|  |  |
| --- | --- |
|  | **I-ISMS Implementation Revision** 1 |

**NP Factory, Ltd.**

**Factory Floor**

**Industrial Information Security Management System**

Guide to conducting infosec vulnerability analysis

Nathan Pocock

https://our.intranet/path/to/document.docx

|  |  |
| --- | --- |
| **I-ISMS Implementation Revision** 1 (30) | **Industrial Information Security Management System**  Guide to conducting infosec vulnerability analysis  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**IISMS**

PRIVATE

|  |  |
| --- | --- |
| 05 - Guide To Infosec Vulnerability Analysis.Docx  Version: 1 Revision 30  Pages: 14 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\05 - Guide to Infosec Vulnerability Analysis.docx  Keywords: vulnerability, assessment, weakness, find, investigate, system, infosec, improve  Last Saved by Nathan Pocock on 9/9/2016 3:01 PM |
|  | **NP Factory, Ltd.**  [Company Address]  Factory Floor  I-ISMS Implementation  704-491-5840  Manager Pocock |

Executive Summary

Provides high-level guidance on how to approach vulnerability analysis at various layers of the industrial automation layers.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 8-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Overview 1](#_Toc461196628)

[2 Physical Location Layer 1](#_Toc461196629)

[3 Network Infrastructure Layer 1](#_Toc461196630)

[4 Computer Systems Layer 1](#_Toc461196631)

[5 Application Layer 1](#_Toc461196632)

[6 Device Layer 1](#_Toc461196633)

Figures

Figure 1 Defense in Depth Onion 1

Figure 2 Stack Methodology of Asset Analysis 1

# 

# Instructions

This page provides quick instructions for using this guide:

1. Read and understand the Overview
2. Obtain the list of assets that you will need to analyze (see [02 - Asset Register.docx](02%20-%20Asset%20Register.docx))
3. Before conducting your analysis of your factory-floor equipment you will first make sure that you have understanding of the types of questions to ask, and information to find out.  
   Review the “Layer” sections and if there are aspects that you are not comfortable with, then try to reach out to your IT dept. If that is not an option, then you may need to simply skip them.
4. Next, prepare by obtaining the necessary tools to help conduct the analysis (see *Analysis Tools Preparation*, below)
5. Conduct your vulnerability analysis on your networked devices (see *Conducting the analysis using analysis tools*, below)  
   **Note**: this step will be time-consuming as you build a documentation register of risks/vulnerabilities for each networked device.
6. Move on to your risk assessment process (see [04 - Risk Register.docx](04%20-%20Risk%20Register.docx))

Finally, delete this page.

# 

# Overview

Cyber-security is a science unto itself and requires a significant level of knowledge and expertise. However, following the conventions in this guide you can more than adequately secure your infrastructure from breaches and attacks originating from within the organization, or externally via the internet etc.

What are we looking for?

* Holes in the network perimeter
* Backdoors
* Vulnerabilities in infrastructure, computers, communications, software, or configuration etc.
* Sabotage attacks
* Communications attacks (man-in-the-middle)

What are we trying to defend against?

* Unauthorized access and disclosure of information, data, configuration, or control
* Unauthorized modification or destruction of information, data, configuration, or control
* Disruption of factory processes that could jeopardize safety or production
* Being used as a launch-pad to conduct attacks on others

How we plan to defend:

* Hardening all systems (network infrastructure, computers, software, and devices, etc.) to remove unnecessary interfaces and capabilities
* Restricting access to all systems that can be restricted physically and/or electronically
* Restricting communications to known/trusted sources only

How we will identify risks and vulnerabilities:

* Utilization of vulnerability scanning software
* Manual analysis based on vulnerability scans along with visual inspection and understanding of systems architecture

This guide will follow the *Defense in Depth* model for conducting an analytical and holistic study of the factory floor system.

