SIMPLIFY PENTEST WORKFLOWS USING CERNO

Chris Traynor

$ whoami

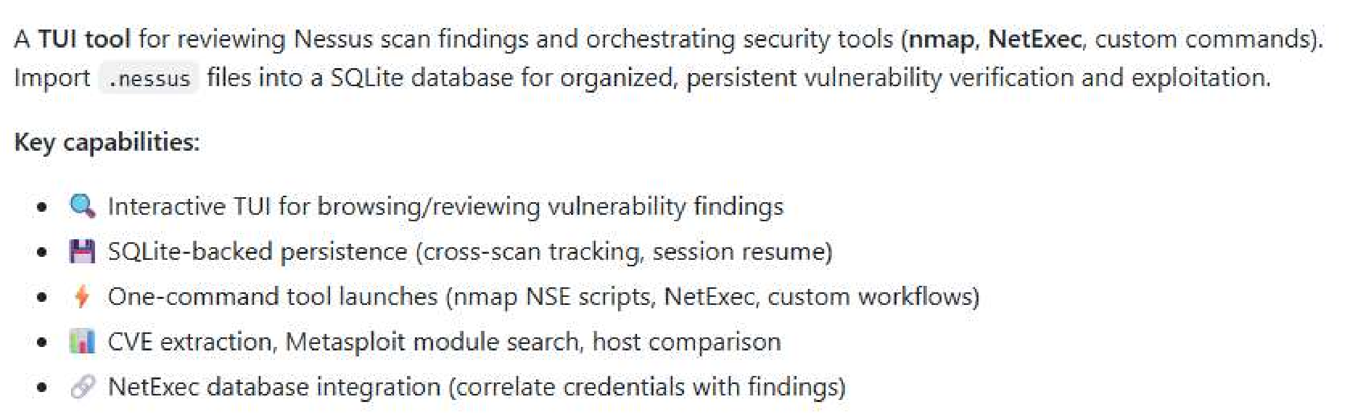
Chris Traynor

- Pentester at Black Hills InfoSec
- Owner of Ridgeback InfoSec, LLC
- Antisyphon Author/Instructor
  - Offensive Tooling Foundations
  - Offensive Tooling for Operators
  - BOTH now available via On-Demand**
- Certs: GSEC, GCIH, GWAPT, & GPEN
- @cstraynor

Cerno

Modern Nessus Review & Security Tool Orchestration

- By Ridgeback InfoSec
- Open Source CLI/TUI Tool
- github.com/ridgebackinfosec/cerno



A **TUI tool** for reviewing Nessus scan findings and orchestrating security tools (**nmap**, **NetExec**, custom commands). Import `.nessus` files into a SQLite database for organized, persistent vulnerability verification and exploitation.

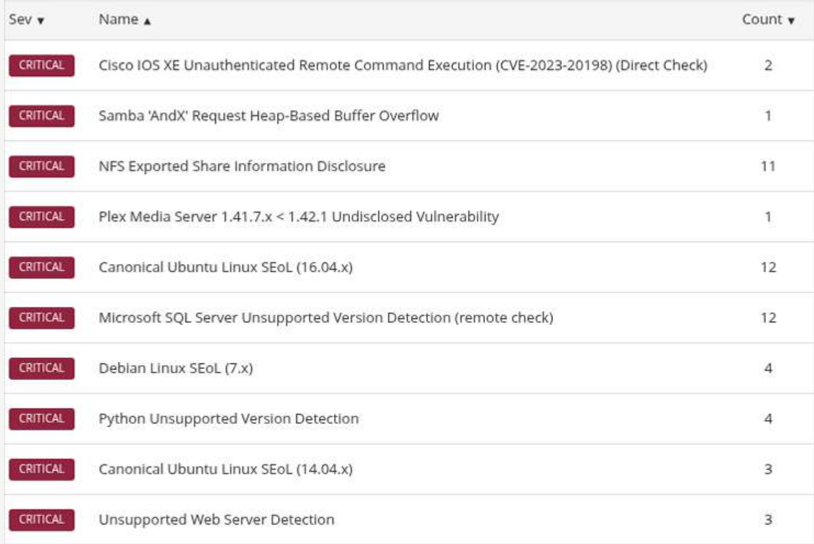
Key capabilities:

- 🔍 Interactive TUI for browsing/reviewing vulnerability findings
- 💾 SQLite-backed persistence (cross-scan tracking, session resume)
- ⚡ One-command tool launches (nmap NSE scripts, NetExec, custom workflows)
- 📊 CVE extraction, Metasploit module search, host comparison
- 🔗 NetExec database integration (correlate credentials with findings)

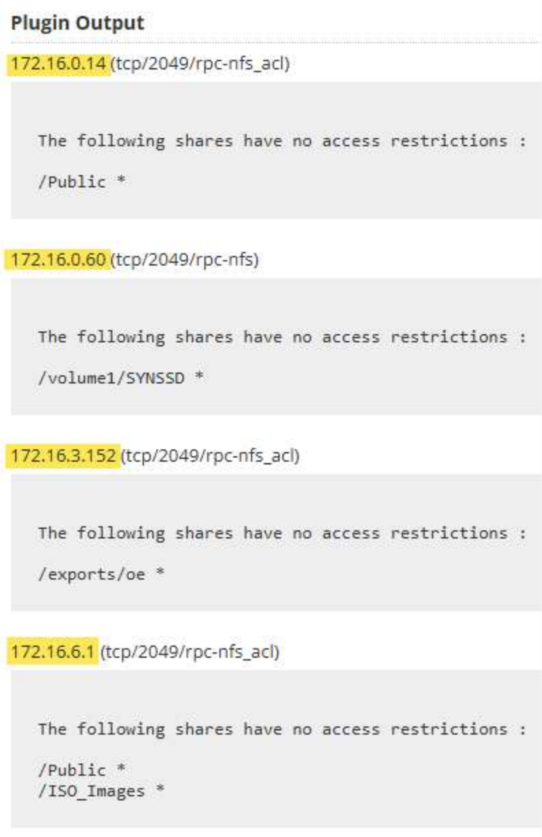
The Problem

The Manual Nessus Review/Verification Struggle

- Thousands of findings across hundreds of hosts
- Context switching between Nessus UI and terminal tools
- No persistent tracking of reviewed findings
- Copy-paste IP addresses and ports for each tool command
- Lost progress when terminals close or sessions end



Sev ▾	Name ▴	Count ▾
CRITICAL	Cisco IOS XE Unauthenticated Remote Command Execution (CVE-2023-20198) (Direct Check)	2
CRITICAL	Samba 'AndX' Request Heap-Based Buffer Overflow	1
CRITICAL	NFS Exported Share Information Disclosure	11
CRITICAL	Plex Media Server 1.41.7.x < 1.42.1 Undisclosed Vulnerability	1
CRITICAL	Canonical Ubuntu Linux SEoL (16.04.x)	12
CRITICAL	Microsoft SQL Server Unsupported Version Detection (remote check)	12
CRITICAL	Debian Linux SEoL (7.x)	4
CRITICAL	Python Unsupported Version Detection	4
CRITICAL	Canonical Ubuntu Linux SEoL (14.04.x)	3
CRITICAL	Unsupported Web Server Detection	3



Plugin Output

172.16.0.14 (tcp/2049/rpc-nfs_acl)

```
The following shares have no access restrictions :

/Public *
```

172.16.0.60 (tcp/2049/rpc-nfs)

```
The following shares have no access restrictions :

/volume1/SYNSSD *
```

172.16.3.152 (tcp/2049/rpc-nfs_acl)

```
The following shares have no access restrictions :

/exports/oe *
```

