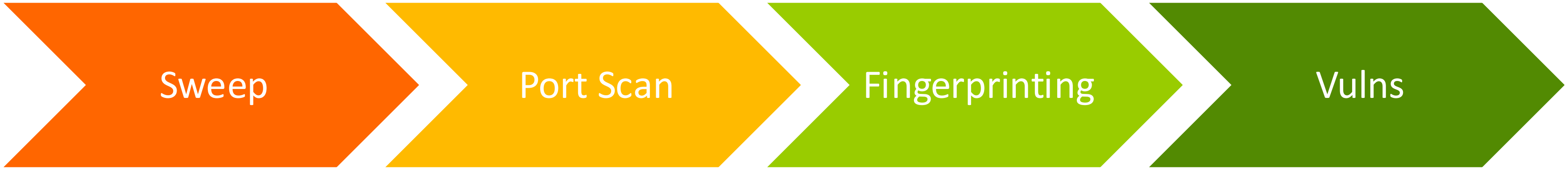
Computer Network Security

COMP 178 | Spring 2024 | University of the Pacific | Jeff Shafer

Penetration Testing: Vulnerability Scanning

Types of Network Scans

- Sweeps/Traces
  - Send out a small number of probes to each IP address and listen for reply
  - Make note of active systems
  - Attempt to deduce network topology



Sweep

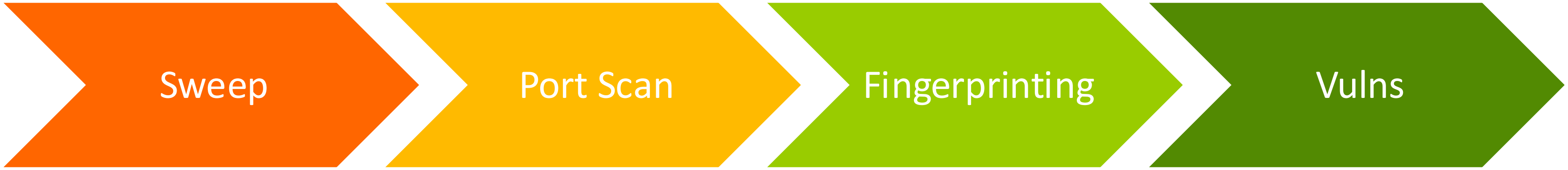
Port Scan

Fingerprinting

Vulns

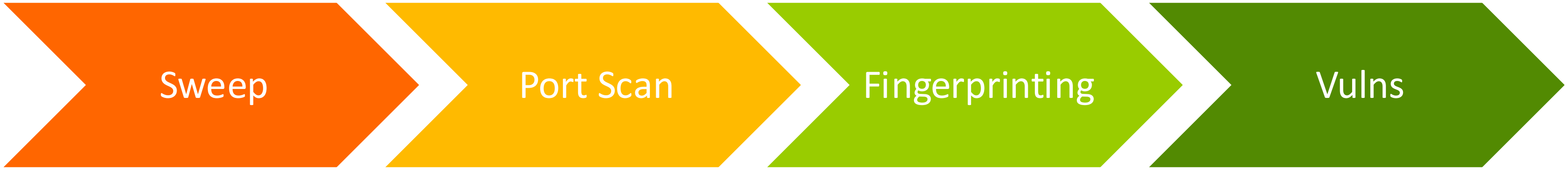
Types of Network Scans

- Port scans
  - Send out a larger number of probes to each *active* IP address and listen for reply
  - Make note of TCP and UDP ports that are listening



Types of Network Scans

- OS Fingerprinting and Version Scanning
  - Send a *larger* number of probes to active hosts with listening ports
  - Deduce the operating system of the host by closely examining the replies
  - Deduce the installed software and version of active network services on the host



