Capstone Project

Penetration Test Walkthrough By Esmond Burke

Artemis Gas, Inc

Global Enterprise

Table of Contents

Phase 1: Perform Reconnaissance

Reconnaissance Report:

Target Information

Company Name: Artemis Gas, Inc.
Website: https://artemisgas.us
Email Address: contactus@artemisgas.us
IP Address: 64.124.109.247 (Simulated AWS)
Online Ordering Portal: https://artemisgas.us/order
Create New Account: https://artemisgas.us/newuser
Oracle 12c: SAP runs on Oracle, with potential access to PARS and APOLLO.
ZScaler: Vulnerabilities, including CVE-2020-11633 (CVSS score: 10)
Cisco: Vulnerabilities, including CVE-2018-0350 (CVSS score: 9.0)
Fortinet: Vulnerabilities, including CVE-2012-0941 (CVSS score: 4.3)
Palo Alto: Vulnerabilities, including CVE-2022-0024 (CVSS score: 9.0)
Office 365 Cloud: Vulnerabilities, including CVE-2020-1483 (CVSS score: 9.3)
F5 (Big IP): Numerous vulnerabilities, including CVE-2015-8611 (CVSS score: 9.0)
Click here for Technical Details

Employee Profiles

1. Ricky Thomas (Marketing Sales Rep):
   - Online Presence: ig@HappyRicky, fb@familyRicky, Twt@OpinionRicky, LkIn@in/ricky-thomas
   - Email: ricky.thomas@artemisgas.us
   - Phone Number: 2189823175
   - Location: Not needed for an attack
   - Attack Vector: Social engineering attack to exploit Ricky's need to get new clients through a LinkedIn connection. Pretend to be a potential buyer from Buckeye International, Inc. Send a malicious email with a fake purchase order link.

2. Viola Jones (Database Engineer):
   - Slack: https://slack.getdbt.com
   - Reddit: Active user discussing database structures
   - Online Presence: lkln@in/viola-jones, ig@chattyjones
   - Email: viola.jones@artemisgas.us
   - Phone Number: 8503669802
   - Location: 1050 S Pace Blvd, Pensacola, FL 32502
   - Attack Vector: Social engineering and Credential stuffing to exploit Viola's remote connection to the database using ZScaler. Focus on the CVE-2020-14750 vulnerability for remote access.

3. Netish Patel (Account Manager):
  - Online Presence: ig@catlover_patel, twtr@iampatelcat, tktk@iampatelcat
  - Email: netish.patel@artemisgas.us
  - Phone Number: (713) 568-2505
  - Location: Houston, assumed based on the phone number and confirmed by US Phone Book
  - Attack Vector: Social engineering by sending a cat video email with a malware attachment. Netish may have access to the archive and patent records.

Click here for Employee Details

Reconnaissance Tools and Actions

1. Kali Linux Virtual Machine:
  - Purpose: Perform reconnaissance
  - Usage: Set up and run various reconnaissance tools and techniques.

2. Express VPN:
  - Purpose: Obscure location and change location as needed
  - Usage: Connect to VPN to hide identity and location during reconnaissance activities.

3. john.doe@protonmail.com (Secure Email Server on Dark Web):
  - Purpose: Create social media accounts for the alias "John Doe"
  - Usage: Use this secure email server on the dark web to create social media accounts on LinkedIn, Instagram, Facebook, and WhatsApp.

4. SpoofCard Account:
  - Purpose: Emulate an employee from Artemis Gas, Inc. (if needed).
  - Usage: Use a SpoofCard account to spoof a caller ID as needed for impersonation purposes.

5. OSINT Framework:
  - Purpose: Gather information from various sources
  - Usage: Utilize the OSINT Framework's reconnaissance tools to gather information about the target.

6. Spiderfoot:
  - Purpose: Query public information sources and process intelligence data
  - Usage: Start the Spiderfoot server using the provided command and perform a scan on https://artemisgas.us to collect information from domain names, email addresses, names, IP addresses, and DNS servers.

7. Pastebin:
  - Purpose: Access and search for plain text information like usernames and passwords
  - Usage: Visit https://pastebin.com/archive to find many plain text documents. Utilize the search engine on the site for specific queries.

Click here for Tool Details

Recommendations

1. Exploit vulnerabilities in the target's Oracle 12c, ZScaler, Cisco, Fortinet, Palo Alto, Office 365 Cloud, and F5 (Big IP) systems to gain unauthorized access or perform denial-of-service attacks.

