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

Vulnerability Scanning

Part 2

Let’s pretend we have an exam/quiz thing next week…

- Option 1:
  - Review Tuesday
  - Test Thursday
- Option 2:
  - Slightly smaller test Tuesday
  - Something else Thursday

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.

Scanning With Nessus

- First, we create a scan
  - Can specify hosts
  - What do we want to do in the scan?
- Launch the scan

- 10.10.20.56

Ok, So Nessus is Great And All…

- …but you should run multiple vulnerability scanners.

OpenVAS

- Part of Greenbone Networks' commercial vulnerability management solution
- Open Source

Installing OpenVAS

- apt-get update
- apt-get install openvas

- openvas-setup
- openvas-start

OpenVAS

- https://localhost:9392
- User: admin
- Password: given on the command line
  - Can create users by using openvasad on the command line

NVT Feed

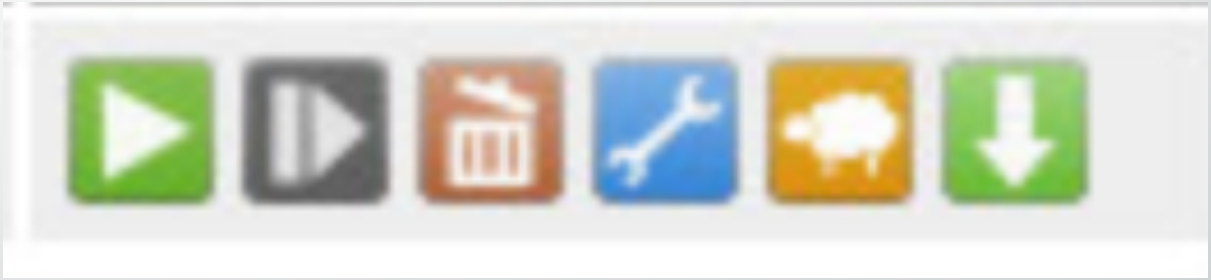
- NVT – Network Vulnerability Test
- Public feed maintained by Greenbone for OpenVAS
- Currently more than 50,000 NVTs
- Extras -> Feed Status
  - Keep these up to date

Scan With OpenVAS

- Create a target
  - Configuration -> Targets
    - IP (Target List)
    - Ports to Scan
    - Creds (If you want)

Scan With OpenVas

- Create New Task
  - Scans -> Tasks
  - (There's also a wizard)
- Start the scan (Play button)