Sweep

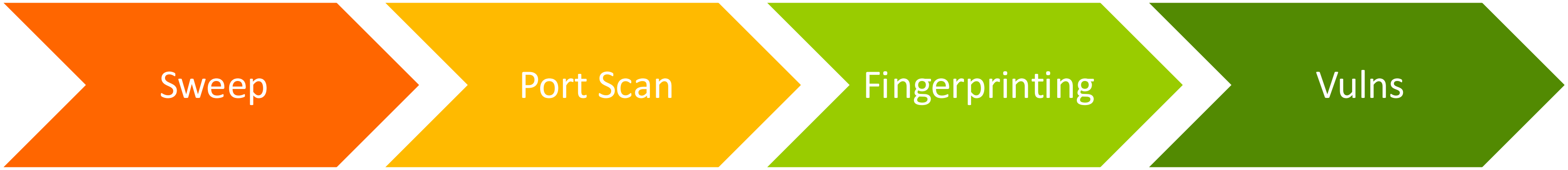
Port Scan

Fingerprinting

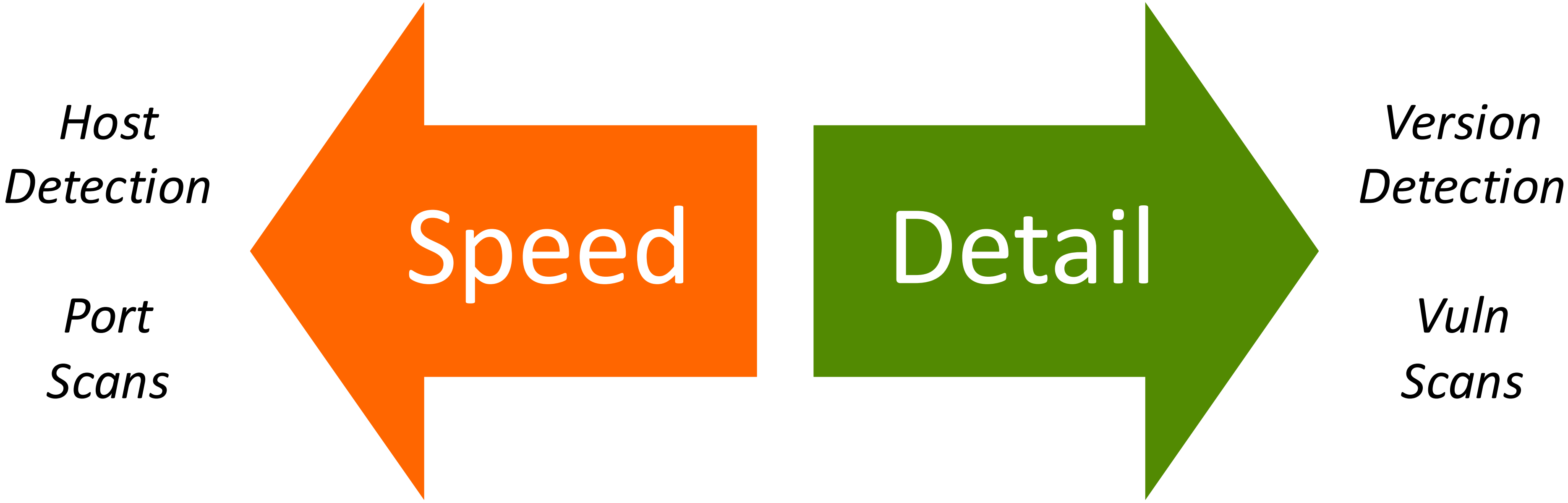
Vulns

Types of Network Scans

- Vulnerability Scanning
  - Armed with lists of active hosts, their OS, and network services, check for known vulnerabilities or common misconfigurations
  - Classify vulnerabilities by category and severity
  - (Potentially) present information on methods to mitigate / eliminate weakness
  - **Useful for both pen testers and sysadmins**



Scanning



Host Detection

Port Scans

Speed

Detail

Version Detection

Vuln Scans

Vulnerability Scanning

- Possible methods for vulnerability scanning
  - Check version numbers and compare against known lists of vulnerabilities
    - Caveat that software might be vulnerable but a firewall or IDS prevents exploitation
    - Patches may be backported to prior versions
  - Check protocol spoken and compare against known protocol (if an older protocol was vulnerable)
  - Examine program behavior and compare to known-vulnerable behavior