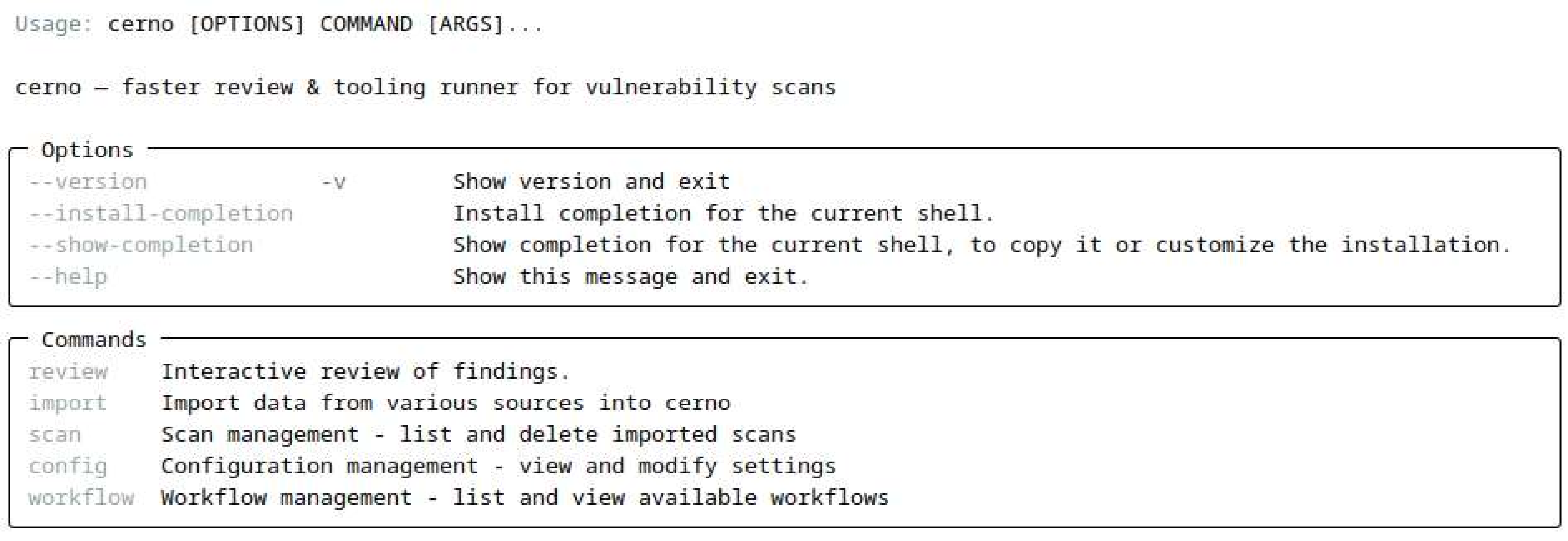
172.16.6.1 (tcp/2049/rpc-nfs_acl)

```
The following shares have no access restrictions :

/Public *
/ISO_Images *
```

The Solution

Cerno: Discern What Matters

- Import .nessus files into SQLite database (single source of truth)
- Interactive TUI with keyboard-driven navigation
- One-command tool launches against exact hosts/ports
- Persistent session tracking (resume where you left off)
- Cross-scan analysis and host tracking

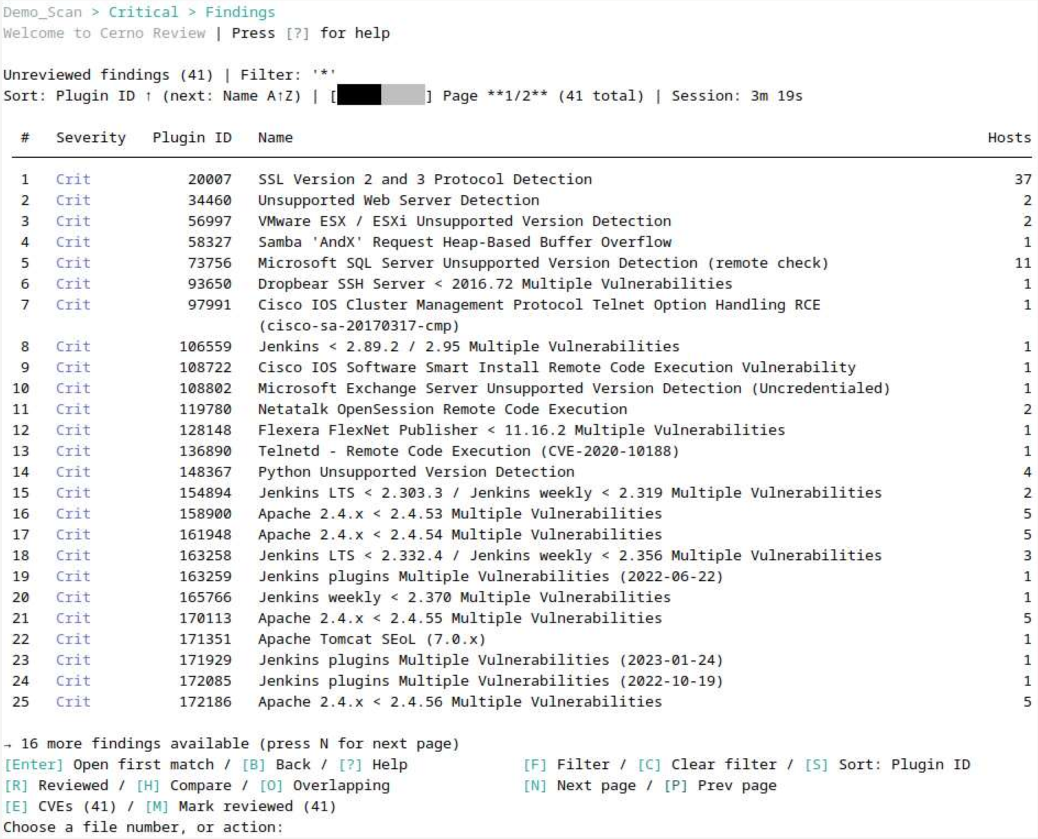


```
Usage: cerno [OPTIONS] COMMAND [ARGS]...

cerno — faster review & tooling runner for vulnerability scans

┌ Options ────────────────────────────────────────────────────────────────────────────────────────────────────┐
│ --version              -v        Show version and exit                                                      │
│ --install-completion             Install completion for the current shell.                                  │
│ --show-completion                Show completion for the current shell, to copy it or customize the installation. │
│ --help                           Show this message and exit.                                                │
└─────────────────────────────────────────────────────────────────────────────────────────────────────────────┘
┌ Commands ───────────────────────────────────────────────────────────────────────────────────────────────────┐
│ review    Interactive review of findings.                                                                   │
│ import    Import data from various sources into cerno                                                       │
│ scan      Scan management - list and delete imported scans                                                  │
│ config    Configuration management - view and modify settings                                               │
│ workflow  Workflow management - list and view available workflows                                           │
└─────────────────────────────────────────────────────────────────────────────────────────────────────────────┘
```

Feature Overview

Key Capabilities

- Interactive Rich-based TUI with color-coded severity levels
- Tool orchestration: nmap (NSE profiles), NetExec, Metasploit, custom commands
- CVE extraction and Metasploit module search
- Host comparison and overlapping findings analysis
- NetExec database integration (credential correlation) [Beta]
- Custom workflow mappings for plugin-specific verification