2. Utilize social engineering tactics to target employees Ricky Thomas, Viola Jones, and Netish Patel. Craft tailored emails with malicious links or attachments to exploit their roles and access privileges.

3. Maintain anonymity and location obfuscation using the Kali Linux Virtual Machine and Express VPN to avoid detection during reconnaissance activities.

4. Continuously monitor and update the OSINT Framework and reconnaissance tools for the latest information sources and techniques to gather valuable data.

5. The main objective is to access confidential information on the PARS and APOLLO systems. These systems contain intellectual property (patents) that can be sold on the dark web and be locked up in a ransomware attack.

Phase 2: Identify Targets and Run Scans

Nmap

Purpose: Nmap is a powerful network scanning tool used to discover live hosts and services on a network. It provides valuable information about open ports and running services. In this project, we will utilize Nmap to scan the IP addresses provided by Artemis Gas to identify open ports.

Usage: Nmap can be run both from the command line and through a GUI called Zenmap. We will use the command line interface and execute the following command for each target IP address: nmap -p 1-65535 -T4 -A -v <target_ip_address>. This command initiates a scan of all ports, using aggressive timing and service detection.

Challenges:

1. By default, Nmap scans only the well-known ports (1000 ports). To scan all 65534 ports, we need to add the -p flag with the port range.
2. Nmap scans can be detected and blocked by blue teams or automated Security Information and Event Management (SIEM) systems.

Benefits:

1. Nmap is adaptable to any operating system.
2. It is a free and open-source tool that is supported by a large community.
3. Zenmap, the GUI interface for Nmap, provides network topology mapping, which is useful when existing maps are unavailable or of poor quality.

Wireshark

Purpose: Wireshark is a free, open-source vulnerability scanning tool that captures and analyzes network traffic. It is commonly used for monitoring and identifying incidents related to improper file transfers. In this project, we will utilize Wireshark to monitor network traffic and identify any incorrect file transfers made by users.

Usage: Wireshark has a graphical user interface (GUI) and allows the application of filters to analyze specific protocols used for file transfers. We will focus on monitoring FTP and HTTP traffic, as these protocols are commonly used for insecure file transfers. A sample filter can be: tcp.port == 21 || tcp.port == 20 || udp.port == 21 || udp.port == 20 for FTP, and a similar filter for port 80 (HTTP).

Challenges:

1. Wireshark captures a large amount of traffic, requiring it to be running for extended periods to capture improper file transfers.
2. Analyzing captured packets, especially encrypted traffic, can be challenging and require specialized knowledge.

Benefits:

1. Wireshark is non-intrusive and does not impact network traffic while running.
2. It provides real-time capture, allowing passive monitoring of network activity on suspicious ports.
3. Wireshark can be configured to run on multiple ports simultaneously.

Gobuster

Purpose: Gobuster is a versatile tool used for brute-forcing various aspects of web applications, including URIs, DNS subdomains, virtual host names, and open storage buckets. In this project, Gobuster will be used to crack AWS credentials and identify any data that employees have failed to properly store in the cloud.

Usage: Gobuster can be executed from the command line with specific parameters. For Amazon S3, a sample command can be: gobuster s3 -k <target_ip_address> --useragent "jack.doe". This command instructs Gobuster to attack the target, skipping TLS certificate verification, and setting the user-agent as "jack.doe".

Challenges:

1. Gobuster is an aggressive scan that can be easily noticed and blocked.
2. It requires manual execution and does not offer automation capabilities.
3. There may be a learning curve associated with using Gobuster effectively.

Benefits:

1. Gobuster is fast at brute-forcing and can discover hidden URLs, files, and directories within websites.
2. It provides a command-line interface, making it suitable for automation and integration into larger workflows.

InfraSOS

Purpose: InfraSOS is a leading Active Directory (AD) reporting tool that provides detailed reports on AD, Office 365, and Azure AD objects and attributes. It helps ensure that administrators adhere to security policies and identify areas where administrators deviate from established practices.

Usage: InfraSOS is a web-based tool with a user-friendly GUI. Users can interact with the interface and generate over 200+ AD reports, which can be exported in various formats. Additionally, it offers an API for integration into SIEM systems to correlate network traffic with AD behavior.

