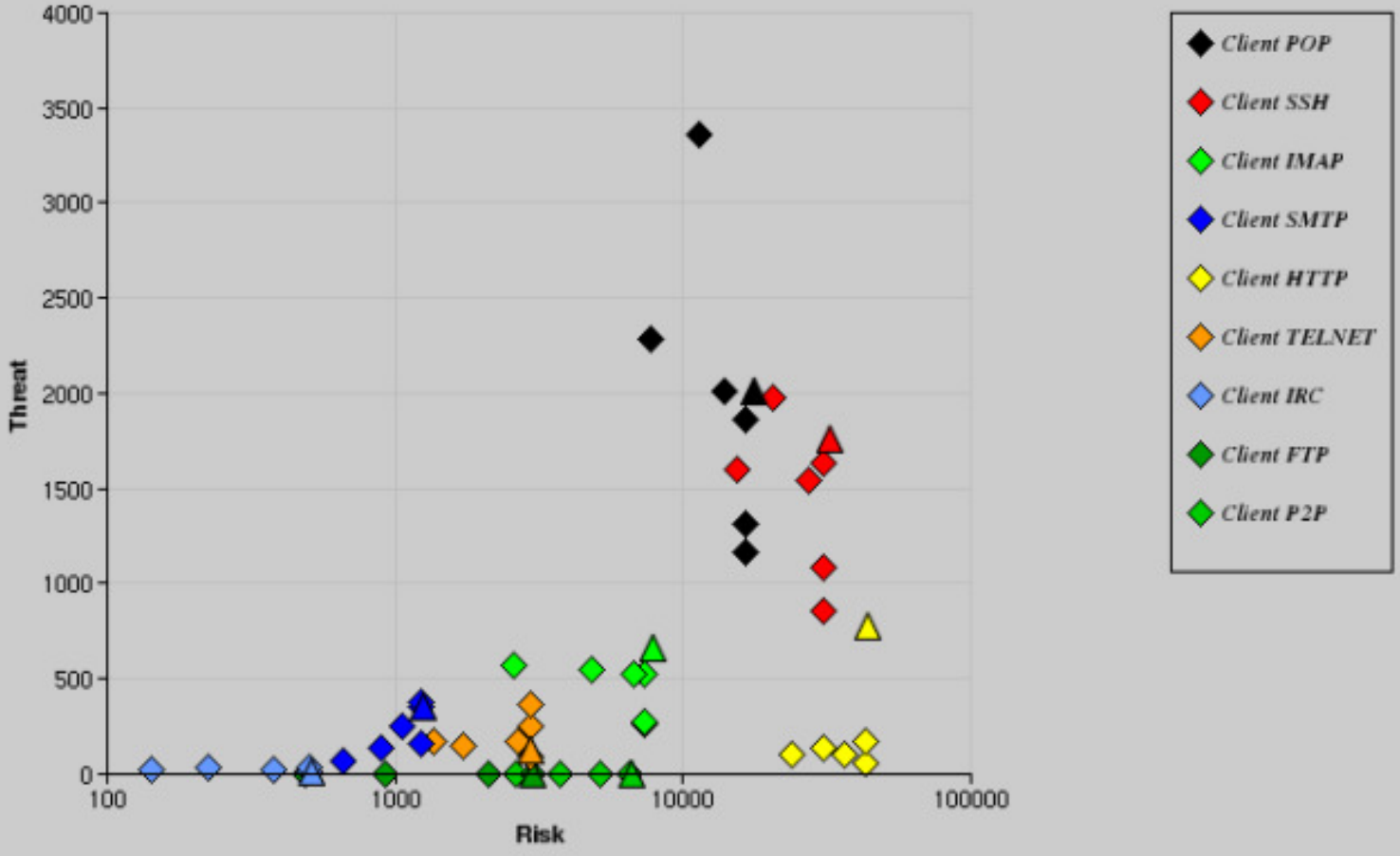
TENABLE

SECURITY CENTER 3

Demo Client
Customer SN: 10
Role: manager

Vulnerabilities | Events | Scans | Reporting | Policies | Users | Log Out

Top 10 Risk-Threat Analysis for last 7 days as of : 2007-07-03



Nessus 3 Configuration Checks for Windows

- **Windows Audit Points**
  - File access control checks
  - Registry access control checks
  - Service access control checks
  - Custom checks (password, audit, Kerberos, .etc)
  - File & registry permissions
  - Existence of a file or registry setting
  - File Content Check
- **Supported Audit Platforms**
  - Windows XP Pro
  - Windows 2000
  - Windows 2003
  - Vista (Soon)

Nessus 3 Configuration Checks for UNIX

- **UNIX Audit Points**
  - File permission checks
  - File content checks
  - Process checks
  - Password & User policy checks
  - MD5 Check of files
- **Supported Audit Platforms**
  - Solaris
  - OS X
  - Most flavors of Linux
  - FreeBSD
  - AIX (Soon)

Example Windows Audit

```