Vulnerability Scanning

- Can also check if system is vulnerable **by attempting to exploit vulnerability**
  - A success will 100% confirm vulnerability!
  - Does a failure prove not vulnerable? Probably not…
- **Higher risk** activity than simply checking version numbers against lists of known vulnerabilities

Vulnerability Scanners

- General architecture
  - Scanning engine - Generates arbitrary network packets, handles multiple threads & concurrency, handles timeouts & failures, aggregates results, etc.
  - Plugins for each and every vulnerability being searched for
- Vulnerability scanners require constant effort (by developers) to keep up to date with latest threats
  - **$$$**

Vulnerability Scanners

- Deployment considerations
  - Scanning from **outside network**? (i.e., public Internet)
    - Scans reflect same view of network that attackers will (initially) see
    - Slow
  - Scanning from **inside network**?
    - Less interference from firewalls and IDS
    - Faster
    - More complete view of network?
    - Challenge of getting scanning tools *inside* target network
  - Credentials to test from **within hosts?**

Vulnerability Scanners

Vulnerability Scanners

Commercial

- **Nessus**
- Industry standard / must-have if you can bill this expense to your company or client
- Nessus Professional
  - Annual subscription - **$3990**
- Nessus Essentials
  - Free home/education version (limited to 16 IPs)