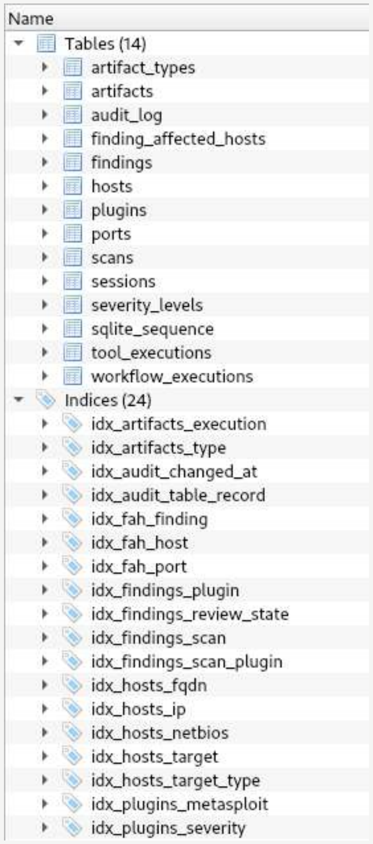


```
Demo_Scan > Critical > Findings
Welcome to Cerno Review | Press [?] for help

Unreviewed findings (41) | Filter: '*'
Sort: Plugin ID ↑ (next: Name A↑Z) | [█████░░░░░] Page **1/2** (41 total) | Session: 3m 19s

  #   Severity   Plugin ID   Name                                                                   Hosts
 ─────────────────────────────────────────────────────────────────────────────────────────────────────────
  1   Crit           20007   SSL Version 2 and 3 Protocol Detection                                    37
  2   Crit           34460   Unsupported Web Server Detection                                           2
  3   Crit           56997   VMware ESX / ESXi Unsupported Version Detection                            2
  4   Crit           58327   Samba 'AndX' Request Heap-Based Buffer Overflow                            1
  5   Crit           73756   Microsoft SQL Server Unsupported Version Detection (remote check)         11
  6   Crit           93650   Dropbear SSH Server < 2016.72 Multiple Vulnerabilities                     1
  7   Crit           97991   Cisco IOS Cluster Management Protocol Telnet Option Handling RCE           1
                             (cisco-sa-20170317-cmp)
  8   Crit          106559   Jenkins < 2.89.2 / 2.95 Multiple Vulnerabilities                           1
  9   Crit          108722   Cisco IOS Software Smart Install Remote Code Execution Vulnerability       1
 10   Crit          108802   Microsoft Exchange Server Unsupported Version Detection (Uncredentialed)   1
 11   Crit          119780   Netatalk OpenSession Remote Code Execution                                 2
 12   Crit          128148   Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities               1
 13   Crit          136890   Telnetd - Remote Code Execution (CVE-2020-10188)                           1
 14   Crit          148367   Python Unsupported Version Detection                                       4
 15   Crit          154894   Jenkins LTS < 2.303.3 / Jenkins weekly < 2.319 Multiple Vulnerabilities    2
 16   Crit          158900   Apache 2.4.x < 2.4.53 Multiple Vulnerabilities                             5
 17   Crit          161948   Apache 2.4.x < 2.4.54 Multiple Vulnerabilities                             5
 18   Crit          163258   Jenkins LTS < 2.332.4 / Jenkins weekly < 2.356 Multiple Vulnerabilities    3
 19   Crit          163259   Jenkins plugins Multiple Vulnerabilities (2022-06-22)                      1
 20   Crit          165766   Jenkins weekly < 2.370 Multiple Vulnerabilities                            1
 21   Crit          170113   Apache 2.4.x < 2.4.55 Multiple Vulnerabilities                             5
 22   Crit          171351   Apache Tomcat SEoL (7.0.x)                                                 1
 23   Crit          171929   Jenkins plugins Multiple Vulnerabilities (2023-01-24)                      1
 24   Crit          172085   Jenkins plugins Multiple Vulnerabilities (2022-10-19)                      1
 25   Crit          172186   Apache 2.4.x < 2.4.56 Multiple Vulnerabilities                             5

→ 16 more findings available (press N for next page)
[Enter] Open first match / [B] Back / [?] Help           [F] Filter / [C] Clear filter / [S] Sort: Plugin ID
[R] Reviewed / [H] Compare / [O] Overlapping             [N] Next page / [P] Prev page
[E] CVEs (41) / [M] Mark reviewed (41)
Choose a file number, or action:
```

Database-First Design

SQLite as Single Source of Truth

- Location: ~/.cerno/cerno.db (global, cross-scan)
- Fully normalized schema with foreign key constraints
- Computed statistics via SQL views (no redundant data)
- Foundation tables: severity_levels, artifact_types, hosts, ports
- Cross-scan tracking: "show all findings for host X across all scans"

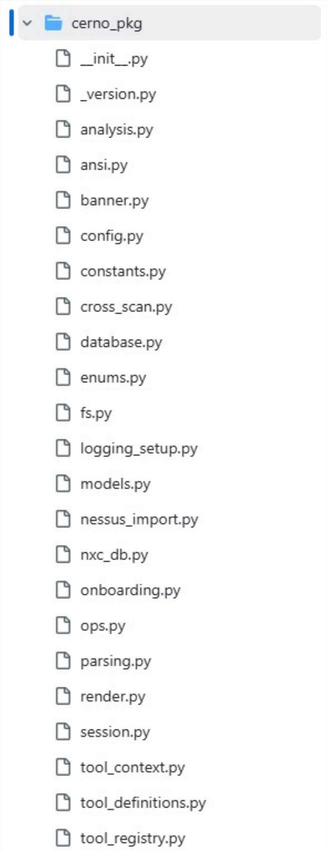


Name
- Tables (14)
  - artifact_types
  - artifacts
  - audit_log
  - finding_affected_hosts
  - findings
  - hosts
  - plugins
  - ports
  - scans
  - sessions
  - severity_levels
  - sqlite_sequence
  - tool_executions
  - workflow_executions
- Indices (24)
  - idx_artifacts_execution
  - idx_artifacts_type
  - idx_audit_changed_at
  - idx_audit_table_record
  - idx_fah_finding
  - idx_fah_host
  - idx_fah_port
  - idx_findings_plugin
  - idx_findings_review_state
  - idx_findings_scan
  - idx_findings_scan_plugin
  - idx_hosts_fqdn
  - idx_hosts_ip
  - idx_hosts_netbios
  - idx_hosts_target
  - idx_hosts_target_type
  - idx_plugins_metasploit
  - idx_plugins_severity

Module Architecture

Clean Separation of Concerns

- cerno.py - CLI entry point (Typer commands)
- nessus_import.py - XML parsing and database import
- render.py - Rich UI tables, panels, menus
- tui.py - Interactive navigation and action handlers
- tools.py - Command builders and tool orchestration
- analysis.py - Host comparison, superset detection

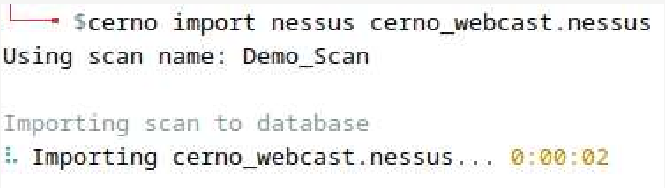


```
cerno_pkg
    __init__.py
    _version.py
    analysis.py
    ansi.py
    banner.py
    config.py
    constants.py
    cross_scan.py
    database.py
    enums.py
    fs.py
    logging_setup.py
    models.py
    nessus_import.py
    nxc_db.py
    onboarding.py
    ops.py
    parsing.py
    render.py
    session.py
    tool_context.py
    tool_definitions.py
    tool_registry.py
```

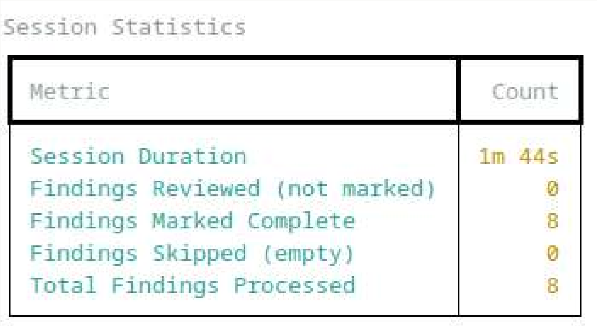
Data Flow

From Nessus to Verified Finding

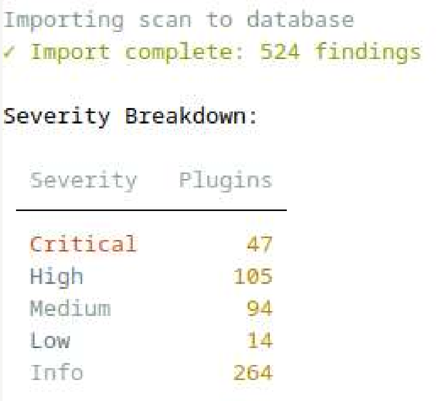
- Import: .nessus XML parsed, hosts/ports normalized into database
- Review: Query findings by severity, display in Rich tables
- Tool Execution: Pass host/port data to nmap/NetExec/MSF
- Track Results: Tool executions and artifacts logged in database
- Resume: Session state persists across terminal closures



```
└──▪ $cerno import nessus cerno_webcast.nessus
Using scan name: Demo_Scan

Importing scan to database
⠇ Importing cerno_webcast.nessus... 0:00:02
```



```
Session Statistics
┏━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━┳━━━━━━━━┓
┃ Metric                         ┃  Count ┃
┡━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━╇━━━━━━━━┩
│ Session Duration               │ 1m 44s │
│ Findings Reviewed (not marked) │      0 │
│ Findings Marked Complete       │      8 │
│ Findings Skipped (empty)       │      0 │
│ Total Findings Processed       │      8 │
└────────────────────────────────┴────────┘
```

