**Phase 3**

**Identify Vulnerabilities**

**Phase 3. Identify Vulnerabilities**

**Tool/Resources 1: Nessus**

**Description:** Nessus is an enterprise network vulnerability scanner that identifies technical vulnerabilities on the device. Vulnerabilities that an attacker could exploit. Nessus can use for host discovery on internal networks, scan internal network hosts for vulnerabilities and use to scan VPS cloud servers for vulnerabilities.

**Ways to use Nessus to discover vulnerabilities:**

* Host Discovery Scan: configurable for host enumeration and OS/Service detection
* Basic Network Scan: A quick vulnerability scan service
* Advanced Scan: Configurate a full vulnerability scan service
* Advanced Dynamic Scan: This scan can filter scan options such as CVE with severity score, CWE (common weakness enumeration) classes, and more.
* Malware Scan: Scan for malware internally on Windows and Unix systems.
* Active Directory Scan: Scan for any misconfiguration in the Active Directory.
* CISA Alerts Scan: Scan and detect any vulnerabilities from recent CISA alerts.
* Ransomware Scan: scan and detect any vulnerabilities used by ransomware.
* TerraScan: A static code analyzer for infrastructure used in automated pipelines to identify policy violations before insecure infrastructure is provisioned.

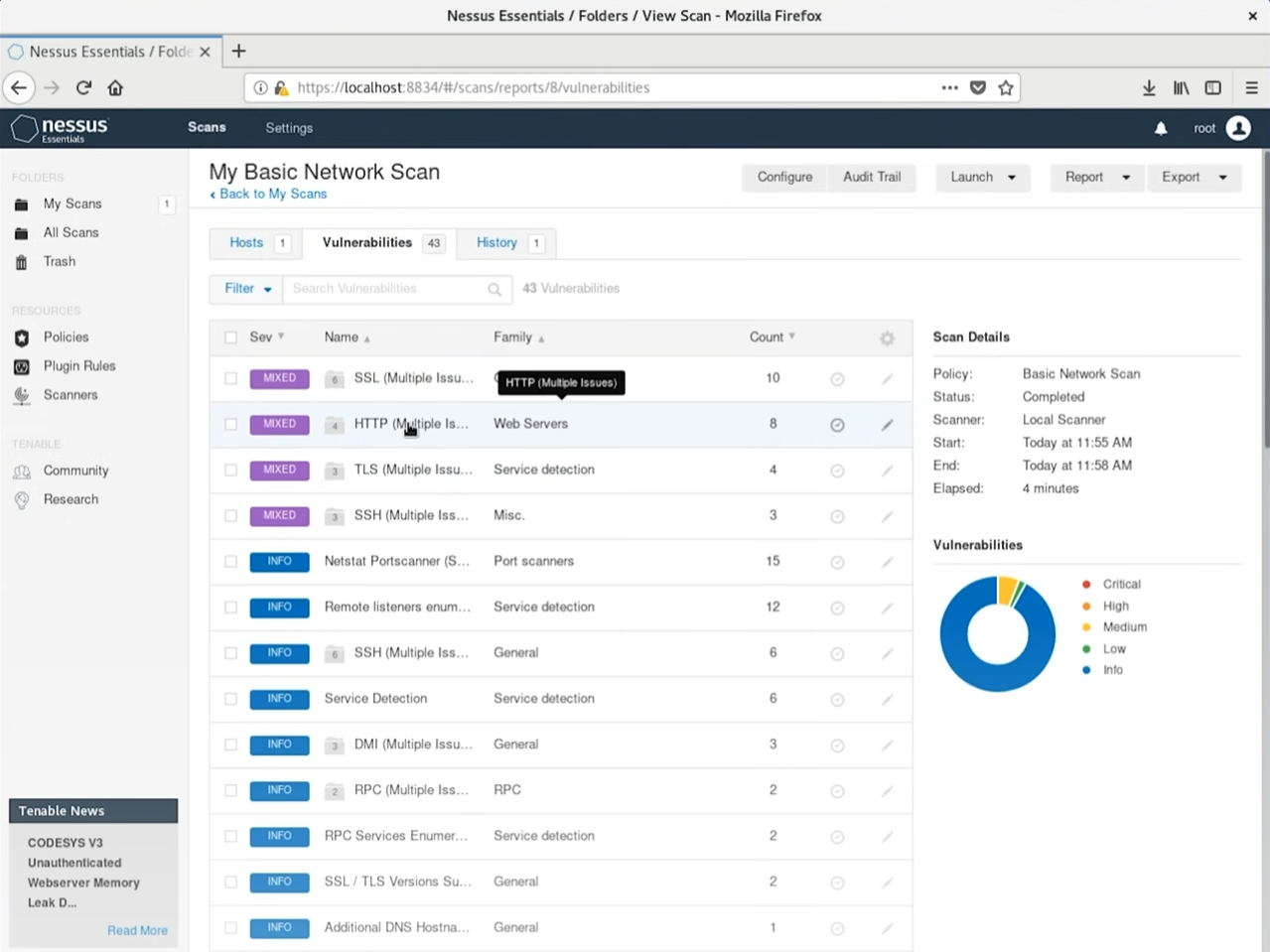
**Reason to use Nessus:**

* Very easy to scan for vulnerabilities, and the UI is user-friendly.
* Results from the network enumeration and port scanning are very good.
* Compatible with various operating systems such as Kali Linux, Fedora, FreeBSD, macOS, Red Hat/CentOS/Oracle, Ubuntu, and Windows.
* Very customizable to organizations’ preferences for the result’s severity.
* It provides encryption for the scan data to have more protection.
* Cover around 50,000 CVEs (Common Vulnerabilities and Exposure)
* Very good customer support.

**Potential drawbacks or limitations of Nessus:**

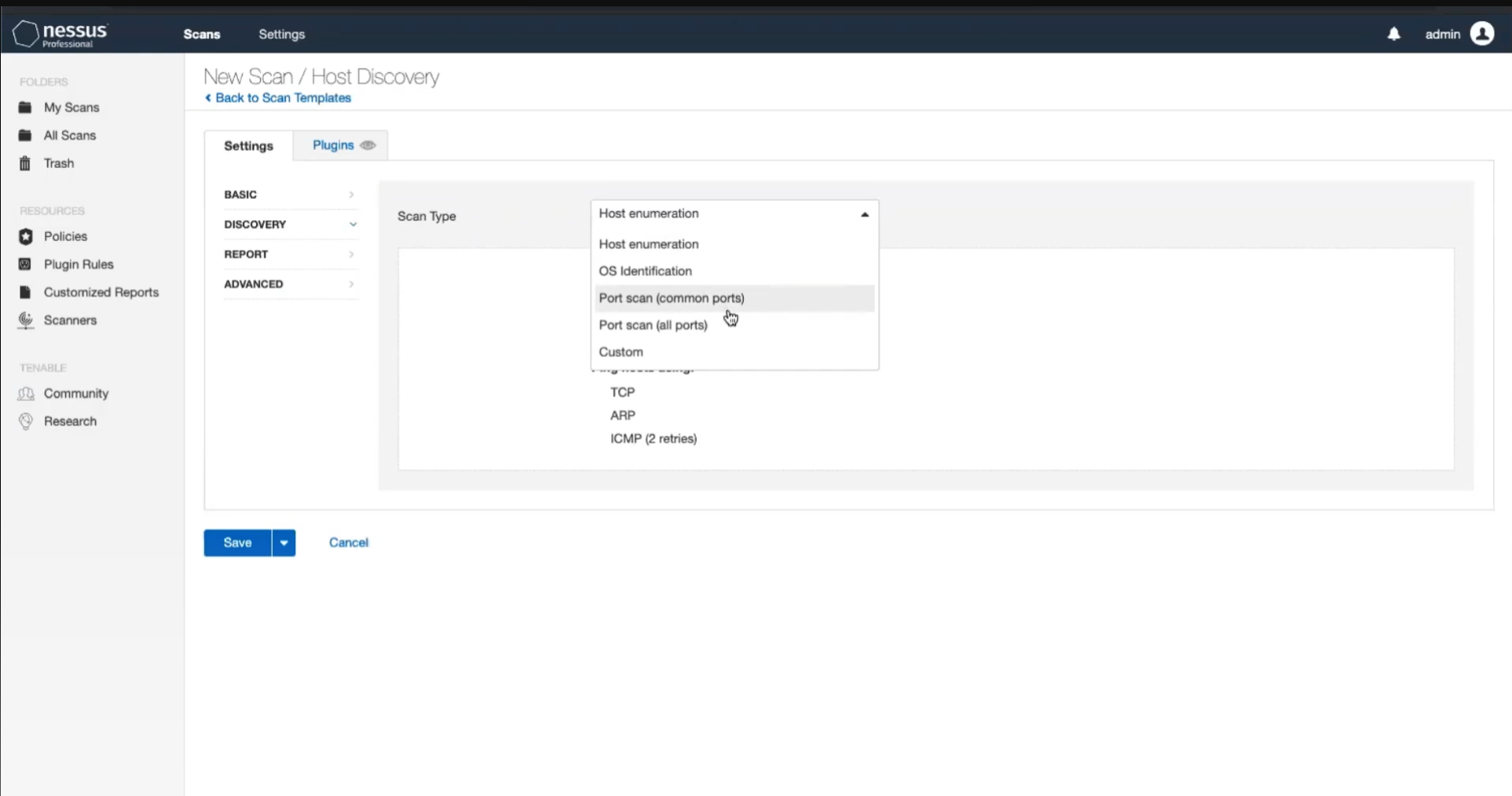
* Networks can overload sometimes.
* Appears hostile when used to scan.
* It is not free, which might not be viable for smaller companies.
* Nessus doesn’t provide as many advanced options and flexibility as Nmap when it runs port scanning.
  + Nmap can use the Kali Linux command line for:
    - Nmap -sS (IP): TCP syn scan, nmap -sT (IP): TCP connects scan, nmap -sU (IP): scan for UDP, etc.
    - Nessus can only run scan types such as Host enumeration, OS identification, Port Scan(common ports), Port scan(all ports), and custom for your port range.
* Once the encryption password for data at rest is lost, there is no way of recovering it.