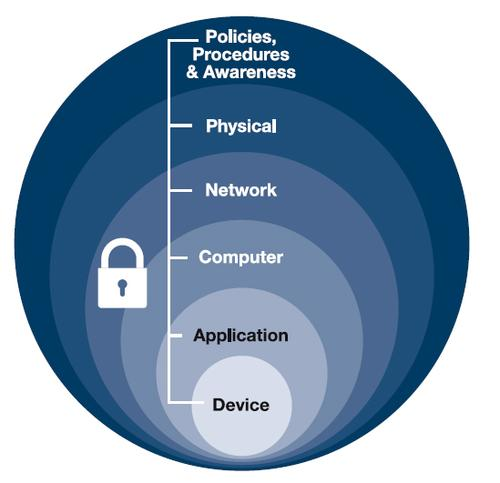
[[1]](#footnote-1)

Figure Defense in Depth Onion

To complement this model, we will also visualize each component using a *Stack* method:

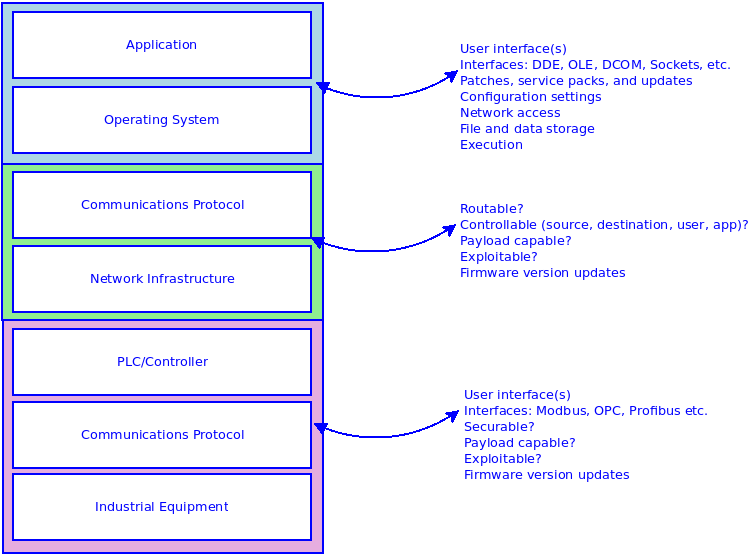


Figure Stack Methodology of Asset Analysis

# Physical Location Layer

Examine the physical premises to determine:

* Entry/exit:
  + Are all doors into the factory floor secured with locks to prevent unauthorized entry?
  + All windows/vents secured to prevent unauthorized entry?
  + Is information regarding entry prominently posted, i.e. for authorized personnel only
  + Does a log of entry exist for visitors and/or employees?
  + Are entry-keys available near the entry ways, e.g. pin numbers or codes on poster?
* Partitioning of offices, production, inventory, and storage etc.:
  + Are offices sufficiently secured to prevent unauthorized entry?
  + Is the production floor sufficiently secured to prevent unauthorized entry? i.e. 2nd door
  + Is there a clean-desk policy in effect and in use?
* Access to equipment:
  + Is device easily accessible, i.e. anybody can literally touch it
  + Is device important to business/production operations?
  + Can device be put behind lock and key, i.e. move to secure room, rack, or closet etc.
  + Regarding device connections:
    - Is the power cable/plug accessible?
    - Is the communications (Ethernet/serial) cable accessible?
    - Are there accessible USB or other ports?
    - Are the cables a hazard, i.e. person could trip over, could be pierced, spliced, etc.?

# Network Infrastructure Layer

Examine the network communications layer for:

* Can a map of the network infrastructure be procured or produced to obtain a list of all equipment showing the connected relationships between:
  + Entry/exit points, i.e. corporate network, internet, dial-in/dial-out, redundant paths
  + Routers and routes
  + Firewalls and rules
  + IDS and rules
  + Computer systems: servers, workstations, laptops, handhelds etc.
  + PLCs/controllers and peripherals, e.g. RS232-to-Ethernet, etc.
  + Industrial equipment
* For each connected device:
  + What is the MAC and IP address? (log it)
  + Can you list which other devices, computers, or software systems require access to/from it?
* Switches, Routers, Firewalls, and any other appliance type:
  + Is the device physically inaccessible to unauthorized personnel?
  + Is the administrative console accessible? If so, is it accessible to anybody from anywhere?
  + Is the firmware up to date or known to contain vulnerabilities?
  + Are the security logs active? Are they forwarded to a central logging source? Is somebody reviewing the logs?
  + Is the device configuration documented, backed-up, reviewed, and under a change-management process?
* Switches:
  + Does the switch implement port-security to restrict port-access to specific network cards?
  + Does the switch block known attacks such as:
    - DHCP guarding to prevent snooping/impersonation
    - MAC address spoofing
    - ARP cache flooding
    - Denial of service
  + Are there devices that must be able to communicate with each other? (deterministic)
  + Are there devices that must not be able to communicate with each other?
  + Are any VLANs configured?
  + Are there any QoS requirements?
* Network cabling:
  + Are cables sufficiently identifiable to know which cable connects a device to a switch?
  + Are cables securely anchored down to prevent accidental damage or destruction?
* Network adapter/cards:
  + Does the NIC (network interface card) require drivers? If so, are they up to date?
  + Do any devices have multiple NICs? If so, then:
    - For redundancy purposes?
    - Each NIC on a separate subnet?
    - Routing permitted between subnets/NICs?
* IP Addressing:
  + Are devices using DHCP or static IP addresses?
  + Which subnet(s) are in use?
  + Are there any routes between subnets?
* Network Access Policy:
  + Can any device connect to the network, assuming physical access is possible?
  + Should any device be able to connect to the network?
  + Are there any restrictions that should be applied to the network connectivity?
  + Is anti-virus required for all computer systems?
  + Is a firewall required for all computer systems and/or devices?
* Domain/workgroup:
  + Is there a domain controller responsible for managing the network?
  + What services does the server provide? Are they required?
  + Is there more than one server?
  + Do all users have a user-account for logging-in to computer systems and the network?
  + Are users generally allowed to access all computers, or specific computers only?
  + Are users generally allowed to login at any time, or specific times only?
  + Are users allowed access to specific network resources? Any resources? No resources?
  + Are users required to use passwords?
  + Is the password policy used for all user accounts?
* Internet:
  + Is there a firewall separating the plant-floor network from the internet connection (perhaps via a corporate network)?
  + Is the internet accessible from the plant-floor network? Should it be?
  + Is the internet connection monitored?
  + Does everybody have access to the internet? Should they?
  + Are there any restrictions to the internet connection, or is all traffic permitted?
  + What traffic should be allowed, and which traffic should absolutely not be allowed?
  + Are there devices that should not be accessible from the internet connection?
* Computer Systems Layer:
  + Is there a modem connection? If so, then:
    - Is it connected to a phone line? Should it be?
    - Can it be disabled?
    - If required, then can anybody dial-out with it? Should they be able to?
    - Is there dial-in capability? Should there be?
    - Can use user dial-in to the computer? Should they be able to? What capabilities does a dial-in user have?
  + Is there a network card/connection?
  + What operating system is installed? Is it up to date with patches?
  + Is automatic operating-system and/or application updates/patches activated? Should it be?
  + Is the computer being backed-up?

# Application Layer

Examine each computer system to identify the software running on it:

* Which operating-system services are installed and configured? For each, consider the following:
  + Is the service necessary? What does it do, what is it for?
  + Is it up to date with the latest service pack and/or patches?
  + How is the service configured?
  + Does the service make information/capabilities available to other systems/users?
  + Is the configuration documented and backed-up?
* What software is installed on the computer? For each product, consider the following:
  + Is it necessary? What does it do, what is it for?
  + Is it up to date with the latest service pack and/or patches?
  + How is the application configured?
  + Can any user use it, or just specific users?
  + What are the application’s capabilities and can they be reduced or controlled?
  + Can the application’s capabilities be restricted by user, e.g. admin vs. user?
  + Is the configuration documented and backed-up?
  + Does the application automatically start on login?
  + Does the application run as a service, or interactively?
  + Does the application expose any interfaces? if so consider the following:
    - What is the interface type, i.e. DDE/FastDDE/Suitelink, OLE, COM/DCOM, REST/JSON, Plain-sockets?
    - Are extensible interfaces available, such as *plugins*?
    - Are any scripting capabilities available? Such as VB, JavaScript, .NET, Python, LUA etc.
  + Where is the application configuration stored? Also consider:
    - Is it accessible to any user?
    - Is the configuration modifiable by any user?
  + Are there any X509 certificate repositories associated to the application? If so, consider:
    - Is the repository available to any user?
    - Can the repository be modified by any user?
  + Can the application do damage if hijacked?
* Are there any application “wrappers” installed to further restrict the capabilities of an application? If so, consider:
  + Which application(s) does it protect?
  + How is it configured?
* Are there any applications that can be centrally administered by a master server?