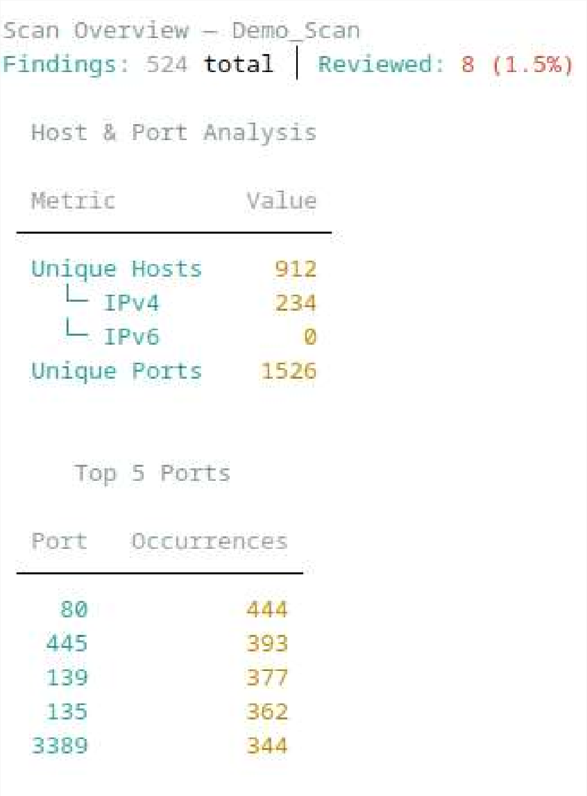


```
Importing scan to database
✓ Import complete: 524 findings

Severity Breakdown:

  Severity   Plugins
 ─────────────────────
  Critical        47
  High           105
  Medium          94
  Low             14
  Info           264
```

Interactive TUI

Keyboard-Driven Review Interface

- Severity selection: 1-5 for levels, M for Metasploit, W for workflows
- Finding list: N/P pagination, F filter, S sort, H host compare
- Detail view: V view hosts, E CVEs, T tools, W workflow, M mark reviewed
- Responsive layouts adapt to terminal width
- Press ? for context-sensitive help anywhere

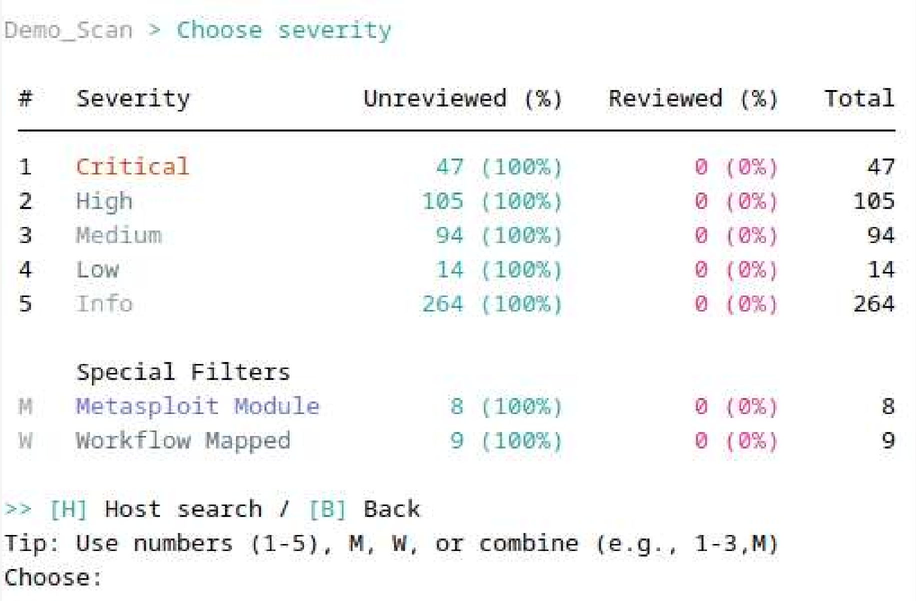


```
Scan Overview — Demo_Scan
Findings: 524 total │ Reviewed: 8 (1.5%)

 Host & Port Analysis

 Metric            Value
─────────────────────────
 Unique Hosts        912
   └─ IPv4           234
   └─ IPv6             0
 Unique Ports       1526


    Top 5 Ports

 Port   Occurrences
───────────────────────
  80            444
 445            393
 139            377
 135            362
 3389           344
```

Severity Filtering

Prioritize What Matters

- Color-coded: Critical (red), High (yellow), Medium (blue), Low (green), Info (cyan)
- Review progress tracking per severity level
- Special filters: [M] Metasploit modules, [W] Workflow mapped
- Sort modes: Severity, Plugin ID, Name, Host count
- Text filtering with partial matching

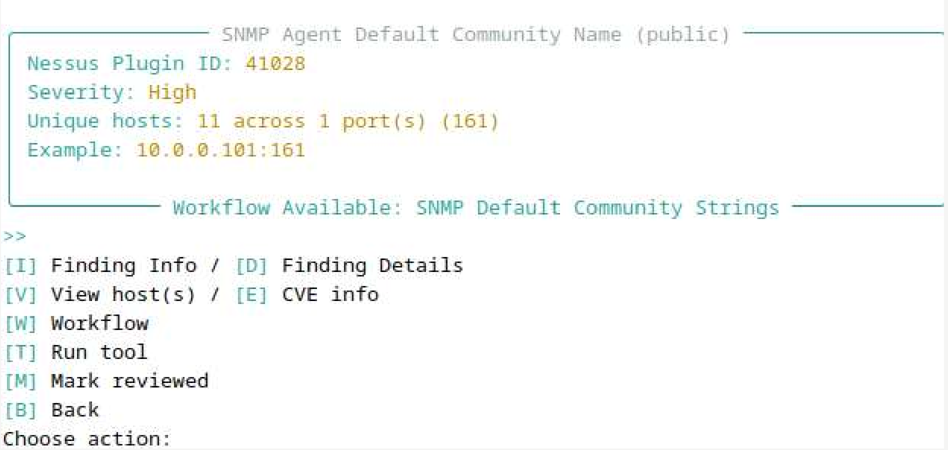


```
Demo_Scan > Choose severity

 #   Severity              Unreviewed (%)   Reviewed (%)   Total
 ──────────────────────────────────────────────────────────────
 1   Critical                  47 (100%)         0 (0%)       47
 2   High                     105 (100%)         0 (0%)      105
 3   Medium                    94 (100%)         0 (0%)       94
 4   Low                       14 (100%)         0 (0%)       14
 5   Info                     264 (100%)         0 (0%)      264

     Special Filters
 M   Metasploit Module          8 (100%)         0 (0%)        8
 W   Workflow Mapped            9 (100%)         0 (0%)        9

>> [H] Host search / [B] Back
Tip: Use numbers (1-5), M, W, or combine (e.g., 1-3,M)
Choose:
```

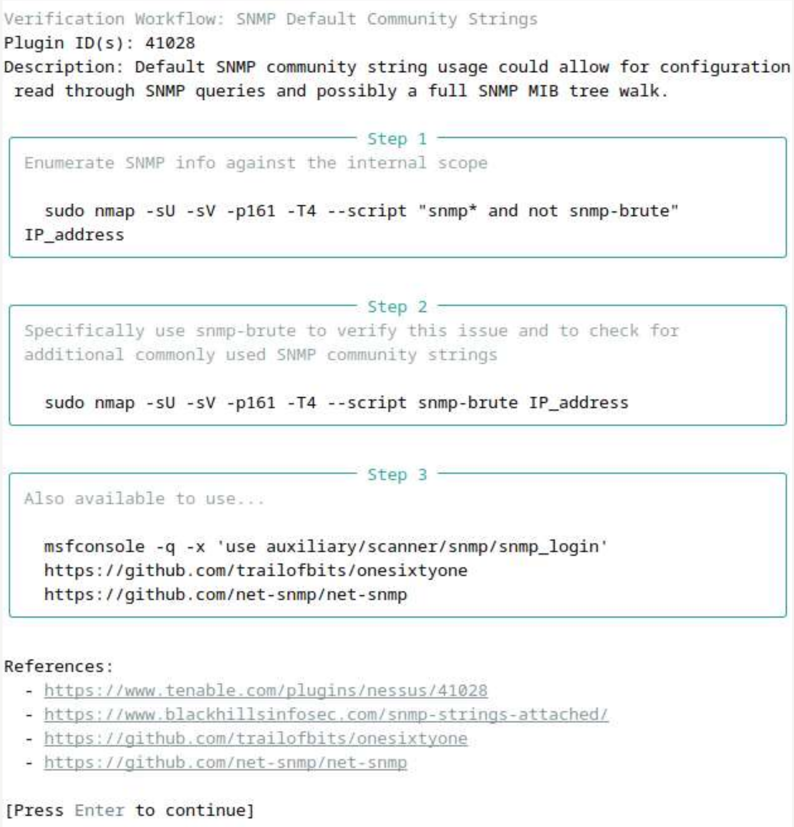
Finding Review

Get To Verifying – Level-Up Your Workflow

- Focus on specific findings
- Affected hosts, Nessus output details, CVE info, & MORE!
- Get flags for existing Metasploit modules & mapped Workflows



```
──────────── SNMP Agent Default Community Name (public) ────────────
 Nessus Plugin ID: 41028
 Severity: High
 Unique hosts: 11 across 1 port(s) (161)
 Example: 10.0.0.101:161

─────────── Workflow Available: SNMP Default Community Strings ───────────
>>
[I] Finding Info / [D] Finding Details
[V] View host(s) / [E] CVE info
[W] Workflow
[T] Run tool
[M] Mark reviewed
[B] Back
Choose action:
```

