Please open your **CSC436_Environment** Kali VM!!

Vulnerability Scanning

Part 1

Installing Nessus

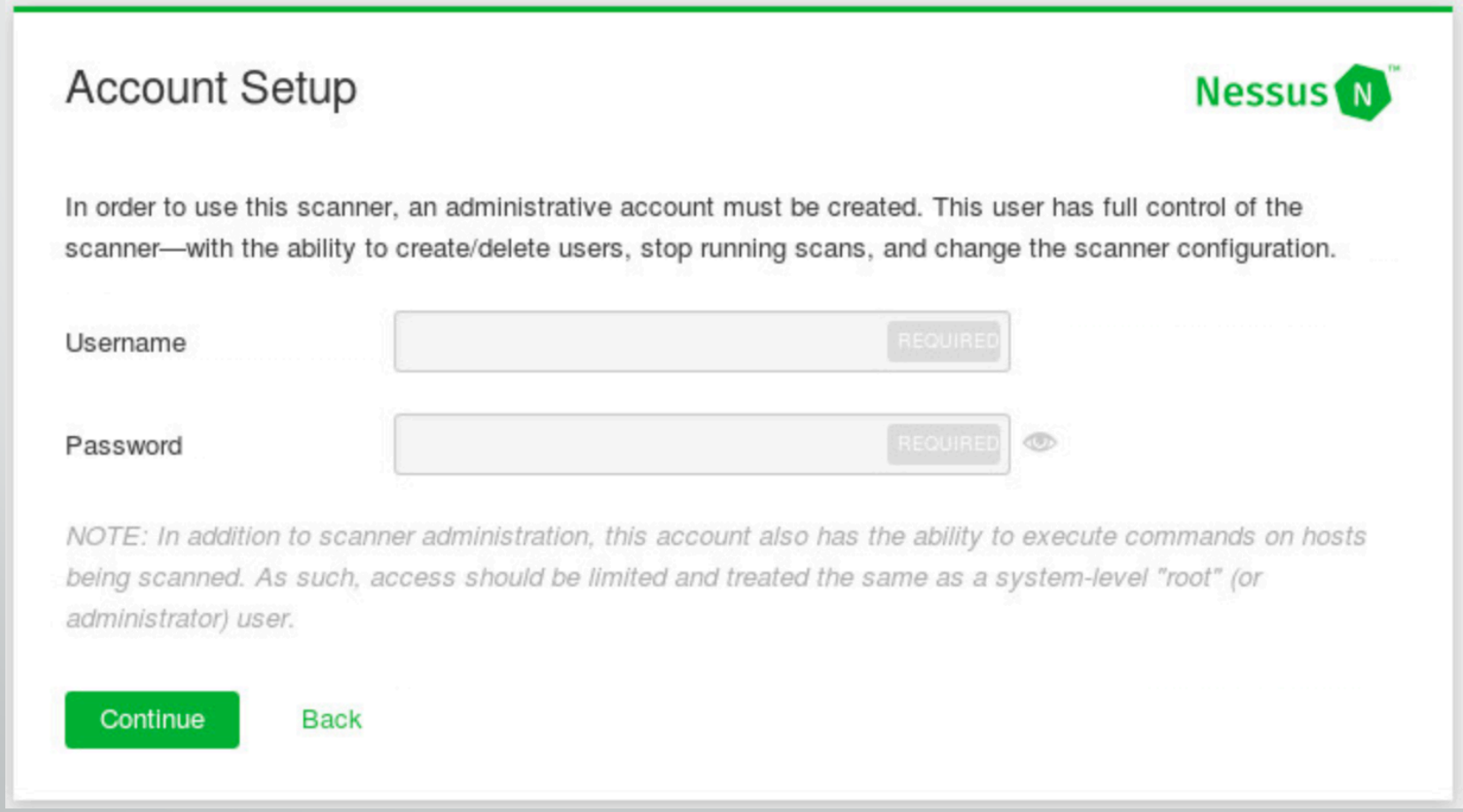
- Available at https://www.tenable.com/products/nessus-home
- Download Nessus
  - OS Specific
- Register for a key
  - Check your Email