<group_policy: "Password Policy">
        <item>
          name: "Enforce password history"
          value: 24
        </item>
        <item>
          name: "Maximum password age"
          value: 90
        </item>
        <item>
          name: "Minimum password age"
          value: 1
        </item>
        <item>
          name: "Minimum password length"
          value: [12..14]
        </item>
</group_policy>
```

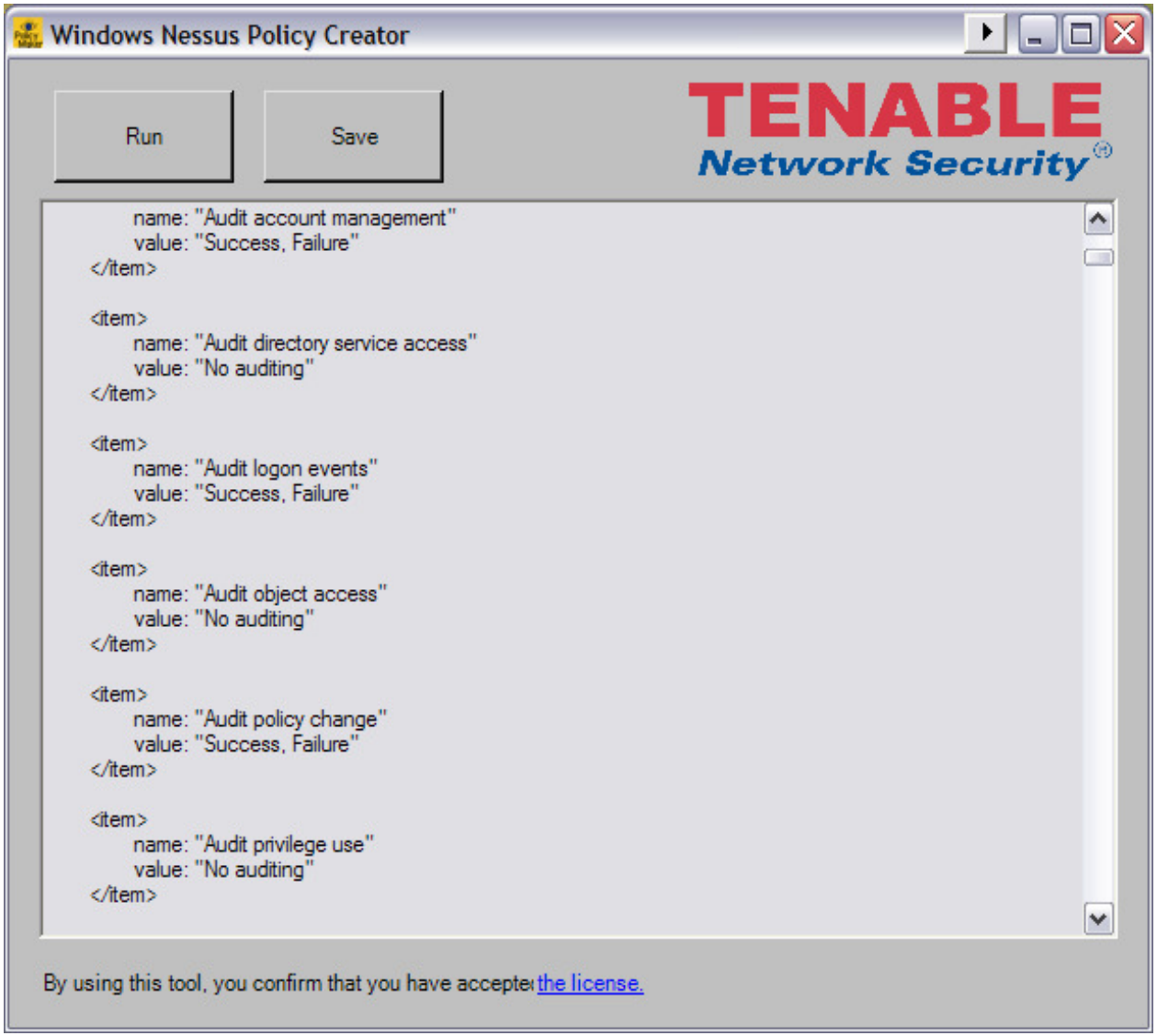
Example UNIX Audit

```
# Example 8
# File content check to audit if file /etc/host.conf
# contains the string described in the regex field.
#
<custom_item>
        #System           : "Linux"
        type              : FILE_CONTENT_CHECK
        description       : "This check reports a problem if the
   order is not 'order hosts,bind' in /etc/host.conf"
        file              : "/etc/host.conf"
        search_locations  : "/etc"
        regex             : "order hosts,bind"
        expect            : "order hosts,bind"
</custom_item>
```