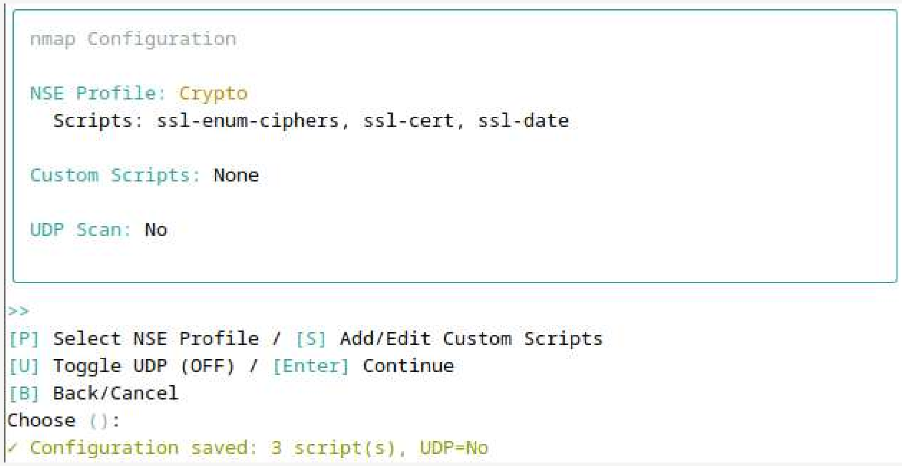


```
Verification Workflow: SNMP Default Community Strings
Plugin ID(s): 41028
Description: Default SNMP community string usage could allow for configuration
 read through SNMP queries and possibly a full SNMP MIB tree walk.

──────────────────────────── Step 1 ────────────────────────────
 Enumerate SNMP info against the internal scope

   sudo nmap -sU -sV -p161 -T4 --script "snmp* and not snmp-brute"
 IP_address

──────────────────────────── Step 2 ────────────────────────────
 Specifically use snmp-brute to verify this issue and to check for
 additional commonly used SNMP community strings

   sudo nmap -sU -sV -p161 -T4 --script snmp-brute IP_address

──────────────────────────── Step 3 ────────────────────────────
 Also available to use...

   msfconsole -q -x 'use auxiliary/scanner/snmp/snmp_login'
   https://github.com/trailofbits/onesixtyone
   https://github.com/net-snmp/net-snmp

References:
  - https://www.tenable.com/plugins/nessus/41028
  - https://www.blackhillsinfosec.com/snmp-strings-attached/
  - https://github.com/trailofbits/onesixtyone
  - https://github.com/net-snmp/net-snmp

[Press Enter to continue]
```

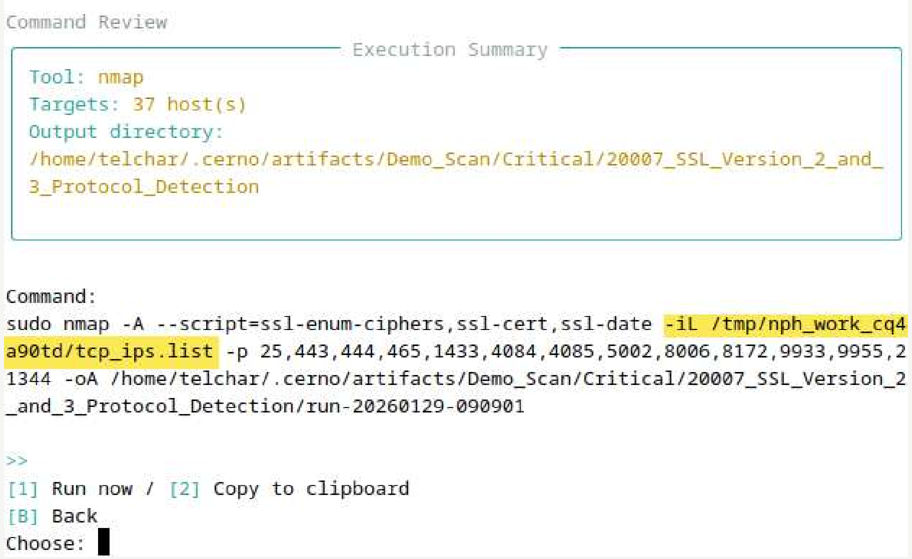
Tool Orchestration – nmap

One-Command Tool Launches

- NSE Profiles: Crypto, SSH, SMB, SNMP, IPMI
- Custom scripts addable alongside profiles
- UDP support for SNMP/IPMI (automatic)
- Pre-flight summary: targets, scripts, output directory
- Results saved: ~/.cerno/artifacts/<scan>/<severity>/<plugin>/



```
nmap Configuration

NSE Profile: Crypto
  Scripts: ssl-enum-ciphers, ssl-cert, ssl-date

Custom Scripts: None

UDP Scan: No

>>
[P] Select NSE Profile / [S] Add/Edit Custom Scripts
[U] Toggle UDP (OFF) / [Enter] Continue
[B] Back/Cancel
Choose ():
✓ Configuration saved: 3 script(s), UDP=No
```

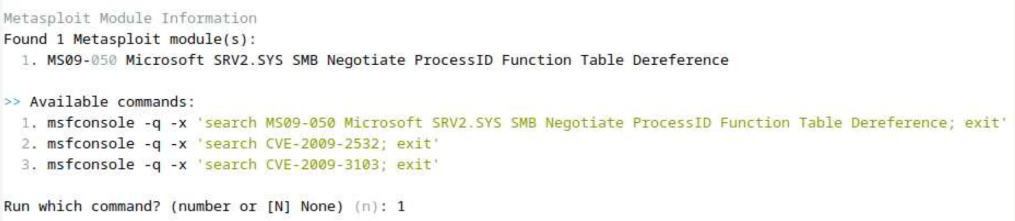


```
Command Review
                     Execution Summary
 Tool: nmap
 Targets: 37 host(s)
 Output directory:
 /home/telchar/.cerno/artifacts/Demo_Scan/Critical/20007_SSL_Version_2_and_
 3_Protocol_Detection


Command:
sudo nmap -A --script=ssl-enum-ciphers,ssl-cert,ssl-date -iL /tmp/nph_work_cq4
a90td/tcp_ips.list -p 25,443,444,465,1433,4084,4085,5002,8006,8172,9933,9955,2
1344 -oA /home/telchar/.cerno/artifacts/Demo_Scan/Critical/20007_SSL_Version_2
_and_3_Protocol_Detection/run-20260129-090901

>>
[1] Run now / [2] Copy to clipboard
[B] Back
Choose:
```

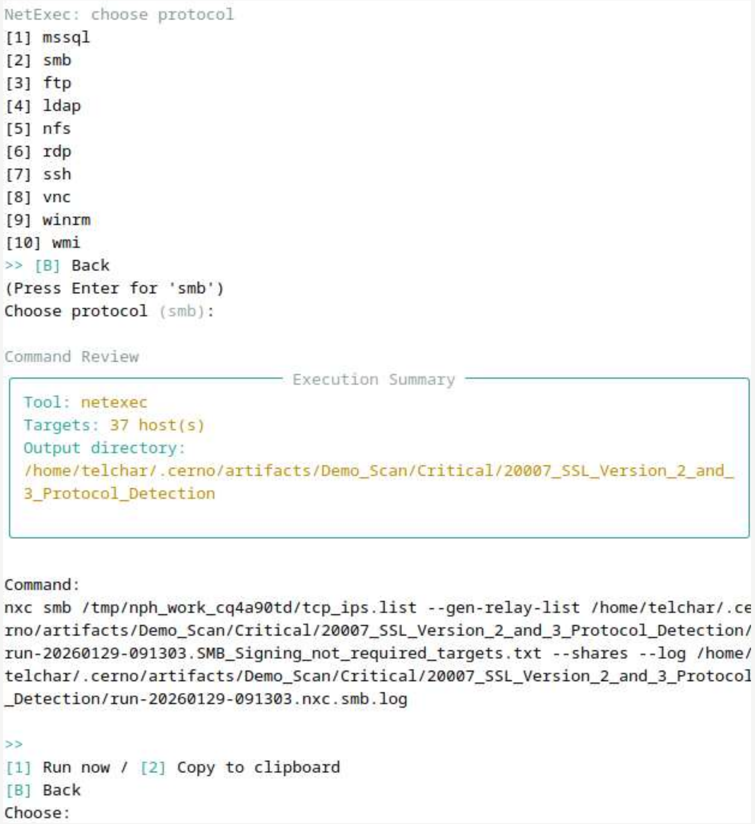
NetExec & Custom Tools

Beyond nmap – NetExec, Metasploit, Custom

- NetExec: Protocol selection (smb, ssh, rdp, etc.), auto-populates targets
- Metasploit: Module search by CVE/description, launch msfconsole
- Custom: Placeholder substitution for flexible templating
- Placeholders: {TCP_IPS}, {UDP_IPS}, {TCP_HOST_PORTS}, {PORTS}
- All executions logged with exit code, duration, sudo usage



```
Metasploit Module Information
Found 1 Metasploit module(s):
  1. MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference

>> Available commands:
  1. msfconsole -q -x 'search MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference; exit'
  2. msfconsole -q -x 'search CVE-2009-2532; exit'
  3. msfconsole -q -x 'search CVE-2009-3103; exit'

Run which command? (number or [N] None) (n): 1
```