- http://10.10.10.50
- dpkg –i Nessus-6.11.1-debian6_amd64.deb

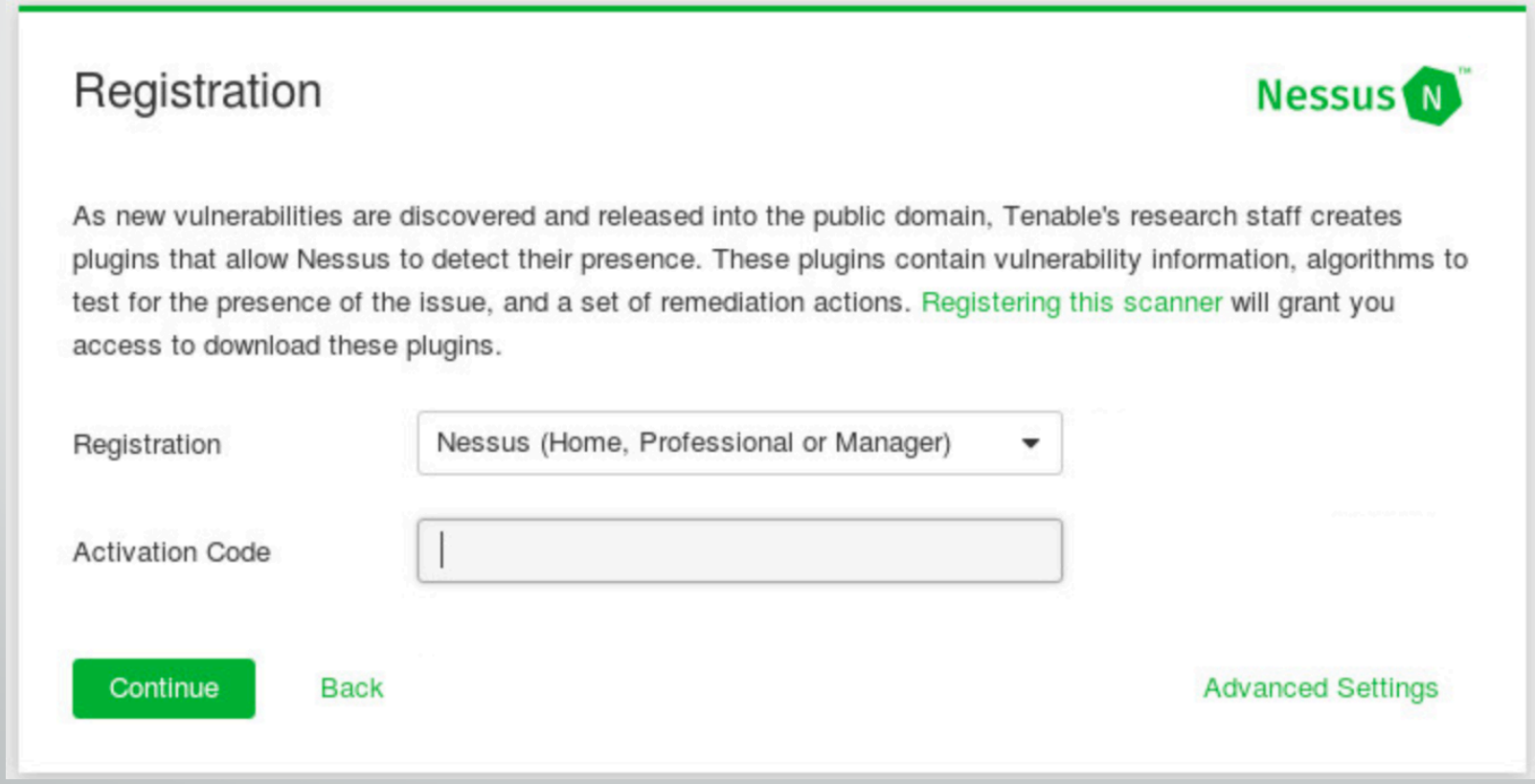
Installing Nessus

- Start the Nessus Service
  - /etc/init.d/nessusd start
- Open Nessus in a browser
  - https://localhost:8834
  - SSL error? Add it to your exceptions.