# Device Layer

Examine each of the industrial devices to determine the possible cyber-security weaknesses. Consider the following:

* Does the device have an Ethernet or WI-FI connection or capability? If so, consider the following:
  + Does the device send or receive data?
  + Is the device a master or slave?
  + Which protocols are supported and which are in use? E.g. Modbus, OPC, Profinet, etc.
* Does the device control other devices/equipment?
* Does the device contain a configuration? If so, consider:
  + - Is it documented?
    - Is it backed-up?
    - Is it accessible to anybody, or select users only?
    - Can it be modified?
* Can the device’s capabilities be restricted? If so, are they?
* Does the device have an accessible firmware? If so, consider:
  + Is the firmware accessible to anybody, or specific users only?
  + Can the firmware be updated?
  + Is the firmware up to date?
  + Is the firmware backed-up to an external/safe location?
* Does the device contain other connections/sockets? If so, consider the following:
  + USB?
    - Is anything connected to the connector? If so, is it necessary?
    - Can USB be disabled?
    - What if somebody changed the connected equipment to something else?
    - Does the device auto-configure and/or auto-run newly connected USB devices/applications?
  + Flash card?
  + RS232?
  + Wiring terminals?
* Ladder logic:
  + Open the ladder logic application
  + Search for the application for the use of variables or input parameters
  + For each parameter that is externally controlled by SCADA, verify that logic is in place to validate input values to ensure they are within safe bounds.

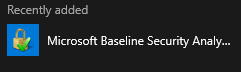
# Analysis tools preparation

There are a many, many security vulnerability analysis tools available. We will use two that are very powerful and freely available; one is for Windows and the other for Linux.

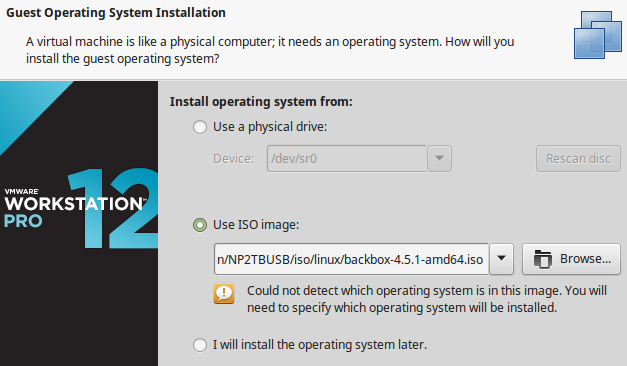
Assumptions made:

* You are using a Windows based laptop
* You have the ability to use virtualized environments (VMware, Hyper-V, VirtualBox, etc.) on that same laptop  
  **Note**: an alternative is to put the security tools on a USB thumb-drive
* You have administrator privileges on your computer and the other computers on the plant-floor

## Windows tool - MBSA

1. Download [Microsoft Baseline Security Analyzer: https:/www.microsoft.com/en-us/download/details.aspx?id=7558](https://www.microsoft.com/en-us/download/details.aspx?id=7558)
2. Double-click the installer and accept all defaults during installation
3. The icon for MBSA should be available in your START menu:   
   

## Linux tool – OpenVAS

1. Download [BackBox](https://backbox.org/download), a complete Linux operating system full of security related tools: <https://backbox.org/download>
2. The download is a CDROM image that you can either burn to CD, or use directly within your virtualization environment. This tutorial will assume VMWare Workstation.
3. In VMWare Workstation, conduct the following:
   1. Click the HOME tab and then Create a new Virtual Machine
   2. Complete the options as desired, but specify the backbox ISO as the installer for the operating system:   
      
   3. Complete the wizard and allow the VM (environment) to boot.
   4. The Linux desktop will be presented. Double-click the “Install BackBox Linux” icon on the desktop.
   5. Simply accept ALL defaults presented during the installation wizard.
   6. At the end of the wizard, allow the VM to reboot to verify the installation is in good order. You should be able to login to the Linux desktop.