Report

- Scans -> Reports
  - Choose Task/Scan
  - Can download report

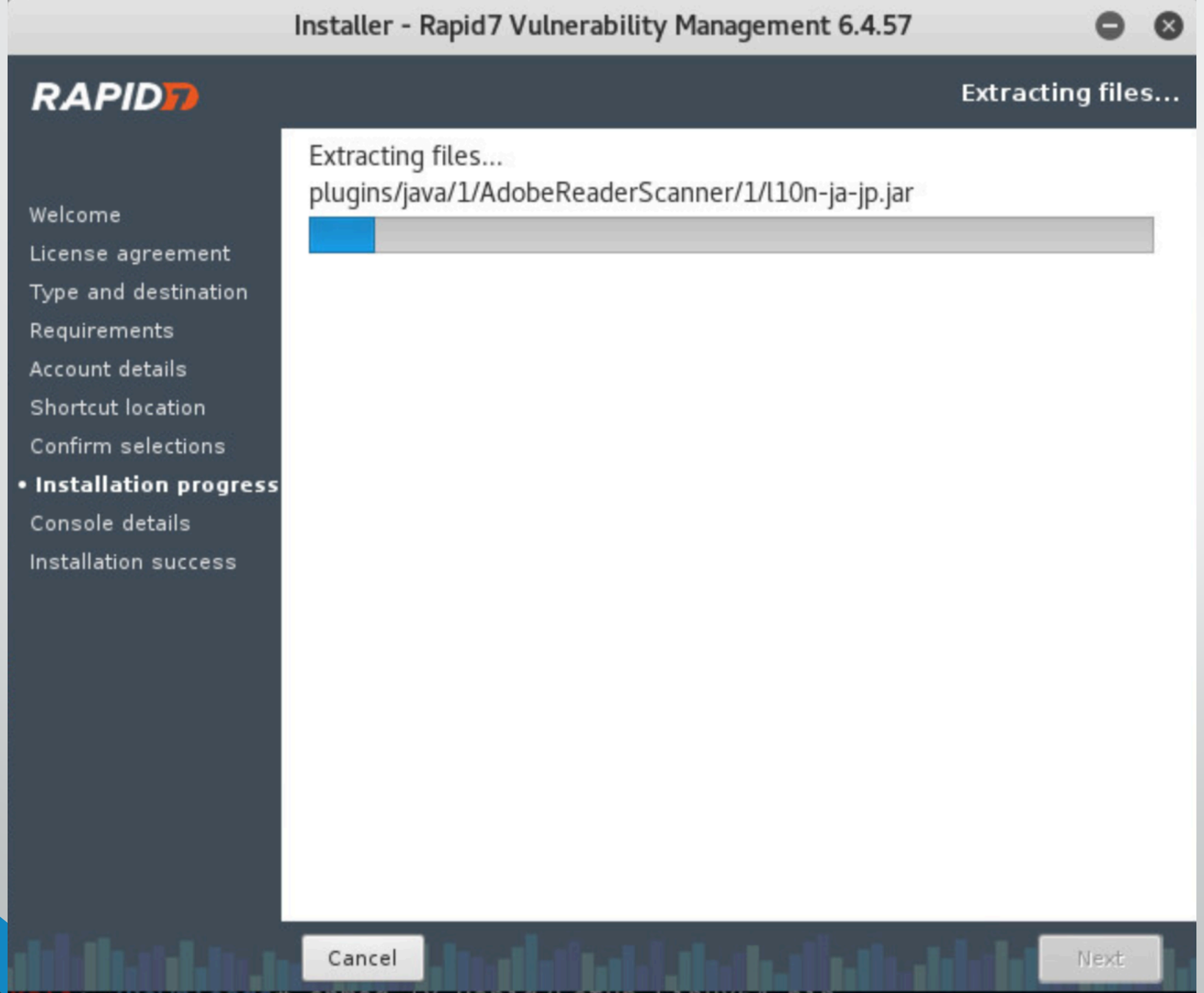
Vulnerability	Severity	QoD	Host	Location
Microsoft Windows Multiple Vulnerabilites (KB4038782)	10.0 (High)	80%	10.10.20.56	general/tcp
Microsoft Windows Multiple Vulnerabilites (KB4022715)	10.0 (High)	80%	10.10.20.56	general/tcp
Microsoft Windows Multiple Vulnerabilites (KB4025339)	10.0 (High)	80%	10.10.20.56	general/tcp
Microsoft Windows Multiple Vulnerabilites (KB4034658)	9.3 (High)	80%	10.10.20.56	general/tcp
Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)	9.3 (High)	80%	10.10.20.56	general/tcp
Microsoft Graphics Component Multiple Vulnerabilities (4013075)	9.3 (High)	80%	10.10.20.56	general/tcp