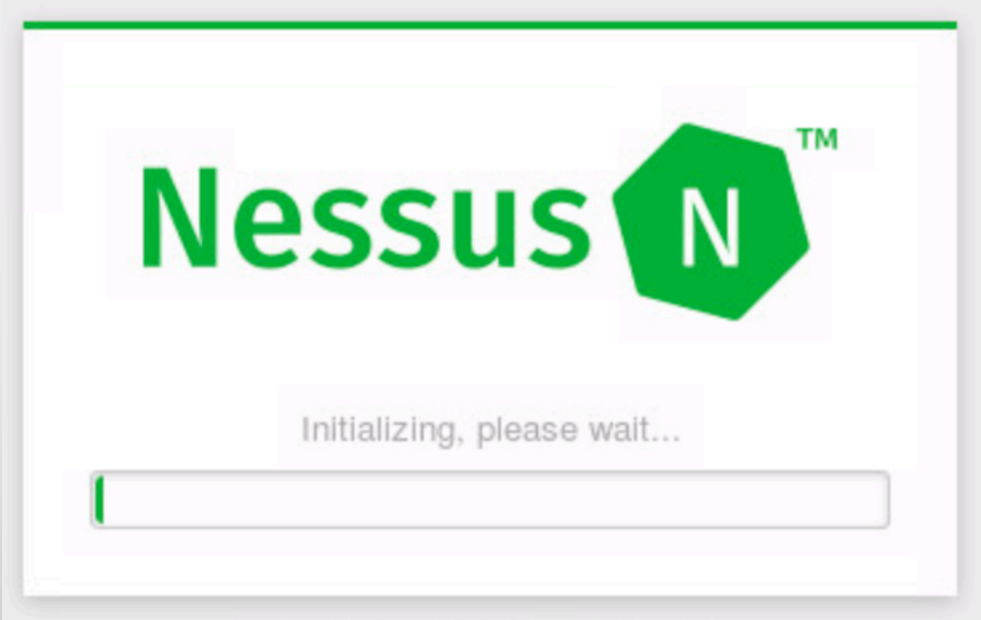
Setup an Account



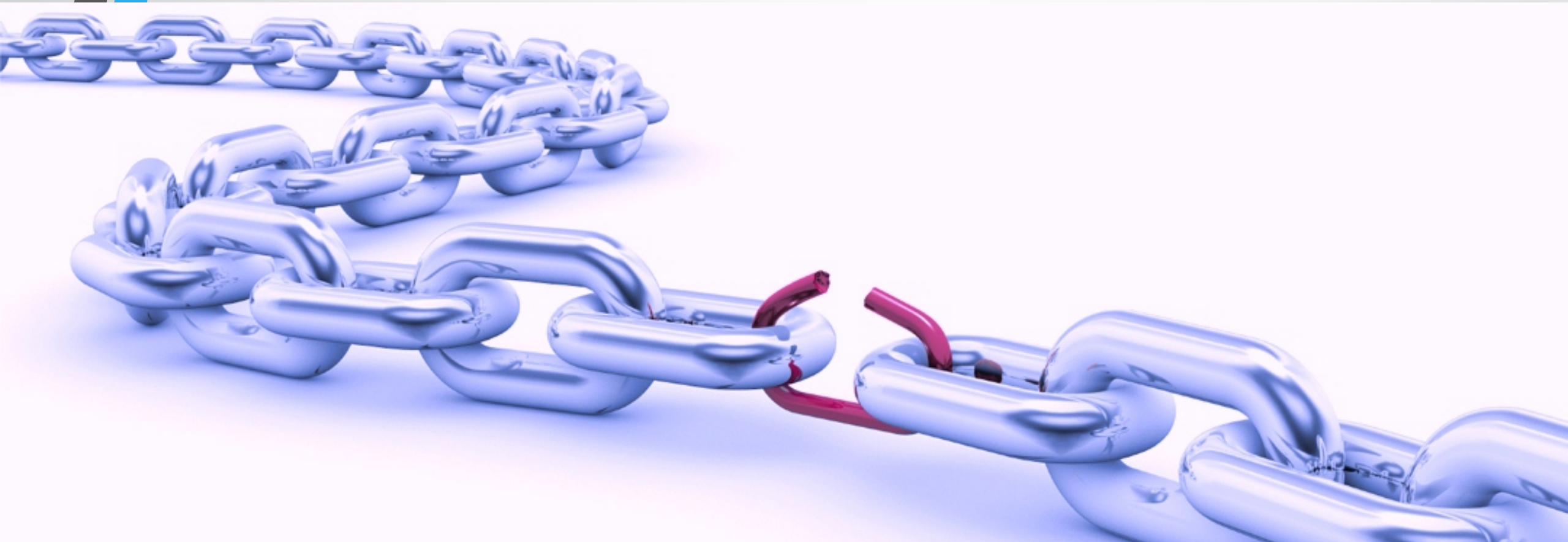
Register


Registration
Nessus
As new vulnerabilities are discovered and released into the public domain, Tenable's research staff creates plugins that allow Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.
Registration
Nessus (Home, Professional or Manager)
Activation Code
Continue
Back
Advanced Settings