Challenges:

1. Some advanced features may require an upgrade to the tool.
2. InfraSOS is currently available only in English.

Benefits:

1. Being web-based, InfraSOS eliminates the need for software installation and enables remote monitoring.
2. It offers features such as Office 365 HealthCheck and the ability to identify vulnerable AD accounts.
3. Encrypted communication ensures security when using InfraSOS.

Metasploit

Purpose: Metasploit is a comprehensive penetration testing tool used for verifying vulnerabilities, managing security assessments, and enhancing security awareness. In this project, we will use Metasploit to validate vulnerabilities discovered during the reconnaissance phase and check for missed patches and misconfigurations.

Usage: Metasploit provides an extensive range of tools and commands to exploit various addresses. For example, we can use the SMB Login Check module to test weak user logins. The following commands demonstrate its usage: (a) msf> use auxiliary/scanner/smb/smb_login, (b) msf auxiliary(smb_login) > set RHOSTS <target_ip_address>, (c) msf auxiliary(smb_login) > set SMBUser victim, (d) msf auxiliary(smb_login) > set SMBPass s3cr3t, (e) msf auxiliary(smb_login) > set THREADS 50, (f) msf auxiliary(smb_login) > run. Here is a breakdown of the above commands:

a. Tells Metasploit to use smb.
b. Sets up the target host.
c. Sets the username to authenticate.
d. Sets the password for the specified user.
e. Sets the number of concurrent threads.
f. Run password login attempts.

Challenges:

1. Metasploit is an advanced tool that requires familiarity and may present a learning curve.
2. It is an intrusive tool and can generate noise, potentially alerting security systems.
3. Improper use of Metasploit can lead to unethical behavior by penetration testers.

Benefits:

1. Metasploit is a popular and well-supported tool used by many security professionals.
2. It is freely available, making it accessible to a wide range of users.
3. The interactive interface simplifies the management and monitoring of multiple sessions and payloads.

Burp Suite

Purpose: Burp Suite is a comprehensive web application penetration testing tool used to test web application security. It offers a range of features and will be utilized to test all applications used by Artemis Gas. Passive testing will be performed to avoid triggering alerts.

Usage: Burp Suite provides a GUI that allows users to enter the web application address and initiate scans. The scans can be customized as needed to suit the project's requirements. Burp Suite is ideal for checking Artemis Gas's web application configuration.

Challenges:

1. The community edition of Burp Suite has limitations in terms of available features.
2. It is primarily focused on web application testing and may not cover other aspects of network security.

Benefits:

1. Burp Suite offers a user-friendly GUI that facilitates the testing process.
2. The professional edition of Burp Suite provides advanced automated tools for more comprehensive testing.
3. It allows both passive and active scanning techniques to identify vulnerabilities.

Zap

Purpose: ZAP (Zed Attack Proxy) is a comprehensive security testing tool actively maintained by OWASP (Open Web Application Security Project). It simulates malicious attackers, scans and analyzes security issues, and is used to test the SAP enterprise in this project. ZAP helps detect users who are not adhering to the company's app-building policies.

Usage: ZAP has a GUI interface that allows users to enter the website URL (e.g., https://artemisgas.us/) and initiate the scan.

Challenges:

1. ZAP is an active testing tool, and its attacks may trigger detection by SIEM systems. Customizing the tool to avoid detection becomes necessary.
2. ZAP has been known to generate false positives and false negatives.
3. It can consume significant CPU memory and may require performance adjustments to avoid system crashes.

Benefits:

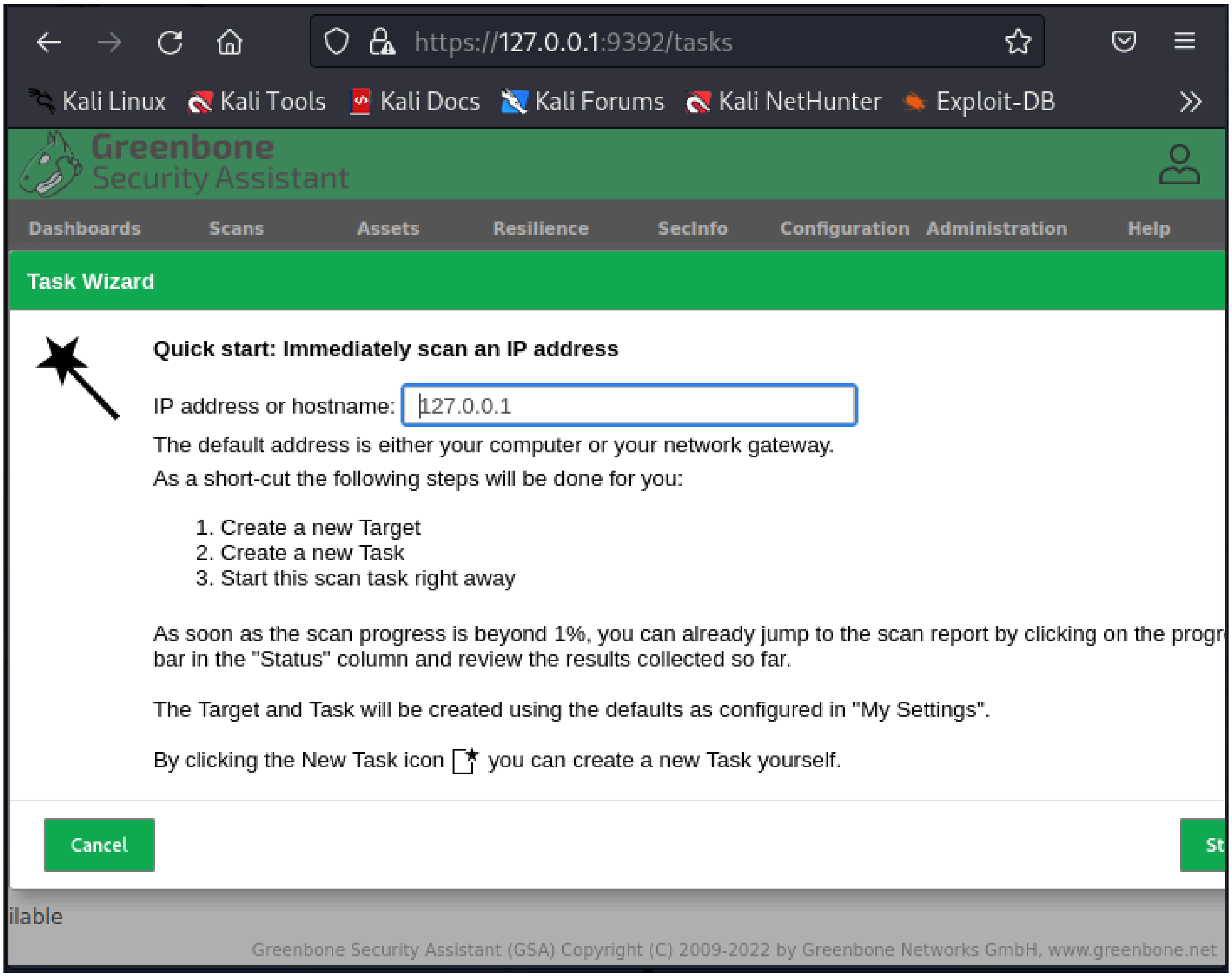
1. ZAP provides a wide range of penetration testing features accessible with a single click.
2. Its main features include the ability to intercept browser requests and responses, create and customize scans, and use custom payloads with a fuzzer.
3. ZAP offers access control capabilities to restrict resources on a server, enhancing security.

Click here for more details…

Phase 3. Identify Vulnerabilities

OpenVAS

Purpose: The OpenVAS scanner is a comprehensive vulnerability assessment system that can detect security issues in all manner of servers and network devices.



Quick start: Immediately scan an IP address

IP address or hostname: 127.0.0.1

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progr bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net

Challenges:

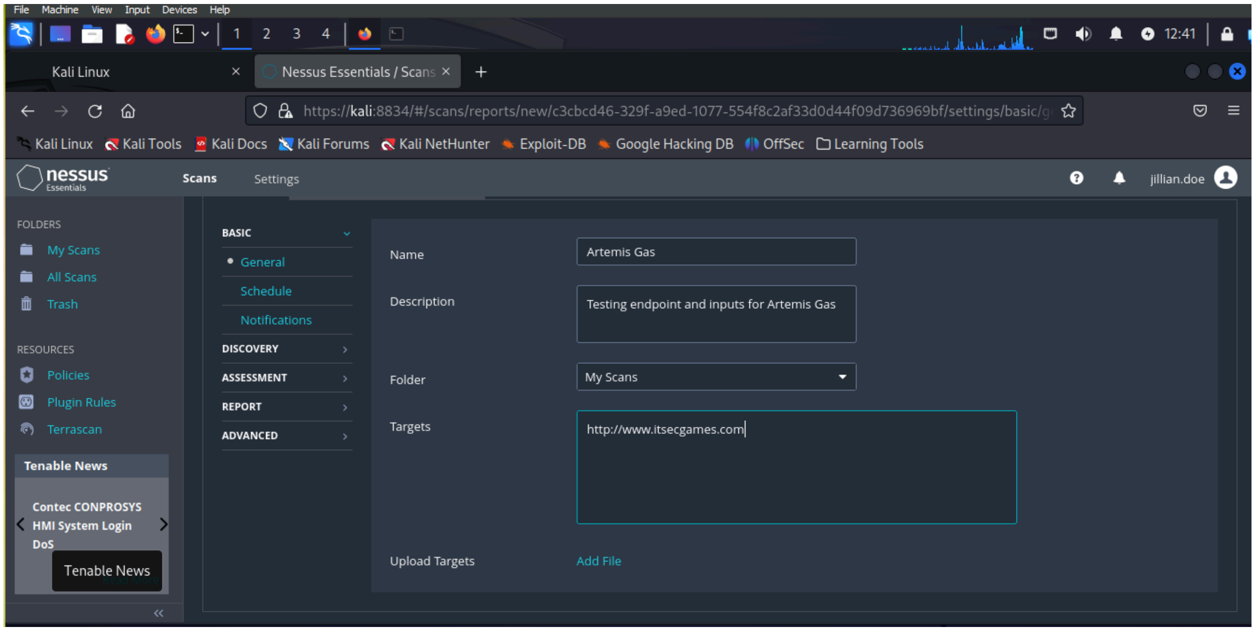
1. Installing and configuring the OpenVAS community edition is difficult
2. Utilizing the scanner for specific configurations proved difficult

Benefits:

1. Comprehensive coverage for a free solution
2. A dedicated community of developers
3. Open-source and free of charge
4. Support for multiple OS'"

Tenable Nessus

Purpose: Nessus is a remote security scanning tool that scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to access any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.


File Machine View Input Devices Help
1 2 3 4
12:41
Kali Linux
Nessus Essentials / Scans
https://kali:8834/#/scans/reports/new/c3cbcd46-329f-a9ed-1077-554f8c2af33d0d44f09d736969bf/settings/basic/g
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Learning Tools
nessus Essentials
Scans
Settings
jillian.doe
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Contec CONPROSYS HMI System Login DoS
Tenable News
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED

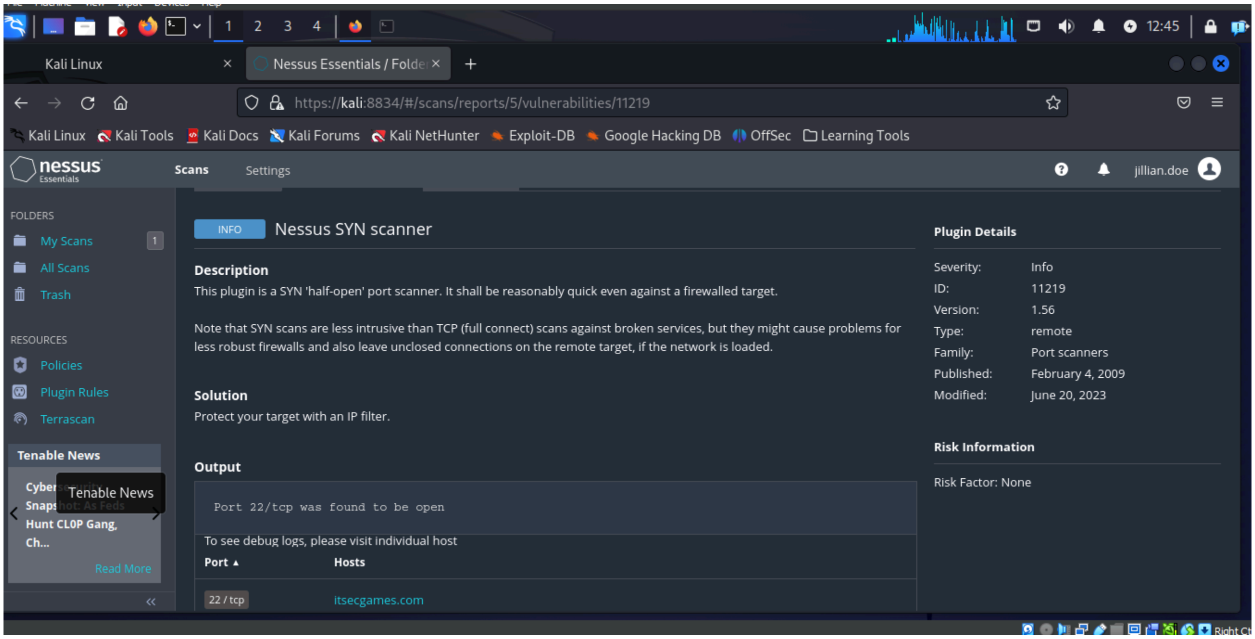
Name: Artemis Gas

Description: Testing endpoint and inputs for Artemis Gas

Folder: My Scans

Targets: http://www.itsecgames.com

Upload Targets: Add File


1 2 3 4
12:45
Kali Linux
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/5/vulnerabilities/11219
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Learning Tools
nessus Essentials
Scans
Settings
jillian.doe
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cyber... Snaps... Hunt CL0P Gang, Ch...
Tenable News
Read More

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 22/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▲	Hosts
22 / tcp	itsecgames.com

Plugin Details

Severity:	Info
ID:	11219
Version:	1.56
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	June 20, 2023

Risk Information

Risk Factor: None

Challenges:

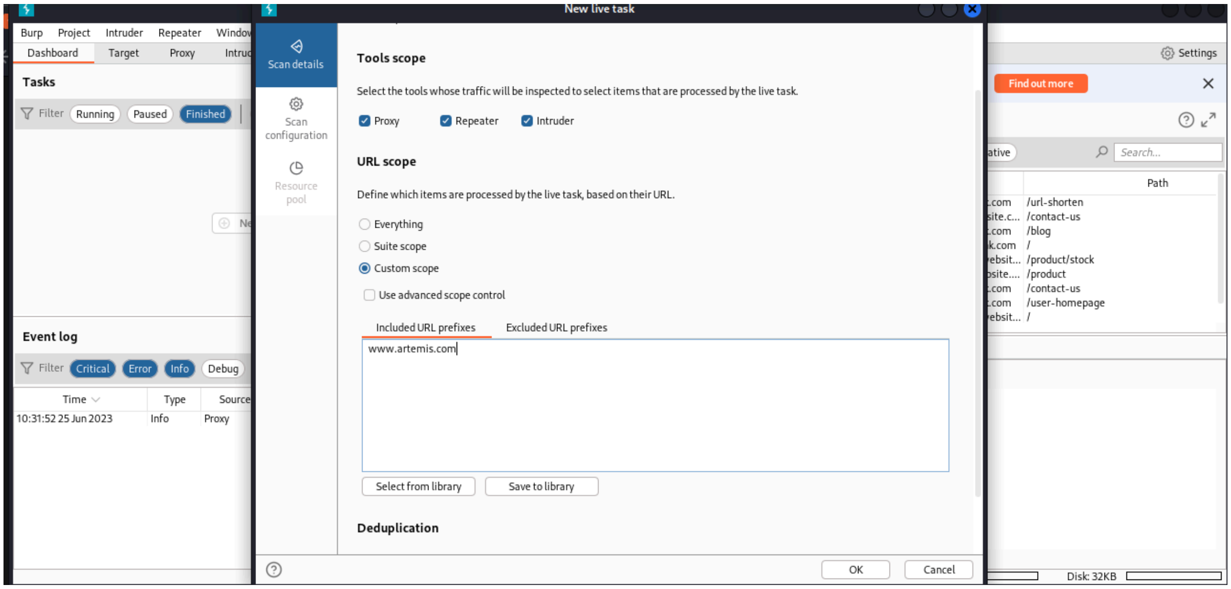
1. Sensitive networks can become congested and give false positives, and bad results, and have an impact on production networks.
2. Using Nessus to scan legacy hardware can cause problems. Sensitive devices include remote terminal units (RTUs) and programmable logic controllers (PLCs), which could cause malfunctions with industrial equipment.
3. The open-source version took a very long time (over 40 minutes) to compile.

Benefits:

1. Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.
2. Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. It also provides a plug-in interface, and many free plugins are available from the Nessus plug-in site.
3. Up-to-date information about new vulnerabilities and attacks.
4. It is open-source.

Burp Suite

Purpose: Burp Suite is a great tool for penetration testing of web applications. It is feature-rich, and we will use it to test all applications that Artemis uses. We can do a passive test on an application since we do not want false-positive alerts. We will choose a new live task and use the default configuration, and conduct a passive scan. Or we can create our own customized scan that allows us to select the tools' scope, URL scope, and task type.