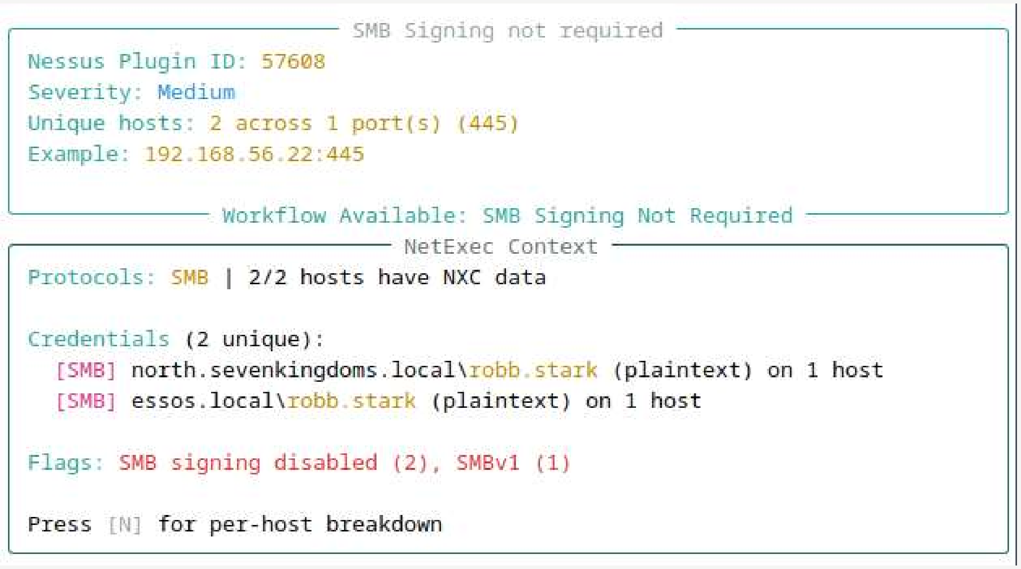


```
NetExec: choose protocol
[1] mssql
[2] smb
[3] ftp
[4] ldap
[5] nfs
[6] rdp
[7] ssh
[8] vnc
[9] winrm
[10] wmi
>> [B] Back
(Press Enter for 'smb')
Choose protocol (smb):

Command Review
┌──────────────────────── Execution Summary ─────────────────────────┐
│ Tool: netexec                                                       │
│ Targets: 37 host(s)                                                 │
│ Output directory:                                                   │
│ /home/telchar/.cerno/artifacts/Demo_Scan/Critical/20007_SSL_Version_2_and_
│ 3_Protocol_Detection                                                │
│                                                                     │
└─────────────────────────────────────────────────────────────────────┘

Command:
nxc smb /tmp/nph_work_cq4a90td/tcp_ips.list --gen-relay-list /home/telchar/.ce
rno/artifacts/Demo_Scan/Critical/20007_SSL_Version_2_and_3_Protocol_Detection/
run-20260129-091303.SMB_Signing_not_required_targets.txt --shares --log /home/
telchar/.cerno/artifacts/Demo_Scan/Critical/20007_SSL_Version_2_and_3_Protocol
_Detection/run-20260129-091303.nxc.smb.log

>>
[1] Run now / [2] Copy to clipboard
[B] Back
Choose:
```

NetExec DB [Beta]

Beyond nmap – NetExec, Metasploit, Custom

- Credential correlation - Shows which NetExec-discovered credentials have access to affected hosts
- Share access - Displays SMB share read/write permissions across hosts
- Security flags - Highlights SMB signing disabled, Zerologon, PetitPotam vulnerabilities
- Per-host breakdown - Press [N] in finding view for detailed per-host NetExec context

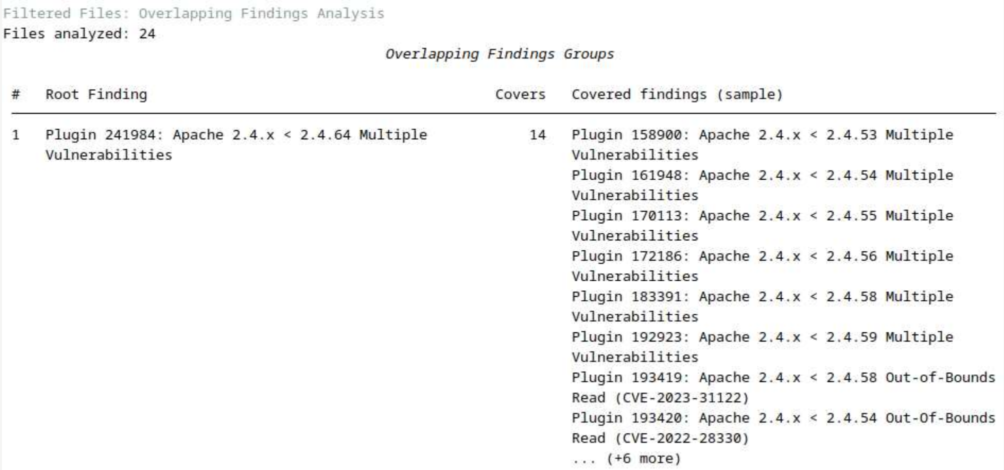


```
┌──────────────────────────── SMB Signing not required ────────────────────────────┐
│ Nessus Plugin ID: 57608                                                          │
│ Severity: Medium                                                                 │
│ Unique hosts: 2 across 1 port(s) (445)                                           │
│ Example: 192.168.56.22:445                                                       │
│                                                                                  │
└─────────────── Workflow Available: SMB Signing Not Required ─────────────────────┘
┌──────────────────────────────── NetExec Context ─────────────────────────────────┐
│ Protocols: SMB | 2/2 hosts have NXC data                                         │
│                                                                                  │
│ Credentials (2 unique):                                                          │
│   [SMB] north.sevenkingdoms.local\robb.stark (plaintext) on 1 host               │
│   [SMB] essos.local\robb.stark (plaintext) on 1 host                             │
│                                                                                  │
│ Flags: SMB signing disabled (2), SMBv1 (1)                                       │
│                                                                                  │
│ Press [N] for per-host breakdown                                                 │
└──────────────────────────────────────────────────────────────────────────────────┘
```