Nessus Downloads Plugins



Vulnerability vs. Exploit?



Vulnerability vs. Exploit?

- Vulnerability = potential
  - "the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally."
- Exploit = weaponized
  - "a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware."

Three Types of Vulnerabilities

- Common Configuration Errors
  - Directory listing enabled on a webserver
- Default Configurations
  - Default password/no password
- Well-known System/Software Flaws
  - MS08-067 (RPC Server Vulnerability)

CVE – Common Vulnerabilities and Exposures

- Common system used to identify publicly known vulnerabilities
- Managed by the MITRE Corporation
- Each CVE is assigned an ID number
  - 76 organizations are CVE Numbering Authorities (CNAs)
    - Mostly vendors

CVE-2008-4250

- https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2008-4250
- Vulnerability in the server service in Windows 200 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold SP1, Server 2008, and 7 Pre-Beta.
- Allows remote code execution
  - Via crafted RPC request triggering an overflow.

Other Vendors Have Other Reporting Avenues

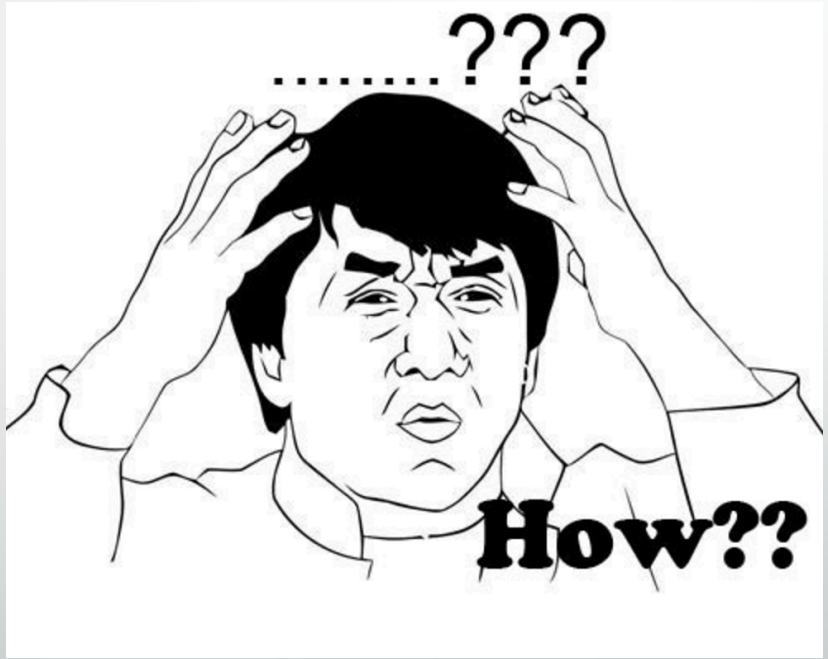
- Microsoft Security Bulletins – Typically are patches, but those are tied to a vulnerability

Date	Bulletin number	Title	Affected Software
March 2017			
March 14, 2017	MS17-023	Security Update for Adobe Flash Player (4014329)	Microsoft Windows Adobe
March 14, 2017	MS17-022	Security Update for Microsoft XML Core Services (4010321)	Microsoft Windows
March 14, 2017	MS17-021	Security Update for Windows DirectShow (4010318)	Microsoft Windows
March 14, 2017	MS17-020	Security Update for Windows DVD Maker (3208223)	Microsoft Windows
March 14, 2017	MS17-019	Security Update for Active Directory Federation Services (4010320)	Microsoft Windows
March 14, 2017	MS17-018	Security Update for Windows Kernel-Mode Drivers (4013083)	Microsoft Windows

MS08-067

- https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
- Security Update the resolves a vulnerability in the Server service.
- Vulnerability allows remote code execution
  - Specifically crafted RPC request
  - Run arbitrary code without authentication
- Critical Bulletin

How Can We Find Vulnerabilities?