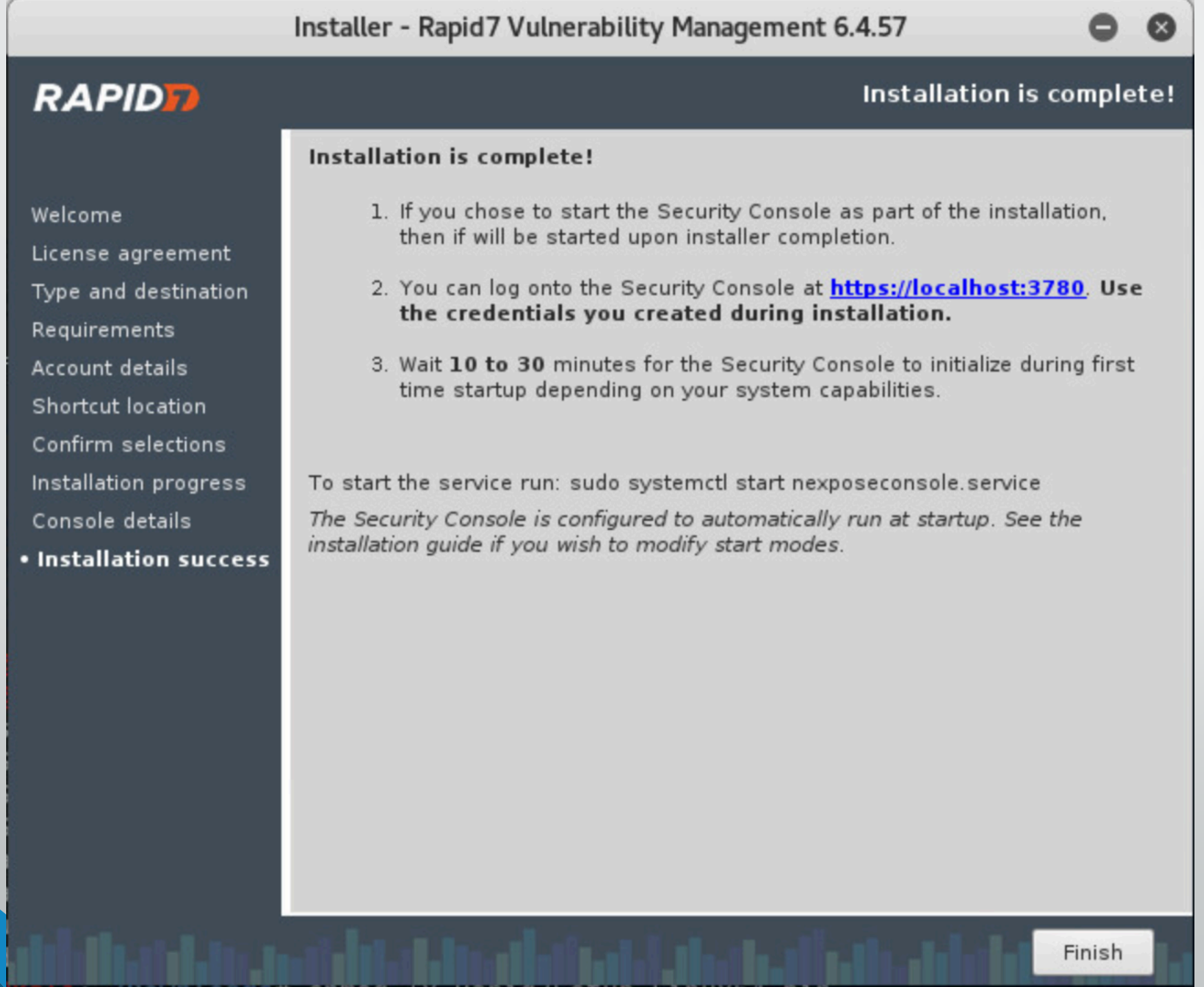
Nexpose

- Built by Rapid7
  - Same company that maintains Metasploit
- Vulnerability Management Software
- Not free, but there is a free trial

Downloading and Installing

- Register for an account/license (Free Trial)
- Download .bin file
- chmod +x Nexpose.bin
- ./Nexpose.bin


Installer - Rapid7 Vulnerability Management 6.4.57
RAPID7
Extracting files...
Welcome
License agreement
Type and destination
Requirements
Account details
Shortcut location
Confirm selections
• Installation progress
Console details
Installation success
Extracting files...
plugins/java/1/AdobeReaderScanner/1/l10n-ja-jp.jar
Cancel
Next


Installer - Rapid7 Vulnerability Management 6.4.57
RAPID7
Installation is complete!
Welcome
License agreement
Type and destination
Requirements
Account details
Shortcut location
Confirm selections
Installation progress
Console details
• Installation success
Installation is complete!
1. If you chose to start the Security Console as part of the installation, then if will be started upon installer completion.
2. You can log onto the Security Console at https://localhost:3780. Use the credentials you created during installation.
3. Wait 10 to 30 minutes for the Security Console to initialize during first time startup depending on your system capabilities.
To start the service run: sudo systemctl start nexposeconsole.service
The Security Console is configured to automatically run at startup. See the installation guide if you wish to modify start modes.
Finish

Starting Nexpose

- systemctl start nexposeconsole.service