**Nessus basic vulnerability Scan Screenshot:**

****

**Source: (Jon Good) <**[**https://www.youtube.com/watch?v=x87gbgQD4eg&t=569s**](https://www.youtube.com/watch?v=x87gbgQD4eg&t=569s)**>**

**Nessus Port Scan options Screenshot:**

****

**Source:(Tenable Product Education), <**[**https://www.youtube.com/watch?v=ntJbLPhX58s**](https://www.youtube.com/watch?v=ntJbLPhX58s)**>**

**Tool/Resources 2: OpenVAS**

**Description:** OpenVAS, or Open Vulnerability Assessment System, is a free software that provides vulnerability assessment services. It is a tool that scans the target system’s software version, configuration, and settings to see if there are any vulnerabilities.

**Ways to use OpenVAS to discover vulnerabilities:**

* Scan for vulnerabilities with multiple options.
  + Full Scan: Full vulnerability scan for network, server, and web applications.
  + Web Server Scan: A vulnerability scan focusing more on web servers and applications (ports 80 and 443).
  + WordPress Scan: A scan that tests for known WordPress vulnerabilities and web server issues.
  + Joomia Scan: A scan that tests for known Joomia vulnerabilities and web server issues.
* OpenVAS can also scan for host discovery and system discovery.

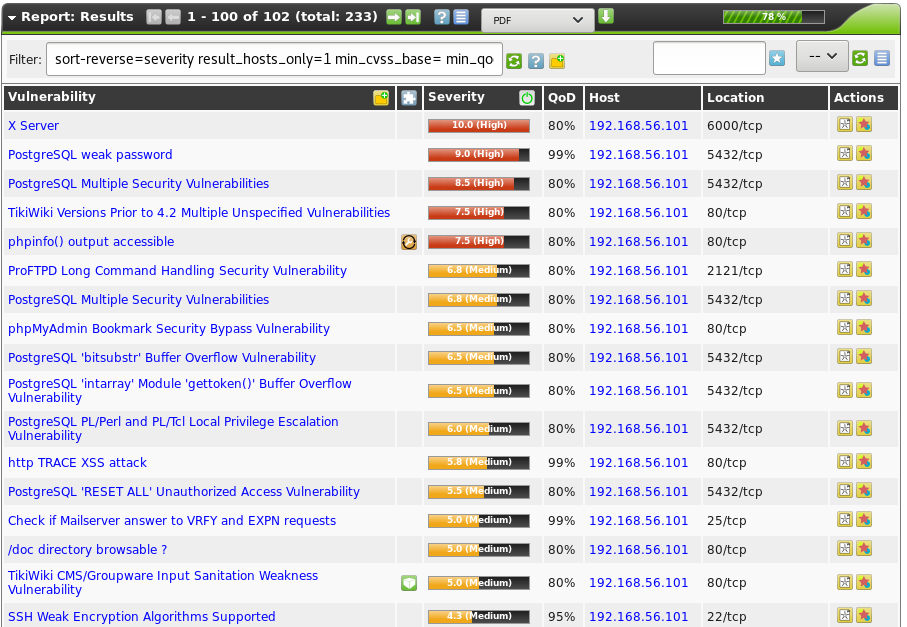
**Reason to use OpenVAS:**

* It is derived from Nessus before version 3. The vulnerability database continued to expand and update free of use.
* Free, since it is open-source, there are a lot of experts online that can help navigate through problems.
* It can provide a report listing all the vulnerabilities and sorting them by severity after scanning. Also shows the QoD (quality of Detection): shows a percentage of the detected vulnerabilities' reliability.
* The result summary from the report is very detailed and even shows the solution to that specific vulnerability.
* Super easy to export and import the report from/to OpenVAS with HTML, PDF, and CSV.