# Conducting the analysis using analysis tools

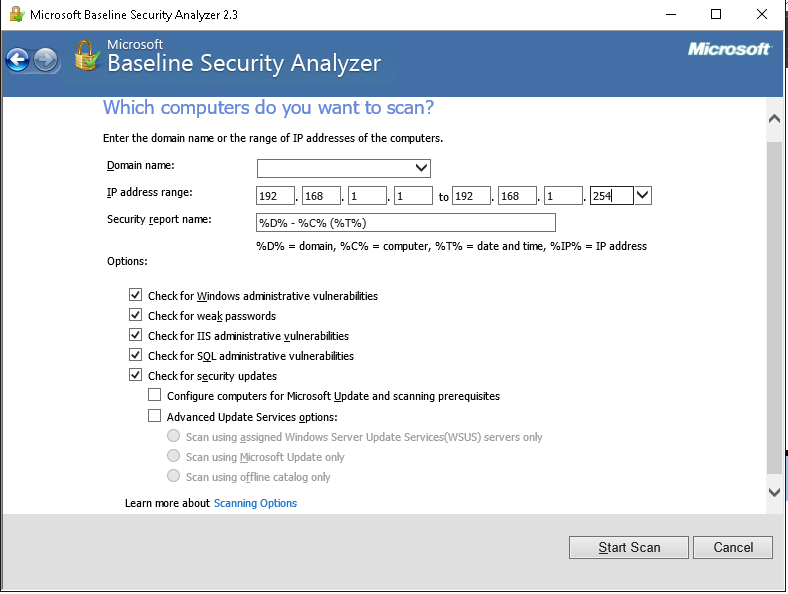
All computer systems should be tested with both MBS and OpenVAS.

All networked devices (infrastructure, industrial equipment, etc.) should be tested with MBSA and OpenVAS with the knowledge that most tests might not be applicable to the target platform.

**Note**: while both tools are relatively easy to use, interpreting their results might not be as easy.

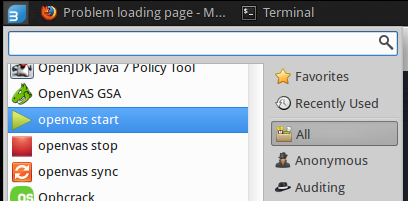
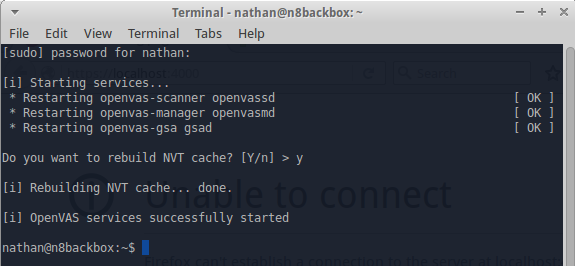
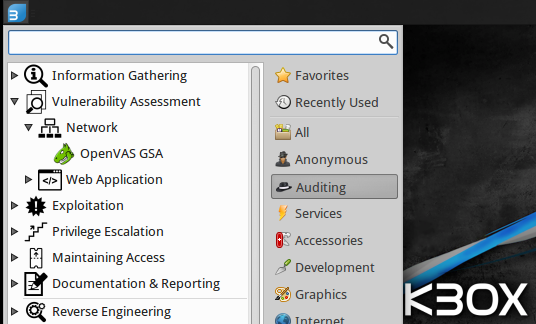
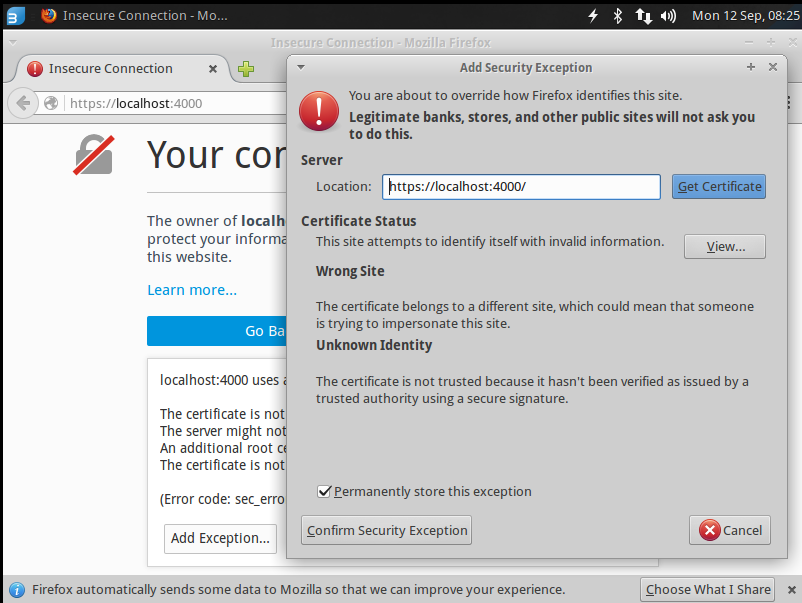
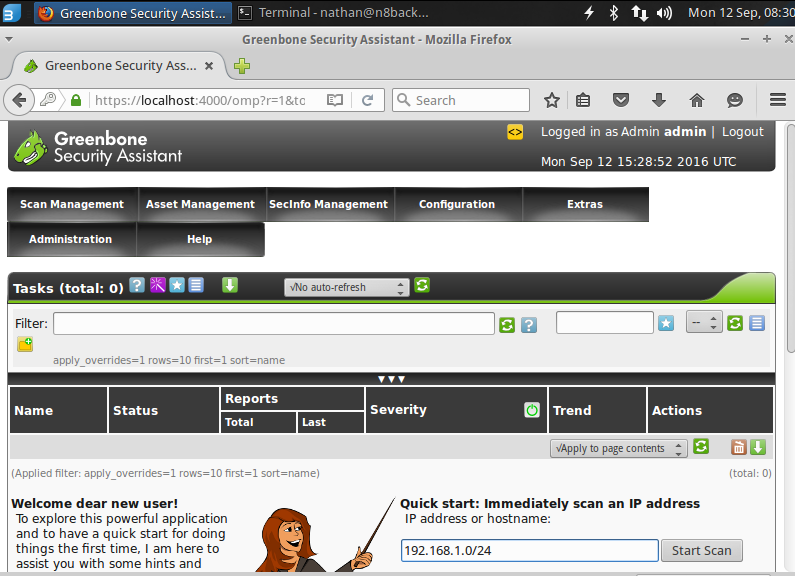
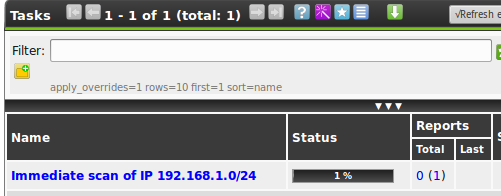
If possible, we will use the tools to scan all equipment on the network. If this is not possible due to network segmentation, then you will need to scan each subnet individually by physically connecting to each subnet.