https://www.tenable.com/products/nessus

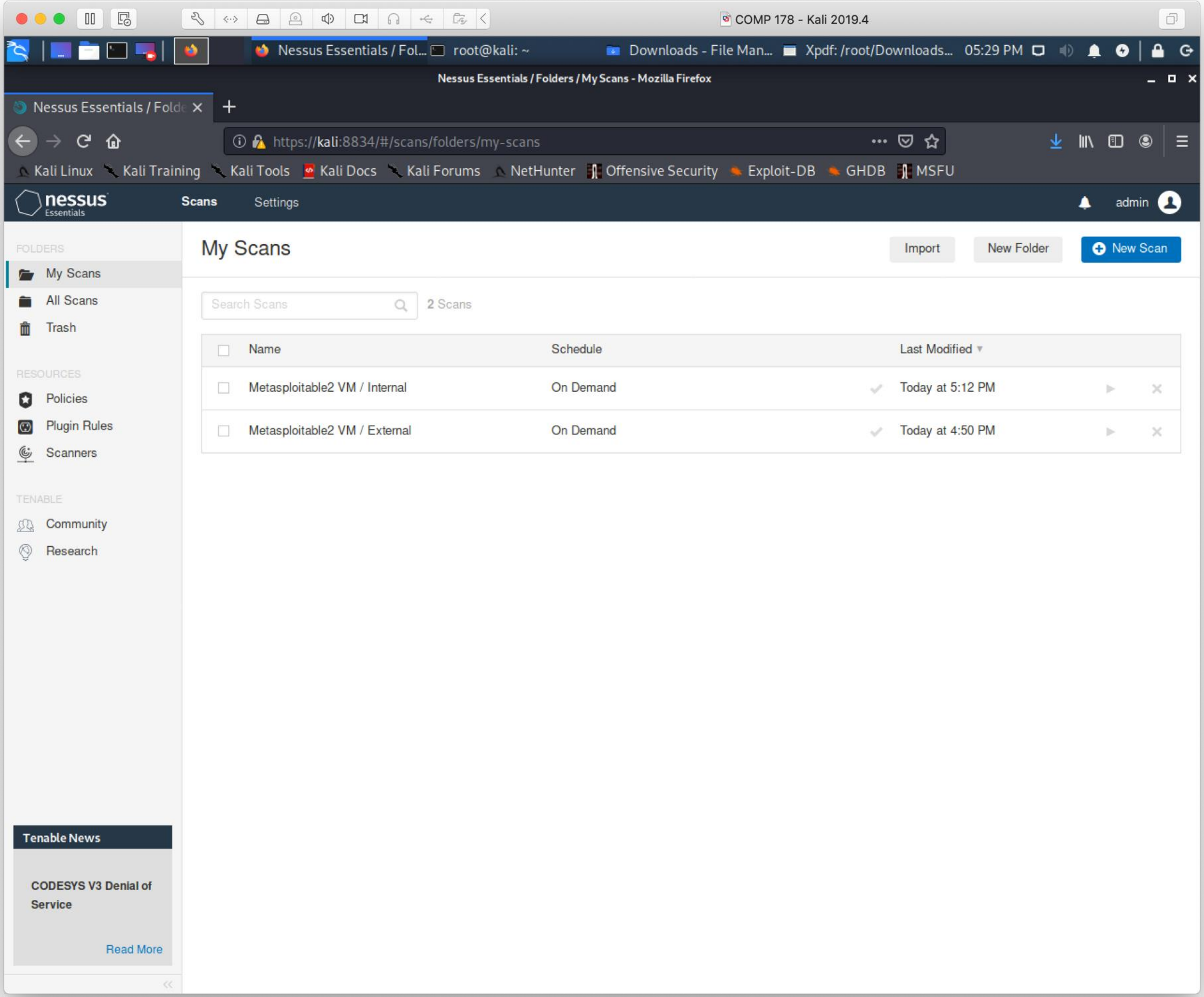
Free

- **OpenVAS**
  - Open **V**ulnerability **A**ssessment **S**canner
- Open source fork of Nessus from 2005 *before* it went commercial
- Regular updates to Network Vulnerability Tests (NVTs)
  - 150,000+ tests

https://openvas.org/

Vulnerability Scanners

- Many other vulnerability scanners
  - **Rapid7 Nexpose** ($)
    - https://www.rapid7.com/products/nexpose/
  - **Core Impact** ($)
    - https://www.coresecurity.com/core-impact
  - **Tripwire IP360** ($)
    - https://www.tripwire.com/products/tripwire-ip360/
  - **…**
- Design question: Do you want your scanner “on premise” or “in the cloud”
  - Vendors happy to take your $$ either way!