**Potential drawbacks or limitations of OpenVAS:**

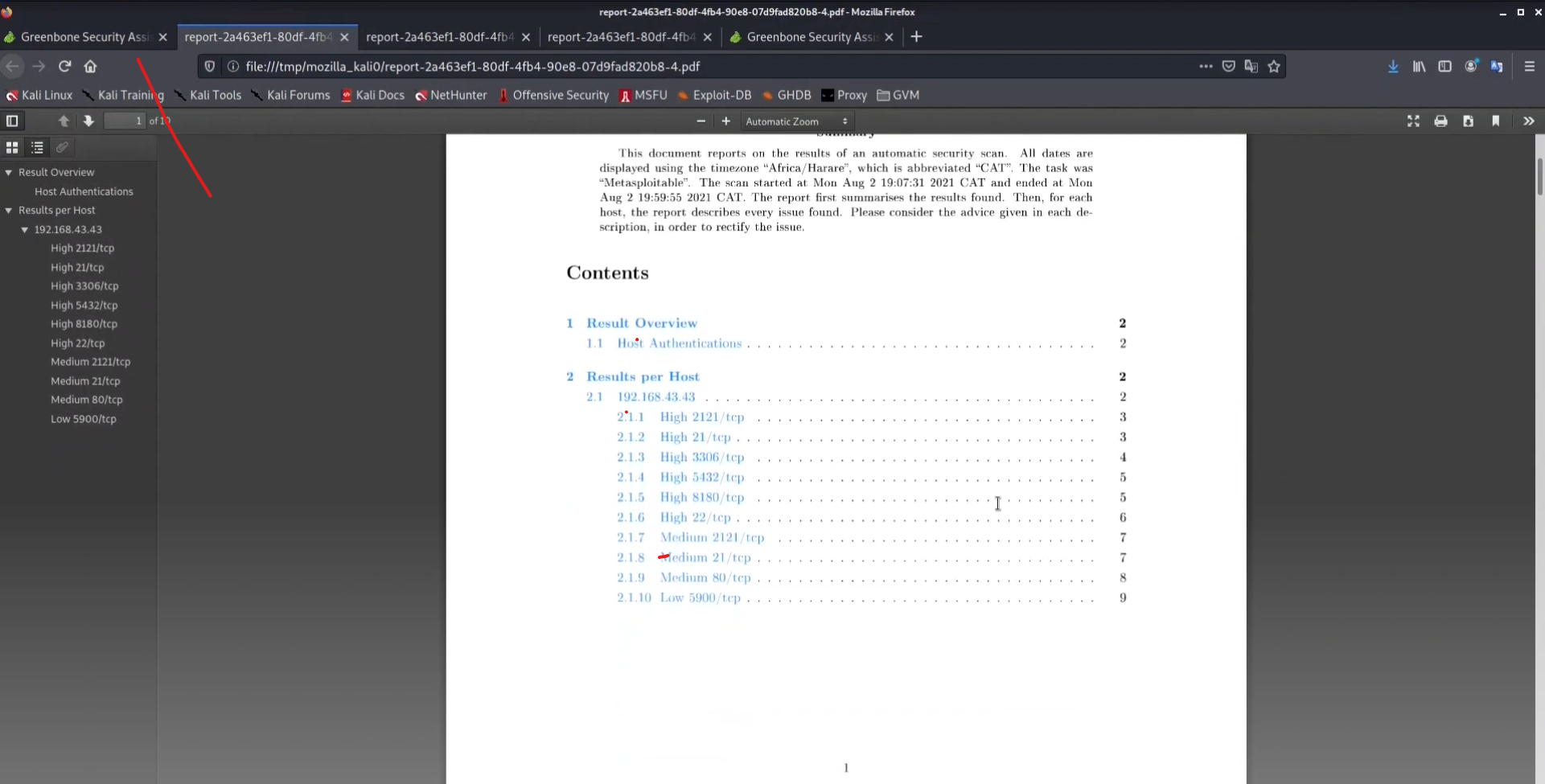
* It covers fewer vulnerabilities compared to Nessus. Might miss some flaws that Nessus would have detected. Only supports around 26,000 CVEs.
* Limitation on OS support only runs on Unix and Linux systems. Doesn’t support Windows or macOS users.

**Screenshot of OpenVAS scanned results:**

****

**Source: rapid7 <**[**https://www.rapid7.com/blog/post/2016/11/22/how-to-use-openvas-to-audit-the-security-of-your-network-22/**](https://www.rapid7.com/blog/post/2016/11/22/how-to-use-openvas-to-audit-the-security-of-your-network-22/)**>**

**Screenshot of OpenVAS scanned downloaded report PDF:**

****

**Source: OPENVAS <**[**https://www.youtube.com/watch?v=G9MXllD9Vt8**](https://www.youtube.com/watch?v=G9MXllD9Vt8)**>**

**Tool/Resources 3: Acunetix**

**Description:** Acunetix is a scalable, quick, and powerful vulnerability scanner with a high level of automation. The scanner audits the web application by checking vulnerabilities such as SQL injection, XSS, weak passwords, and other exploitable vulnerabilities.