Available Configuration Audit Content

- **NIST S-CAP**
- DISA STIG
- CERT
- NSA SNAC
- NERC (SCADA)
- CIS
- PCI
- Vendors
- Tenable Research

Content Tools - Windows Nessus Policy Creator

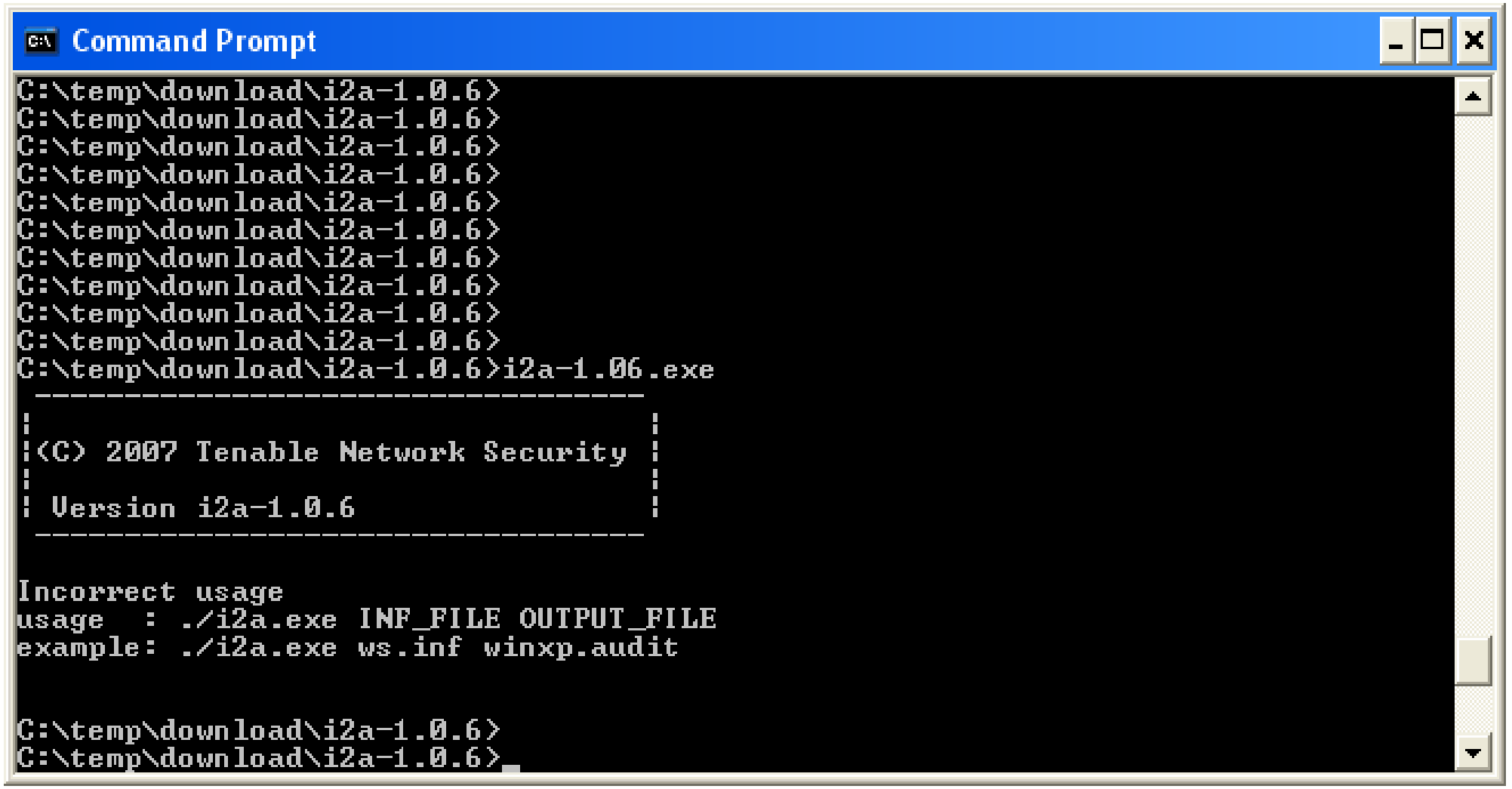


Content Tools - x2a

- Tenable is about to release the **x2a** tool which will convert XCCDF files to Nessus 3 and Security Center audit policies files

- Currently available "S-CAP" files have been derived from a pre-release version and are available on our support web site

Content Tools - inf2audit.exe



Content Tools - c2a.pl

```
#
# This file is auto-generated with c2a.pl script
# Copyright 2006 Tenable Network Security Inc
#

<check_type : "Unix">

<custom_item>
        #System :       "Linux"
        type    :       FILE_CHECK
description     :       "Check MD5 for /etc/snort/snort.conf"
        file    :       "/etc/snort/snort.conf"
        md5     :       "823b28cbc726f68538abdb0451f29a01"
</custom_item>

<custom_item>
        #System :       "Linux"
        type    :       FILE_CHECK
description     :       "Check MD5 for /opt/sc3/daemons/daemons.cfg"
        file    :       "/opt/sc3/daemons/daemons.cfg"
        md5     :       "3403c4c155a94c4c915ac0b01d4a60dc"
</custom_item>

<custom_item>
        #System :       "Linux"
        type    :       FILE_CHECK
description     :       "Check MD5 for /opt/pvs/etc/pvs.conf"
        file    :       "/opt/pvs/etc/pvs.conf"
        md5     :       "3b4a4b0b7a3cdf7fa3aff3c54f5e6ad4"
</custom_item>

</check_type>
```

Configuration Auditing Roadmap

- Continued support for **SCAP** and **CIS** standards
- Nessus configuration audit support for **Routers**, **Switches** and **Firewalls**
- 100% (we're 95% today) **OVAL XCCDF** support
- **Passive network analysis** and mapping to determine configurations
- Nessus 3.2 (in beta now) will support **IPv6**
- Continued refinement of **log and network** event analysis as it pertains to compliance and configuration auditing

Contact Information

- http://www.tenablesecurity.com
- http://blog.tenablesecurity.com
- http://www.nessus.org

- Video Demos
- White Papers
- Multiple Webinars on Compliance
- Free Nessus Download