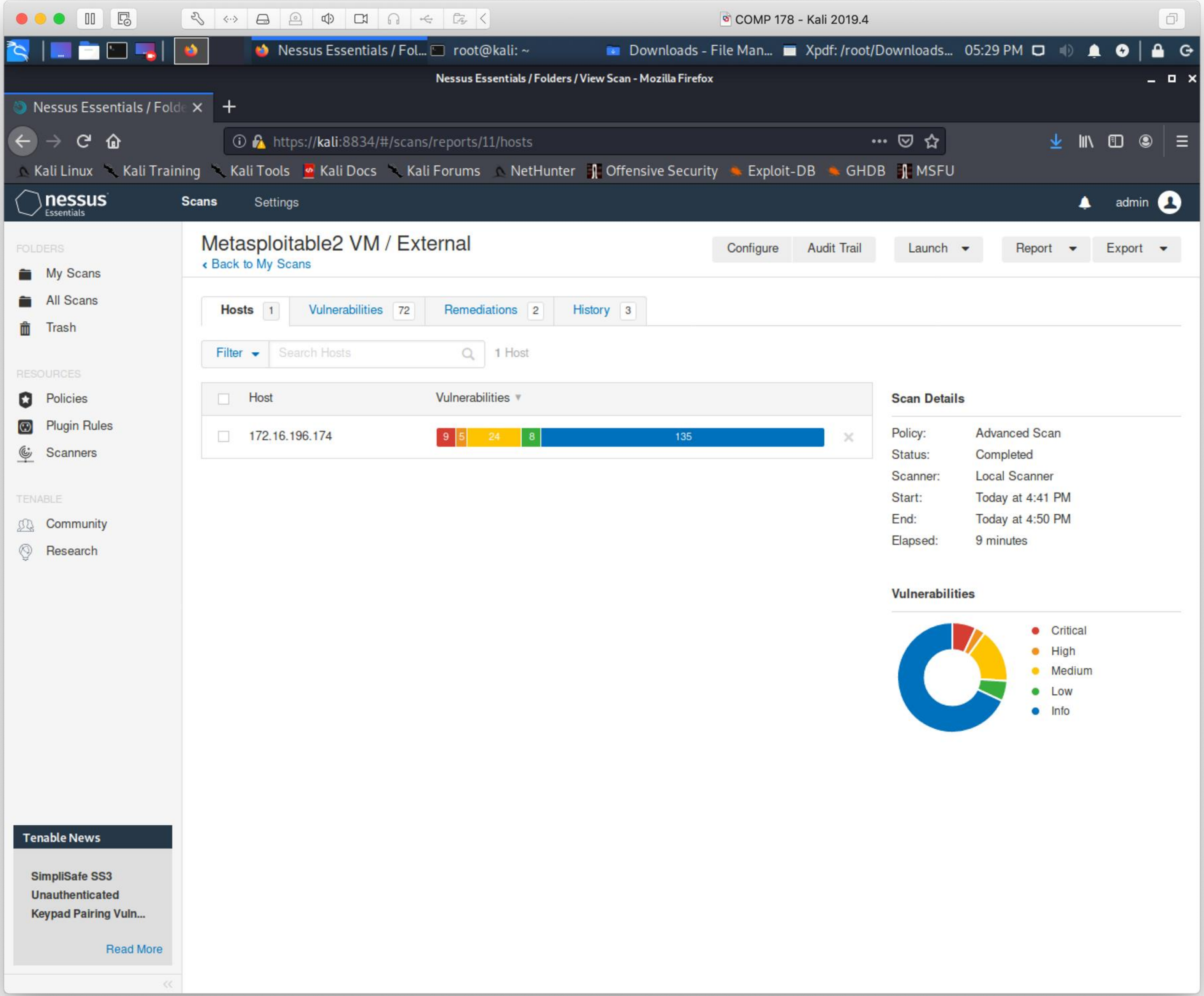


My Scans

2 Scans

□	Name	Schedule	Last Modified ▾
□	Metasploitable2 VM / Internal	On Demand	Today at 5:12 PM
□	Metasploitable2 VM / External	On Demand	Today at 4:50 PM

CODESYS V3 Denial of Service



COMP 178 - Kali 2019.4
Nessus Essentials / Fol... | root@kali: ~ | Downloads - File Man... | Xpdf: /root/Downloads... | 05:29 PM
Nessus Essentials / Folders / View Scan - Mozilla Firefox
https://kali:8834/#/scans/reports/11/hosts
Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU
nessus Essentials | Scans | Settings | admin
FOLDERS | My Scans | All Scans | Trash
RESOURCES | Policies | Plugin Rules | Scanners
TENABLE | Community | Research
Configure | Audit Trail | Launch | Report | Export
Hosts 1 | Vulnerabilities 72 | Remediations 2 | History 3
Filter | Search Hosts | 1 Host
Critical | High | Medium | Low | Info
Tenable News | SimpliSafe SS3 Unauthenticated Keypad Pairing Vuln... | Read More