**Ways to use Acunetix to discover vulnerabilities:**

* Scan a website using Acunetix.
  + Go to the applications' targets tab and click on add target.
  + Type in the website that the user wants to target.
  + Click on Scan and select the scan type: Full scan, high-risk vulnerabilities, Cross-site scripting vulnerabilities, SQL injection vulnerabilities, or weak password scan.
  + Click scan.

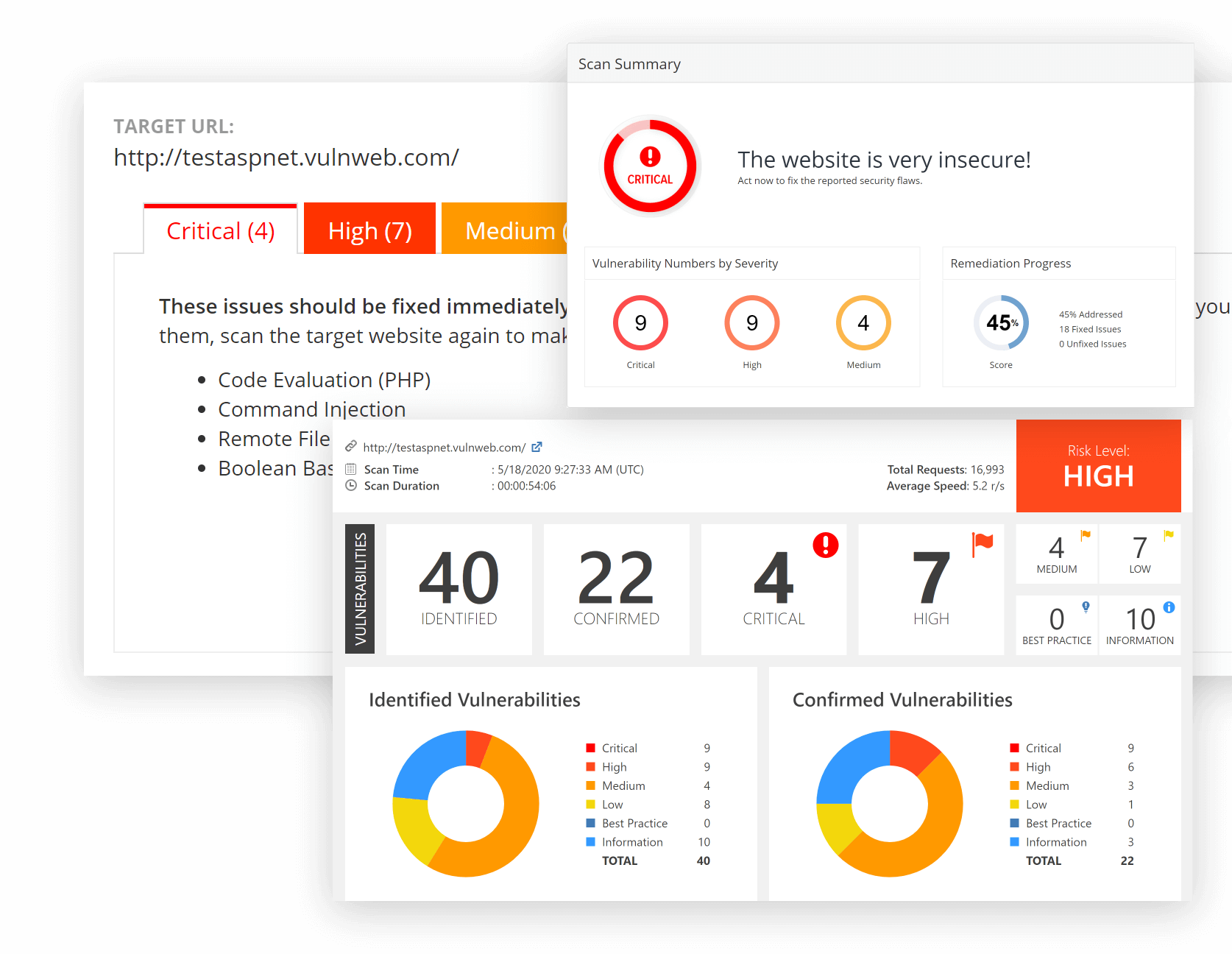
**Reason to use Acunetix:**

* Very user-friendly GUI and is available for Windows, Linux, and macOS.
* Ability to detect SQL injection vulnerabilities.
* Has very good report options. Users can locate and fix the vulnerability very quickly. It is because Acunetix provides details about the vulnerability, such as source-code line number, stack trace, and affected query.
* Low rate of getting a false positive when scanning a website because the tool understands the web application's behavior.