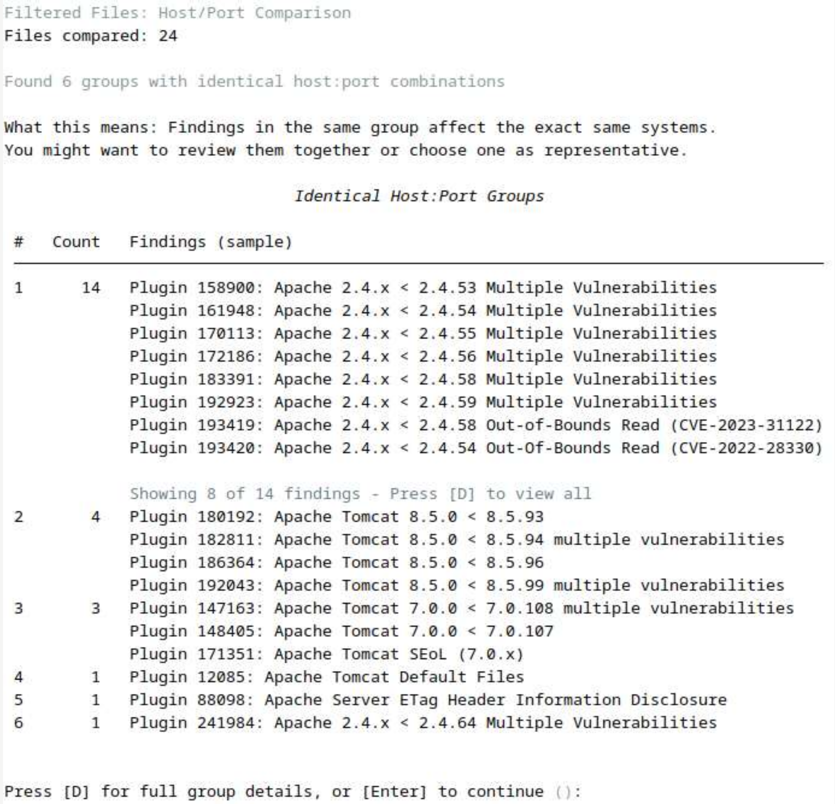
Host Comparison

Find Patterns Across Findings

- [H] Compare Hosts: Groups findings with identical host:port combinations
- [O] Overlapping: Identifies superset relationships
- Group filtering: Focus on related findings
- Use case: "5 findings affect same 3 hosts" - review together
- Reduces duplicate work across plugins



```
Filtered Files: Overlapping Findings Analysis
Files analyzed: 24
                              Overlapping Findings Groups

 #   Root Finding                                       Covers   Covered findings (sample)
 ─────────────────────────────────────────────────────────────────────────────────────────────
 1   Plugin 241984: Apache 2.4.x < 2.4.64 Multiple          14   Plugin 158900: Apache 2.4.x < 2.4.53 Multiple
     Vulnerabilities                                             Vulnerabilities
                                                                 Plugin 161948: Apache 2.4.x < 2.4.54 Multiple
                                                                 Vulnerabilities
                                                                 Plugin 170113: Apache 2.4.x < 2.4.55 Multiple
                                                                 Vulnerabilities
                                                                 Plugin 172186: Apache 2.4.x < 2.4.56 Multiple
                                                                 Vulnerabilities
                                                                 Plugin 183391: Apache 2.4.x < 2.4.58 Multiple
                                                                 Vulnerabilities
                                                                 Plugin 192923: Apache 2.4.x < 2.4.59 Multiple
                                                                 Vulnerabilities
                                                                 Plugin 193419: Apache 2.4.x < 2.4.58 Out-of-Bounds
                                                                 Read (CVE-2023-31122)
                                                                 Plugin 193420: Apache 2.4.x < 2.4.54 Out-Of-Bounds
                                                                 Read (CVE-2022-28330)
                                                                 ... (+6 more)
```

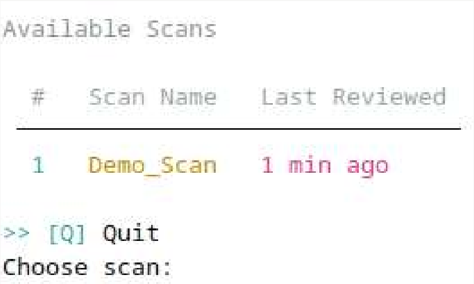


```
Filtered Files: Host/Port Comparison
Files compared: 24

Found 6 groups with identical host:port combinations

What this means: Findings in the same group affect the exact same systems.
You might want to review them together or choose one as representative.

                             Identical Host:Port Groups

 #   Count   Findings (sample)
 ────────────────────────────────────────────────────────────────────────────────────
 1      14   Plugin 158900: Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
             Plugin 161948: Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
             Plugin 170113: Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
             Plugin 172186: Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
             Plugin 183391: Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
             Plugin 192923: Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
             Plugin 193419: Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
             Plugin 193420: Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)

             Showing 8 of 14 findings - Press [D] to view all
 2       4   Plugin 180192: Apache Tomcat 8.5.0 < 8.5.93
             Plugin 182811: Apache Tomcat 8.5.0 < 8.5.94 multiple vulnerabilities
             Plugin 186364: Apache Tomcat 8.5.0 < 8.5.96
             Plugin 192043: Apache Tomcat 8.5.0 < 8.5.99 multiple vulnerabilities
 3       3   Plugin 147163: Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities
             Plugin 148405: Apache Tomcat 7.0.0 < 7.0.107
             Plugin 171351: Apache Tomcat SEoL (7.0.x)
 4       1   Plugin 12085: Apache Tomcat Default Files
 5       1   Plugin 88098: Apache Server ETag Header Information Disclosure
 6       1   Plugin 241984: Apache 2.4.x < 2.4.64 Multiple Vulnerabilities


Press [D] for full group details, or [Enter] to continue ():
```

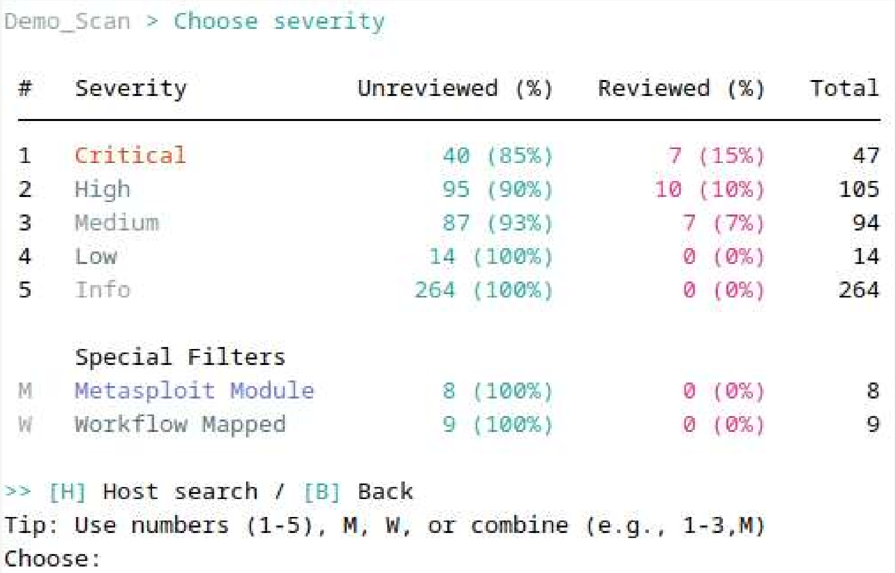
Session Persistence

Never Lose Your Progress

- Sessions auto-save to database (start time, scan context)
- Resume prompt on startup shows session details
- Review states: Unreviewed or Reviewed
- Undo capability: [U] restores completed to pending
- Session statistics: duration, per-severity breakdown



```
Available Scans

 #   Scan Name   Last Reviewed
 ─────────────────────────────
 1   Demo_Scan   1 min ago

>> [Q] Quit
Choose scan:
```

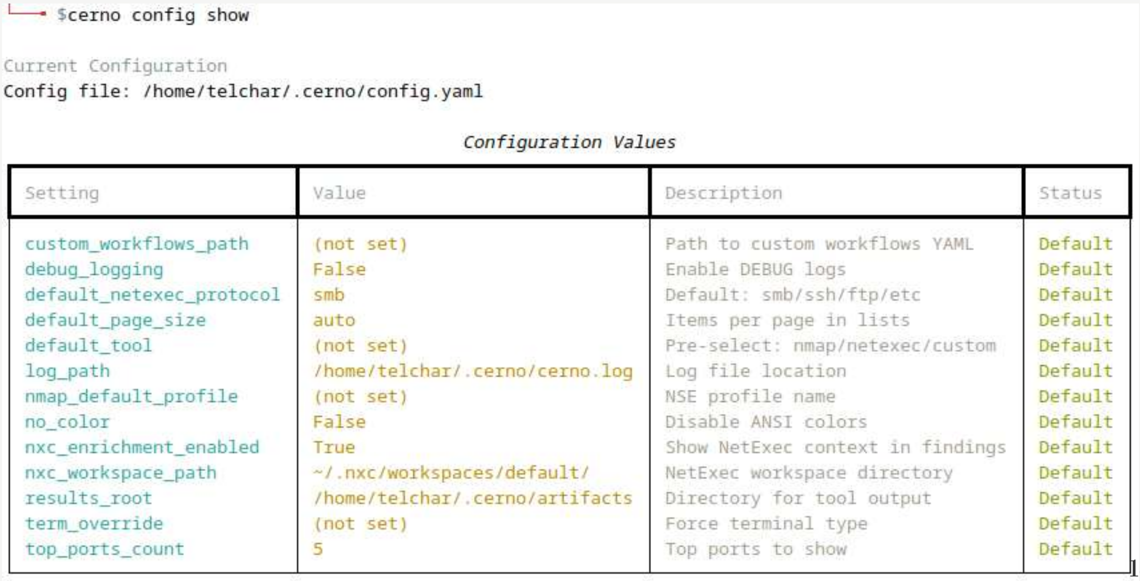


```
Demo_Scan > Choose severity

 #   Severity              Unreviewed (%)   Reviewed (%)   Total
 ───────────────────────────────────────────────────────────────
 1   Critical                   40 (85%)       7 (15%)       47
 2   High                       95 (90%)      10 (10%)      105
 3   Medium                     87 (93%)        7 (7%)       94
 4   Low                       14 (100%)        0 (0%)       14
 5   Info                     264 (100%)        0 (0%)      264

     Special Filters
 M   Metasploit Module          8 (100%)        0 (0%)        8
 W   Workflow Mapped            9 (100%)        0 (0%)        9

>> [H] Host search / [B] Back
Tip: Use numbers (1-5), M, W, or combine (e.g., 1-3,M)
Choose:
```