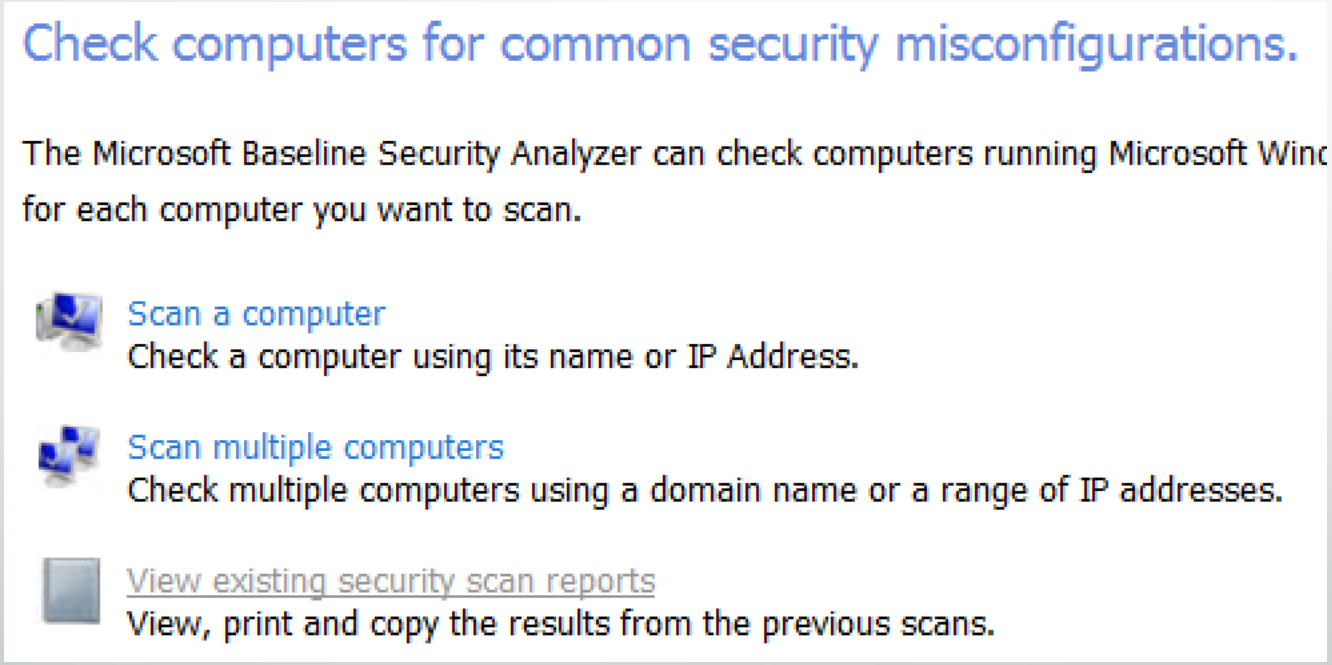
Vulnerability Scanner

- Automates the process of looking for vulnerabilities
  - Many include port scanners
- Most vulnerability scanners include…
  - Vulnerability DB
  - User configuration tool
  - Scanning engine
  - Knowledge base of current scan
  - Results repository

