**Download VirtualBox & follow default installation settings**: <https://www.virtualbox.org/>

**Download & Import Windows 11 virtual machine**

Download: <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/> > “Download a virtual machine, VirtualBox modal” <https://aka.ms/windev_VM_virtualbox>

* Download the (zipped) Windows 11 OVA file (40 mins)
* Extract the OVA file (3 mins, 22GB)
* Via VirtualBox, Import the OVA file (10-15 mins, 43GB)

***<Download the rest from your VM>***

**Git**

Download: <https://git-scm.com/downloads>

* Git clone instructions: <https://git-scm.com/docs/git-clone>

**Sysmon**

Download Sysmon Zip file: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

Extract all Zip file contents

Download a config

* Recommended: <https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml>
* Great alternative: <https://raw.githubusercontent.com/SwiftOnSecurity/sysmon-config/master/sysmonconfig-export.xml>

Install Sysmon: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon#examples>

**Sigma Rules public repository**

<https://github.com/SigmaHQ/sigma>

*git clone* [*https://github.com/SigmaHQ/sigma.git*](https://github.com/SigmaHQ/sigma.git)

**Chainsaw**

Recommend downloading the pre-compiled binary: <https://github.com/WithSecureLabs/chainsaw/releases>

* e.g. this version for Windows: <https://github.com/WithSecureLabs/chainsaw/releases/download/v2.6.0/chainsaw_x86_64-pc-windows-msvc.zip>
* Main repo: <https://github.com/WithSecureLabs/chainsaw>
* Wiki (Usage): <https://github.com/WithSecureLabs/chainsaw/wiki/Usage#hunting>
* Clear usage walkthrough: <https://www.vanimpe.eu/2022/08/16/down-the-chainsaw-path-to-analyse-windows-event-logs/>

Key command syntax: *chainsaw\chainsaw.exe hunt evtx\ -s sigma\ --mapping chainsaw\mappings\sigma-event-logs-all.yml*

* Presenter’s example: *chainsaw\chainsaw.exe hunt C:\Windows\System32\winevt\ -s sigma\rules\target\_tests\ --mapping chainsaw\mappings\sigma-event-logs-all.yml*

**Atomic Testing**

Atomic Red Team repository: <https://github.com/redcanaryco/atomic-red-team/>

*git clone* [*https://github.com/redcanaryco/atomic-red-team.git*](https://github.com/redcanaryco/atomic-red-team.git)

Invoke-AtomicRedTeam wiki: <https://github.com/redcanaryco/invoke-atomicredteam/wiki>

Install via PowerShell

* Recommended approach: *Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser*

Import Invoke-AtomicRedTeam module: *Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force*

Key command syntax:

* *Invoke-AtomicTest T1539 -ShowDetailsBrief*
* *Invoke-AtomicTest T1539 -CheckPrereqs*
* *Invoke-AtomicTest T1539 -GetPrereqs*
* *Invoke-AtomicTest T1539 -TestNumbers 2*
  + Output stored at: *C:\Users\User\AppData\Local\Temp*
* Invoke-AtomicTest T1539 -Cleanup

**Optional downloads**

Download & install Chrome

Download & install Firefox

Log in to a credentialed account, e.g. Reddit (suggest a dummy account), accept browser credential saving

Download & install Notepad++ (easier working with Sigma & Atomic Red Team YAML files)