## Microsoft Baseline Security Analyzer

1. Locate MBS in the START menu and then right-click on it and launch as an administrator (this is important)
2. Click “Scan Multiple Computers” from the home page
3. Enter the IP address range as appropriate:   
   
4. Click “Start Scan” to proceed with testing. This can take a while depending on the number of devices to be scanned.

Save the results.

## OpenVAS

1. Boot into the BackBox VM and wait until the desktop is visible
2. Start the OpenVAS service from the menu by navigating to All > openvas start:   
   
3. A prompt will open where you will need to enter your password.
4. You will be asked to update the cache, select “Y” (yes). This can take a while as the latest tests/signatures are downloaded from the internet.  
   The prompt should look like this:   
     
   Close the terminal window.
5. Launch OpenVAS from the menu and navigating to Auditing > Vulnerability Assessment > Network > OpenVAS GSA:   
   
6. The browser will open but not successfully as the connection is not yet trusted.
7. Click the “Advanced” button and then “Add Exception”.
8. In the “Add Security Exception” dialog ensure the “Permanently store this exception” checkbox is checked and then click “Confirm Security Exception”:   
   
9. The browser will now display a login window where you will enter the following credentials:   
   username: admin  
   password: admin
10. You will now see the main home-screen where you will enter the IP address of a specific device, or range:   
    
11. Using the “Quick start” option (near the bottom of the screen) specify your subnet IP, e.g. 192.168.1.0/24 and then click “Start Scan”.
12. The request will be queued by the worker and then eventually start; this is visible in the “Tasks” section of the same page.
13. Wait for the task to complete. This can take a while to complete, depending upon the number of devices needing to be scanned.  
    Note: you can keep an eye on the task progress, such as:   
    

The results are automatically saved in the OpenVAS database.

# Reviewing the analysis results

Both MBSA and OpenVAS are quite technica and understanding the output may be a little difficult. Ultimately, any major problems will be easily identifiable.

For each computer/device scanned, create a new document based on [06 - Computer Vulnerability and Risk Analysis.dotx](06%20-%20Computer%20Vulnerability%20and%20Risk%20Analysis.dotx). This document contains space for you to specify information about the device, it’s associated relationships, risks, and vulnerabilities.

Once all of the documents exist for each networked device, take them to the risk management group for a team meeting.

1. (Spiegel, 2016) [↑](#footnote-ref-1)