Configuration

Customize Your Workflow

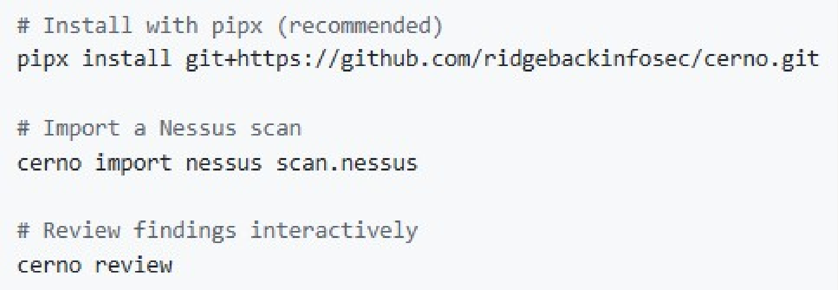
- Config file: ~/.cerno/config.yaml (auto-created)
- Commands: cerno config show/set/reset
- Custom workflows: YAML mapping plugin IDs to verification steps
- NetExec: Configure workspace path



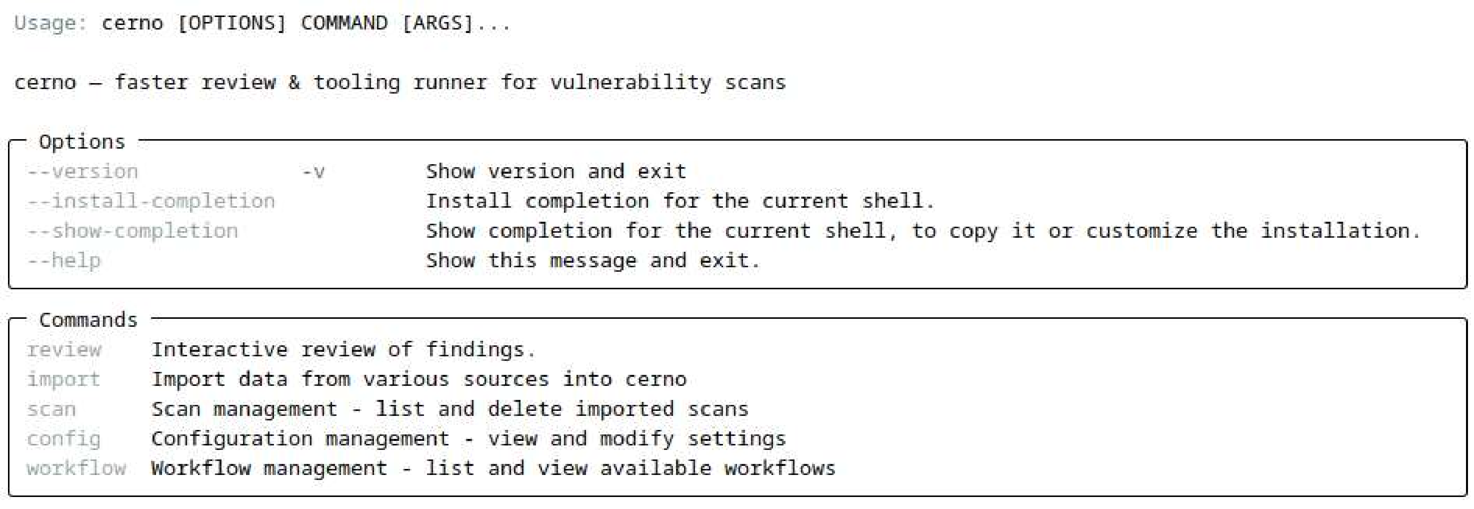
```
└──• $cerno config show

Current Configuration
Config file: /home/telchar/.cerno/config.yaml

                               Configuration Values
┌──────────────────────────┬──────────────────────────────────┬────────────────────────────────────┬─────────┐
│ Setting                  │ Value                            │ Description                        │ Status  │
├──────────────────────────┼──────────────────────────────────┼────────────────────────────────────┼─────────┤
│ custom_workflows_path    │ (not set)                        │ Path to custom workflows YAML      │ Default │
│ debug_logging            │ False                            │ Enable DEBUG logs                  │ Default │
│ default_netexec_protocol │ smb                              │ Default: smb/ssh/ftp/etc           │ Default │
│ default_page_size        │ auto                             │ Items per page in lists            │ Default │
│ default_tool             │ (not set)                        │ Pre-select: nmap/netexec/custom    │ Default │
│ log_path                 │ /home/telchar/.cerno/cerno.log   │ Log file location                  │ Default │
│ nmap_default_profile     │ (not set)                        │ NSE profile name                   │ Default │
│ no_color                 │ False                            │ Disable ANSI colors                │ Default │
│ nxc_enrichment_enabled   │ True                             │ Show NetExec context in findings   │ Default │
│ nxc_workspace_path       │ ~/.nxc/workspaces/default/       │ NetExec workspace directory        │ Default │
│ results_root             │ /home/telchar/.cerno/artifacts   │ Directory for tool output          │ Default │
│ term_override            │ (not set)                        │ Force terminal type                │ Default │
│ top_ports_count          │ 5                                │ Top ports to show                  │ Default │
└──────────────────────────┴──────────────────────────────────┴────────────────────────────────────┴─────────┘
```

DEMO

Getting Started



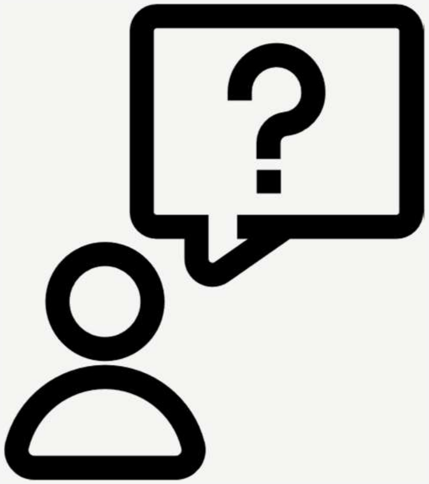
```
# Install with pipx (recommended)
pipx install git+https://github.com/ridgebackinfosec/cerno.git

# Import a Nessus scan
cerno import nessus scan.nessus

# Review findings interactively
cerno review
```



```
Usage: cerno [OPTIONS] COMMAND [ARGS]...

cerno — faster review & tooling runner for vulnerability scans

┌─ Options ──────────────────────────────────────────────────────────────────────────────────────────┐
│ --version               -v        Show version and exit                                              │
│ --install-completion              Install completion for the current shell.                          │
│ --show-completion                 Show completion for the current shell, to copy it or customize the installation. │
│ --help                            Show this message and exit.                                        │
└──────────────────────────────────────────────────────────────────────────────────────────────────────┘
┌─ Commands ───────────────────────────────────────────────────────────────────────────────────────────┐
│ review    Interactive review of findings.                                                            │
│ import    Import data from various sources into cerno                                                │
│ scan      Scan management - list and delete imported scans                                           │
│ config    Configuration management - view and modify settings                                        │
│ workflow  Workflow management - list and view available workflows                                    │
└──────────────────────────────────────────────────────────────────────────────────────────────────────┘
```

Questions?

- GitHub: github.com/ridgebackinfosec/cerno
- Issues: github.com/ridgebackinfosec/cerno/issues
- Docs: docs/ folder in repository



THANK YOU

FOR ATTENDING

Chris Traynor

blackhillsinfosec.com

antisyphontraining.com

ridgebackinfosec.com

FREE LABS!

https://tinyurl.com/freelabsfree