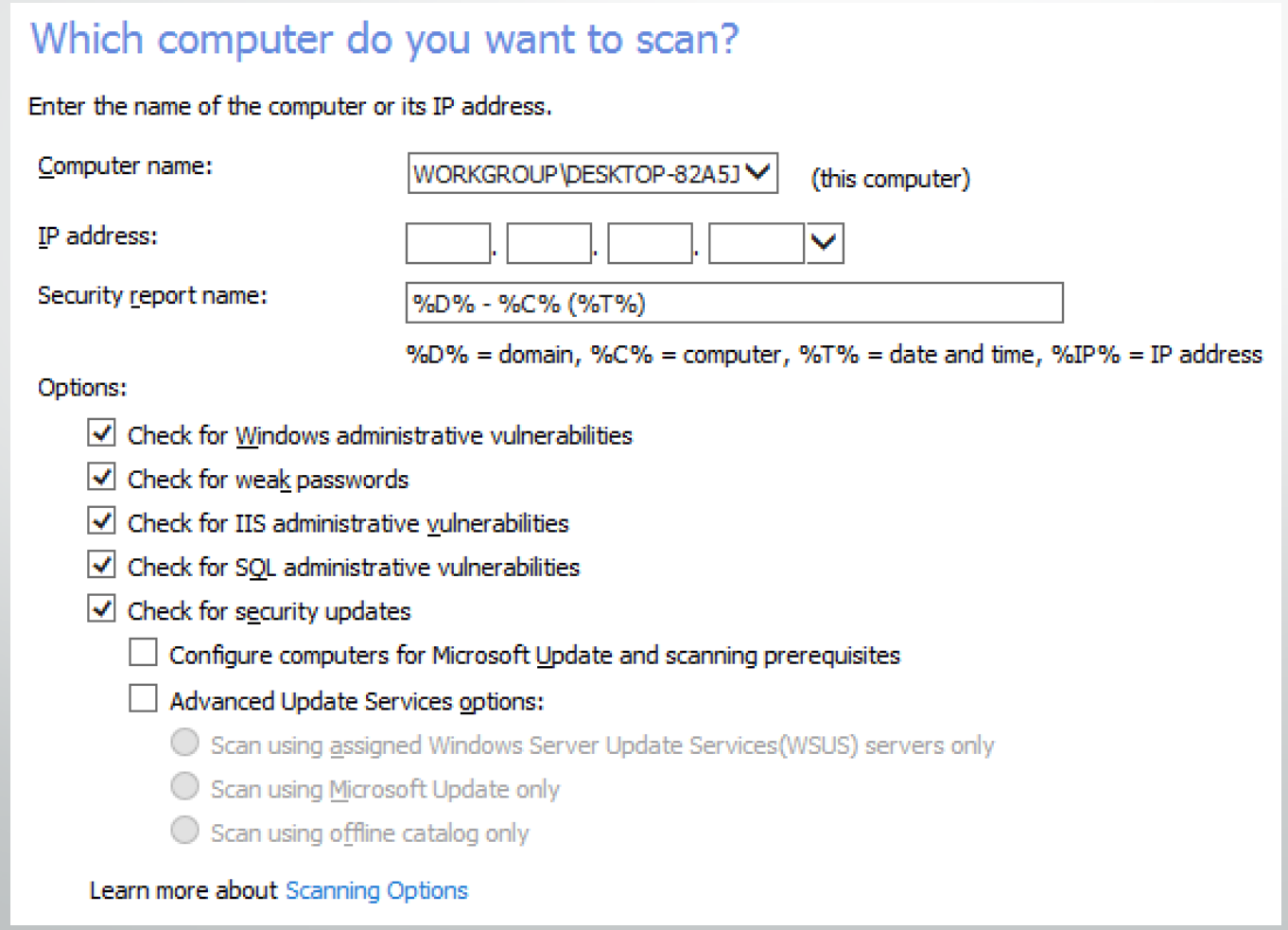
Microsoft Baseline Security Analyzer (MBSA)

- Patch scanner for Microsoft products.
  - Only security patches. Nothing else.
- Scriptable
  - Set it as a background task
  - Can alert when something is missing a patch, for example.