**Potential drawbacks or limitations of Acunetix:**

* Once configured the website, the user can not edit it. So the user has to be very careful when configuring the options. And when dealing with customer service, it can be a very slow response time.
* It only has a trial period of 14 days. The scanner is not available in the free version.
* The price of the tool can be expensive for smaller companies. The price can be from $4500 to $26600.

**Screenshot of Acunetix report of the impact:**

****

**Source: acunetix <**[**https://www.acunetix.com/product/acunetix360/**](https://www.acunetix.com/product/acunetix360/)**>**

**Tool/Resources 4: WireShark**

**Description:** Wireshark is a free and open-source powerful packet-capturing tool l that can deep dive into a user’s network to analyze the traffic and discover the problem. It is a tool that lets the user put the network traffic under a microscope and examine it to find the root cause of the problem.

**Ways to use WireShark to discover vulnerabilities:**

* Scan for network vulnerabilities
  + Capture the traffic packets for a few minutes, then stop the capturing.
  + Check if all the traffic belongs there.
  + If a protocol looks suspicious, you click on it and see whether it is an attack or an error.
  + Can also go to the statistics tab and look at the protocol hierarchy.
    - If a protocol has the word “data” under it, that means Wireshark doesn’t recognize the application, and the user can filter to that specific protocol.

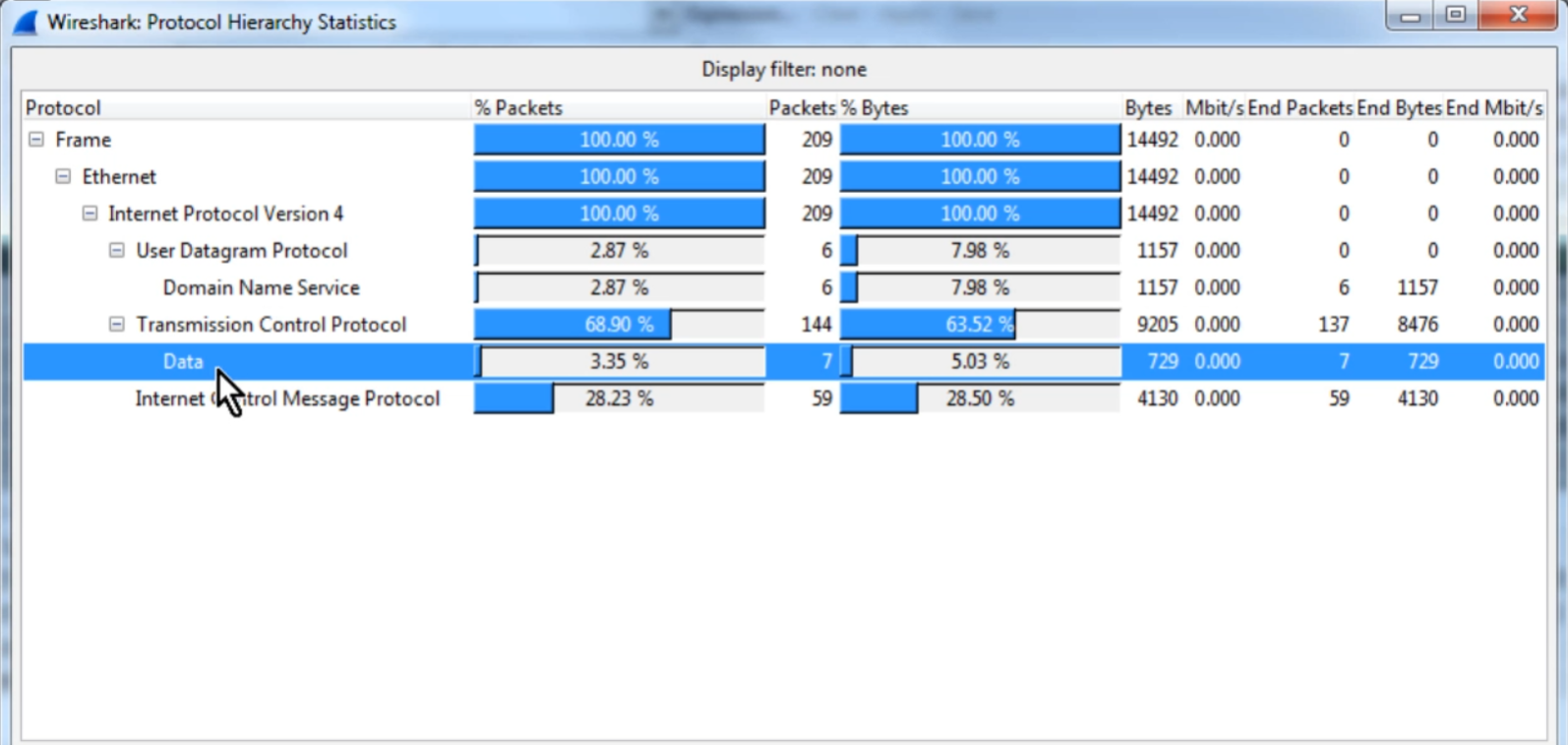
**Reason to use WireShark:**

* Free software and open-source.
* Available in various operating systems, Windows and UNIX.
* Easy to use, one click can see the details of the packet traffic.