Metasploitable2 VM / External

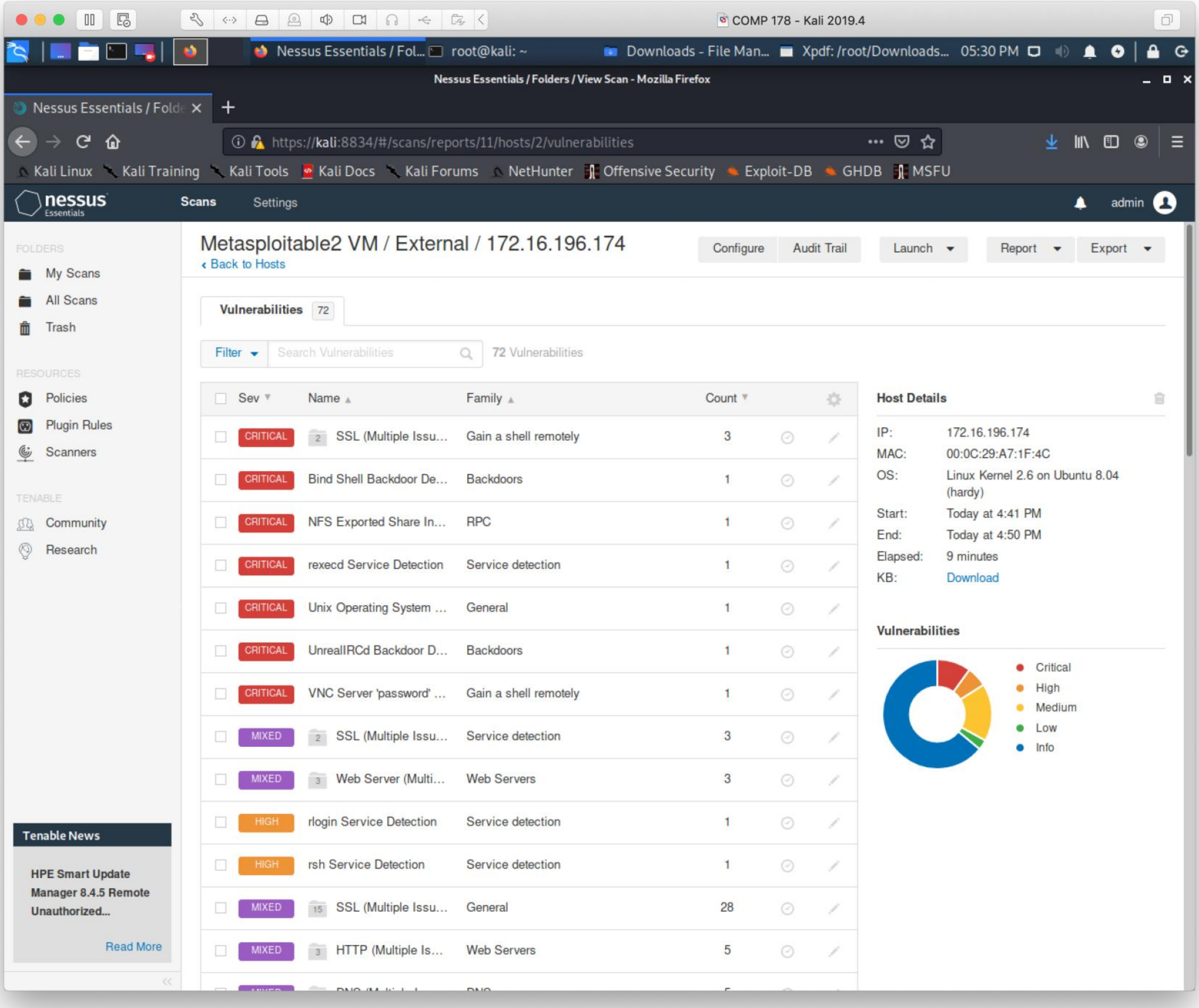
‹ Back to My Scans

Host	Vulnerabilities
172.16.196.174	9 | 5 | 24 | 8 | 135

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 4:41 PM
End:	Today at 4:50 PM
Elapsed:	9 minutes

Vulnerabilities



Metasploitable2 VM / External / 172.16.196.174

‹ Back to Hosts

Vulnerabilities 72

72 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	2 SSL (Multiple Issu...	Gain a shell remotely	3
CRITICAL	Bind Shell Backdoor De...	Backdoors	1
CRITICAL	NFS Exported Share In...	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System ...	General	1
CRITICAL	UnrealIRCd Backdoor D...	Backdoors	1
CRITICAL	VNC Server 'password' ...	Gain a shell remotely	1
MIXED	2 SSL (Multiple Issu...	Service detection	3
MIXED	3 Web Server (Multi...	Web Servers	3
HIGH	rlogin Service Detection	Service detection	1
HIGH	rsh Service Detection	Service detection	1
MIXED	15 SSL (Multiple Issu...	General	28
MIXED	3 HTTP (Multiple Is...	Web Servers	5
MIXED	DNS (Multiple I...	DNS	5

Host Details

IP: 172.16.196.174
MAC: 00:0C:29:A7:1F:4C
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 4:41 PM
End: Today at 4:50 PM
Elapsed: 9 minutes
KB: Download

Vulnerabilities

Tenable News

HPE Smart Update Manager 8.4.5 Remote Unauthorized...

Read More

Next Steps

- Presentation Proposal
- Lab 3 – Scanning with Nmap
- Lab 4 – Vulnerability Scanning