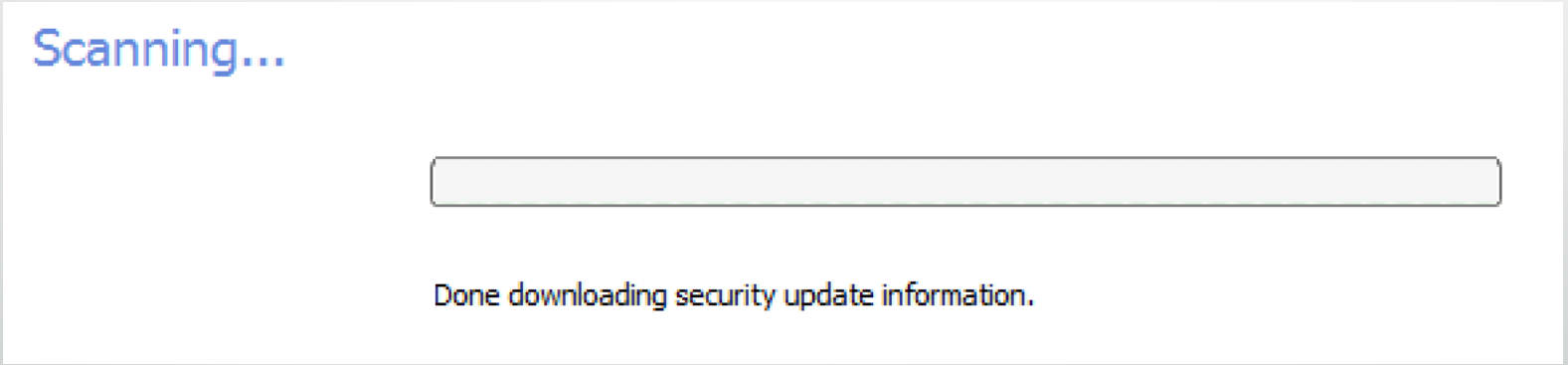
MBSA


Check computers for common security misconfigurations.
The Microsoft Baseline Security Analyzer can check computers running Microsoft Winc
for each computer you want to scan.
Scan a computer
Check a computer using its name or IP Address.
Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.
View existing security scan reports
View, print and copy the results from the previous scans.

MBSA Scan


Which computer do you want to scan?
Enter the name of the computer or its IP address.
Computer name:
WORKGROUP\DESKTOP-82A5J
(this computer)
IP address:
Security report name:
%D% - %C% (%T%)
%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address
Options:
Check for Windows administrative vulnerabilities
Check for weak passwords
Check for IIS administrative vulnerabilities
Check for SQL administrative vulnerabilities
Check for security updates
Configure computers for Microsoft Update and scanning prerequisites
Advanced Update Services options:
Scan using assigned Windows Server Update Services(WSUS) servers only
Scan using Microsoft Update only
Scan using offline catalog only
Learn more about Scanning Options

MBSA Scanning...



MBSA Report

Report Details for WORKGROUP - DESKTOP-82A5J9C (2017-09-25 23:15:52)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\DESKTOP-82A5J9C
IP address:	192.168.205.138
Security report name:	WORKGROUP - DESKTOP-82A5J9C (9-25-2017 11-15 PM)
Scan date:	9/25/2017 11:15 PM
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	2017-09-11T16:31:15Z
Security update catalog:	Microsoft Update (offline)

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
	Developer Tools, Runtimes, and Redistributables Security Updates	2 security updates are missing. What was scanned Result details How to correct this
	SQL Server Security Updates	No security updates are missing. What was scanned Result details
	Windows Security Updates	No security updates are missing. What was scanned Result details

Nessus

- Released in 1998
- Previously open source
- Uses a client/server technology
- Can conduct testing from different locations
- Can scan multiple OSs

Nessus Plugins

- Each vulnerability check is based on a small program, aka plugin
- Each plugin conducts one check on a target system
- Thousands of plugins available
  - Make up the Nessus Vulnerability Database
  - 90,635 at last check
- Downloadable from https://www.tenable.com/plugins/index.php

Nessus Plugin Categories

- http://static.tenable.com/documentation/Tenable_Products_Plugin_Families.pdf
- …there's a few.

Nessus Is Not Free…kinda

- Nessus Home
  - No support
  - No compliance checks
  - No content audits
  - Cannot use Nesssus virtual appliance
  - Only 16 addresses per scanner
  - $free
- Nessus Professional
  - $2,190/year
    - But there's a 7 day free trial
      - Trial is limited to 16 addresses

Let’s switch our network back…

Scan Templates

‹ Back to Scans

Search Library

Scanner

Advanced Scan
Configure a scan without using any recommendations.

UPGRADE
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan
A full system scan suitable for any host.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

DROWN Detection
Remote checks for CVE-2016-0800.

Host Discovery
A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

UPGRADE
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan
Scan for malware on Windows and Unix systems.

UPGRADE
MDM Config Audit
Audit the configuration of mobile device managers.

UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

UPGRADE
Offline Config Audit
Audit the configuration of network devices.

UPGRADE
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

UPGRADE
Policy Compliance Auditing
Audit system configurations against a known baseline.

UPGRADE
SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

WannaCry Ransomware
Remote and local checks for MS17-010.

Web Application Tests
Scan for published and unknown web vulnerabilities.