**Potential drawbacks or limitations of WireShark:**

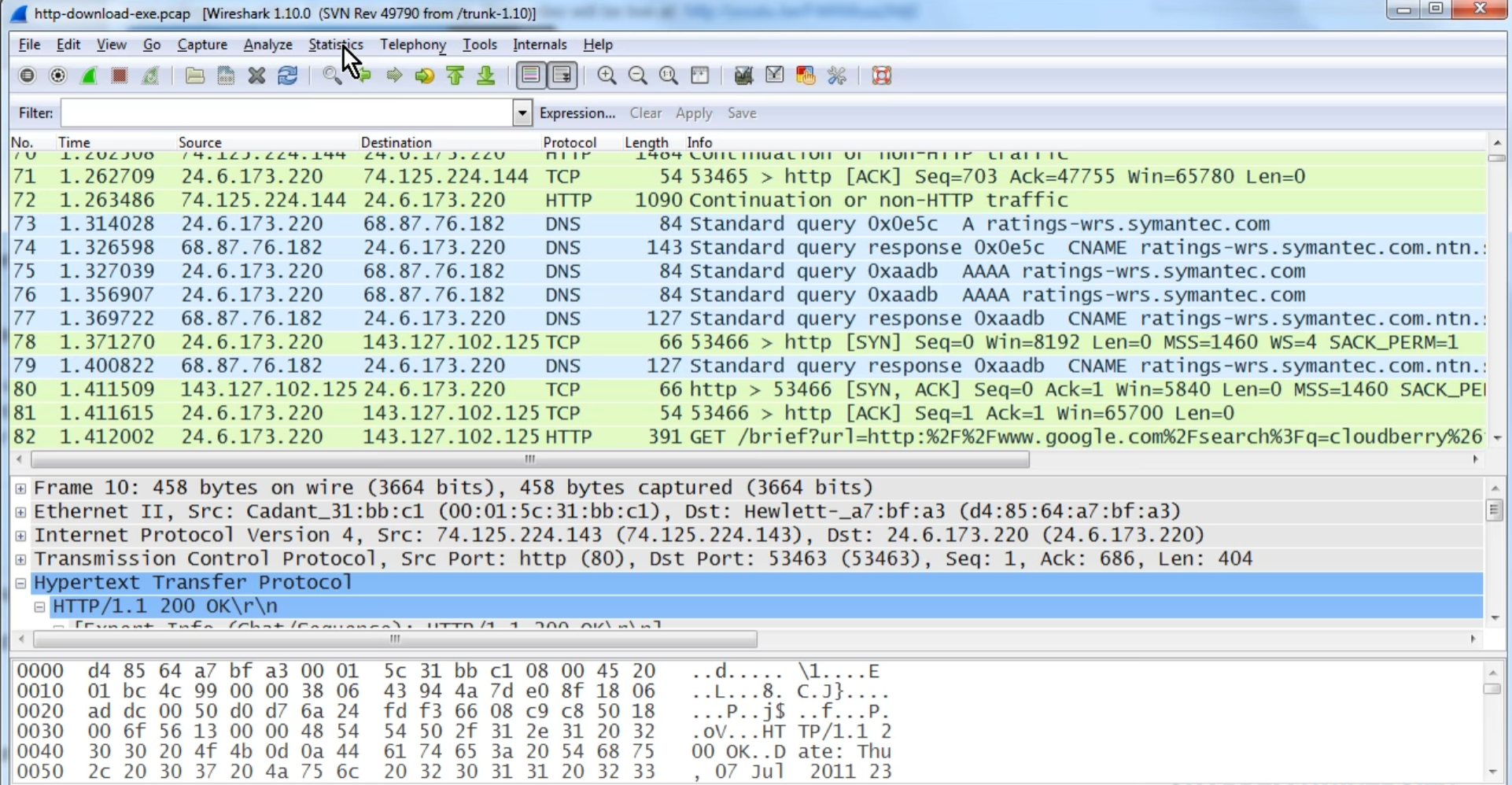
* Since it’s free, it is a very easy tool for hackers to sniff out network traffic for an attack if the hacker gets into the Wi-Fi.
* The protocols are very confusing for beginners to understand. Therefore, it’s not user-friendly.
* It can be a very long and tedious wait to capture and analyze all the packages.

**Screenshot of Wireshark Protocol Hierarchy Statistics Has Data:**

****

**Source: Laura Chappell <**[**https://www.youtube.com/watch?v=OwQmwbD1uIs&t=217s**](https://www.youtube.com/watch?v=OwQmwbD1uIs&t=217s)**>**

**Screenshot of Wireshark Capturing packets:**

****

**Source: Laura Chappell <**[**https://www.youtube.com/watch?v=OwQmwbD1uIs&t=217s**](https://www.youtube.com/watch?v=OwQmwbD1uIs&t=217s)**>**

**Tool/Resources 5: Burp Suite**

**Description:** Burp Suite is a Web penetration testing framework based on Java. It helps users identify the vulnerabilities and attack vectors that affect web-based applications. Burp Suite has three versions: free, professional, and enterprise-licensed editions. Burp Suite configures the browser to divert traffic with the help of the proxy. The proxy will act as a man-in-middle to capture and analyze every response from the web application.

**Ways to use Burp Suite to discover vulnerabilities:**

* Proxy tool: intercepts proxies that let users see and modify the contents of requests and responses during their transmission.
* Spider tool: used to map the target web application to observe its functionality and discover potential vulnerabilities.
* Scanner tool: used to scan the website application automatically for common vulnerabilities.
* Intruder tool: A fuzzer that runs a set of values through an input point. Used for Brute-force, dictionary attack, and testing the attacking rate limit on the web application.
* Repeater tool: let the user send requests repeatedly with modifications of their liking.
* Sequencer tool: An entropy checker that checks for the randomness of token generation by the webserver.
* Decoder tool: Used for decoding URLs, HTML, Base64, Hex, and more. It is also used for construction payload for vulnerability.

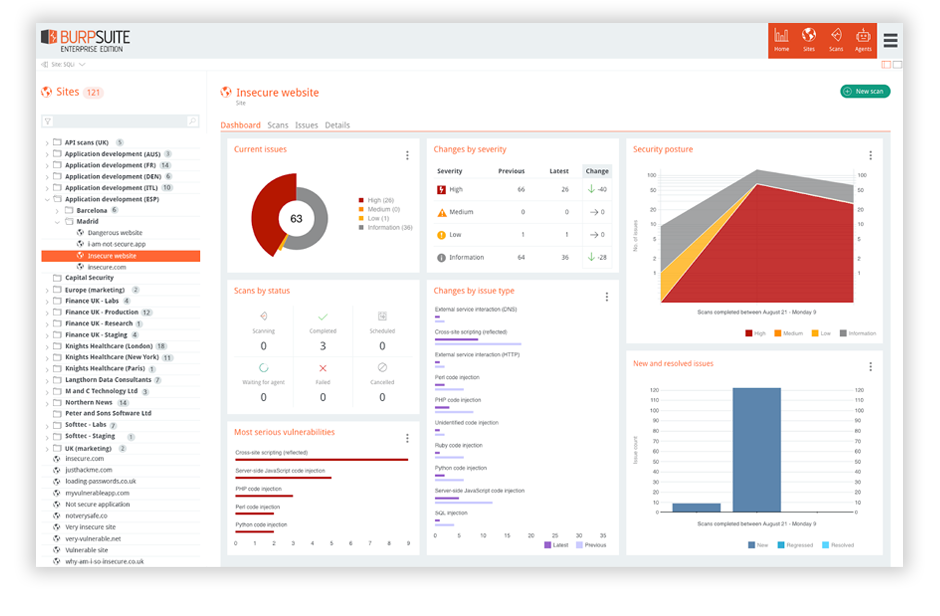
**Reason to use Burp Suite:**

* Burp Suite is available on the most popular operating systems: Windows, Linux, and Mac OS X.
* Burp Suite is also available on Android mobile.
* Burp Suite has various tools to use and find right on the GUI, and the community version is free.
* It is very easy to install and set up. And the report is very GUI is very user-friendly.
* Using Burp Suite, users can find vulnerabilities such as injection, broken authentication, XSS, CSRF, insurance direct object references, security misconfiguration, and sensitive data exposure.

**Potential drawbacks or limitations of Burp Suite:**

* False positive results can be high but can mark as false positives for future reports.
* It can crash when the user uses a high number of treads.
* The function (scanner tool) is not available in the free version.
* Price: The Enterprise edition can be expensive, 6000 per year. And the professional is 450 for one user per year.

**Screenshot of Burp Suite scanned results:**

****

**Source: portswigger <**[**https://portswigger.net/organizations/security-reporting**](https://portswigger.net/organizations/security-reporting)**>**