New live task

Tools scope

Select the tools whose traffic will be inspected to select items that are processed by the live task.

☑ Proxy ☑ Repeater ☑ Intruder

URL scope

Define which items are processed by the live task, based on their URL.

○ Everything
○ Suite scope
● Custom scope

□ Use advanced scope control

Included URL prefixes | Excluded URL prefixes

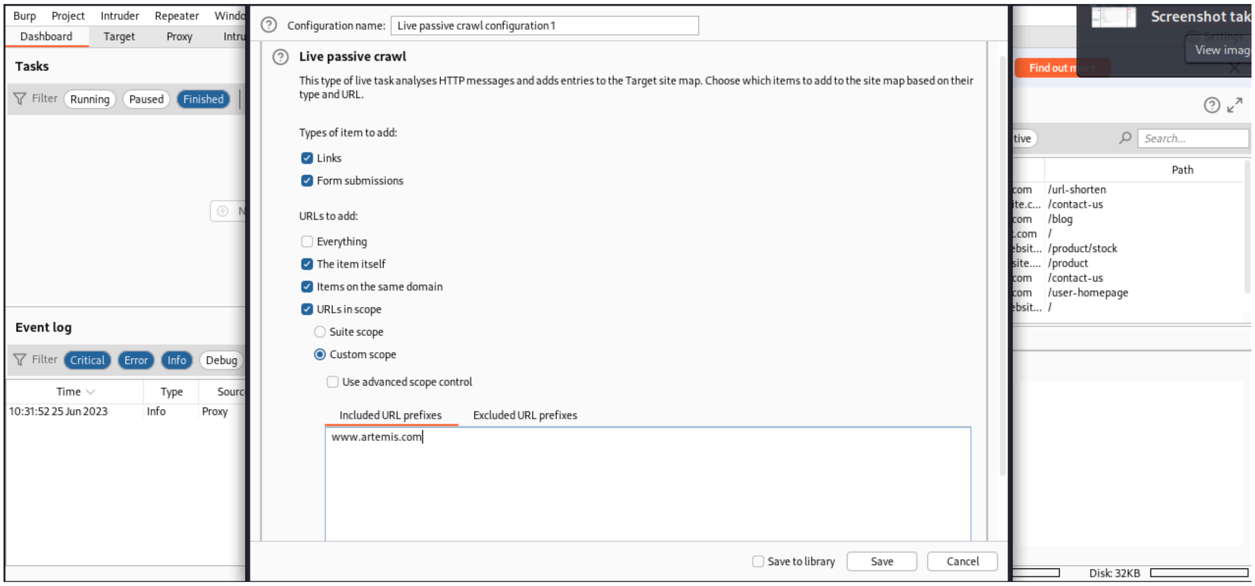
www.artemis.com

Select from library | Save to library

Deduplication

OK | Cancel

Time	Type	Source
10:31:52 25 Jun 2023	Info	Proxy



Configuration name: Live passive crawl configuration 1

Live passive crawl

This type of live task analyses HTTP messages and adds entries to the Target site map. Choose which items to add to the site map based on their type and URL.

Types of item to add:

☑ Links
☑ Form submissions

URLs to add:

□ Everything
☑ The item itself
☑ Items on the same domain
☑ URLs in scope
○ Suite scope
● Custom scope
□ Use advanced scope control

Included URL prefixes | Excluded URL prefixes

www.artemis.com

□ Save to library

```
Time               Type   Sourc
10:31:52 25 Jun 2023  Info   Proxy
```

```
com     /url-shorten
ite.c...  /contact-us
com     /blog
.com    /
bsit...  /product/stock
site....  /product
com     /contact-us
com     /user-homepage
bsit...  /
```

Challenges:

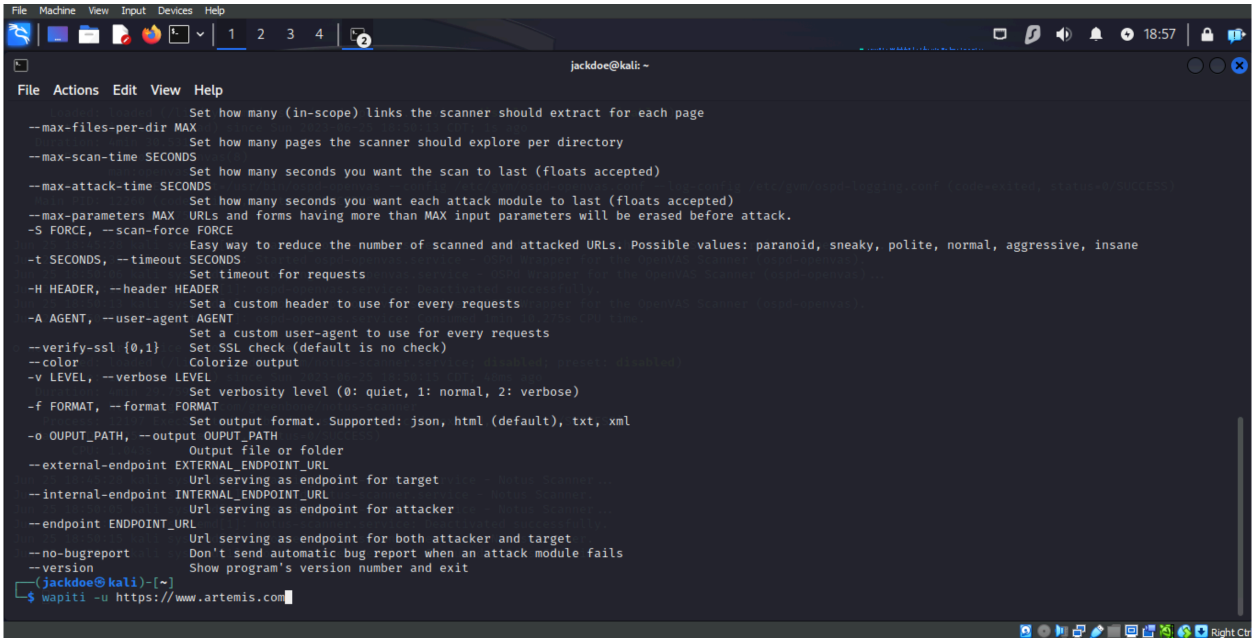
1. The community free edition is limited in features
2. Mainly used for web applications

Benefits:

1. Burp Suite has an excellent, intuitive GUI.
2. The professional edition contains advanced automated tools.
3. Can use passive scans and active scans

Wapiti

Purpose: Wapiti allows you to audit the security of your web applications. It performs “black-box” scans, i.e., it does not study the source code of the application but scans the web pages of the deployed web applications, looking for scripts and forms where it can inject data.


File Machine View Input Devices Help
1 2 3 4
18:57
jackdoe@kali: ~
File Actions Edit View Help
Right Ctrl

```
                        Set how many (in-scope) links the scanner should extract for each page
  --max-files-per-dir MAX
                        Set how many pages the scanner should explore per directory
  --max-scan-time SECONDS
                        Set how many seconds you want the scan to last (floats accepted)
  --max-attack-time SECONDS
                        Set how many seconds you want each attack module to last (floats accepted)
  --max-parameters MAX  URLs and forms having more than MAX input parameters will be erased before attack.
  -S FORCE, --scan-force FORCE
                        Easy way to reduce the number of scanned and attacked URLs. Possible values: paranoid, sneaky, polite, normal, aggressive, insane
  -t SECONDS, --timeout SECONDS
                        Set timeout for requests
  -H HEADER, --header HEADER
                        Set a custom header to use for every requests
  -A AGENT, --user-agent AGENT
                        Set a custom user-agent to use for every requests
  --verify-ssl {0,1}    Set SSL check (default is no check)
  --color               Colorize output
  -v LEVEL, --verbose LEVEL
                        Set verbosity level (0: quiet, 1: normal, 2: verbose)
  -f FORMAT, --format FORMAT
                        Set output format. Supported: json, html (default), txt, xml
  -o OUPUT_PATH, --output OUPUT_PATH
                        Output file or folder
  --external-endpoint EXTERNAL_ENDPOINT_URL
                        Url serving as endpoint for target
  --internal-endpoint INTERNAL_ENDPOINT_URL
                        Url serving as endpoint for attacker
  --endpoint ENDPOINT_URL
                        Url serving as endpoint for both attacker and target
  --no-bugreport        Don't send automatic bug report when an attack module fails
  --version             Show program's version number and exit
┌──(jackdoe㉿kali)-[~]
└─$ wapiti -u https://www.artemis.com
```

Challenges:

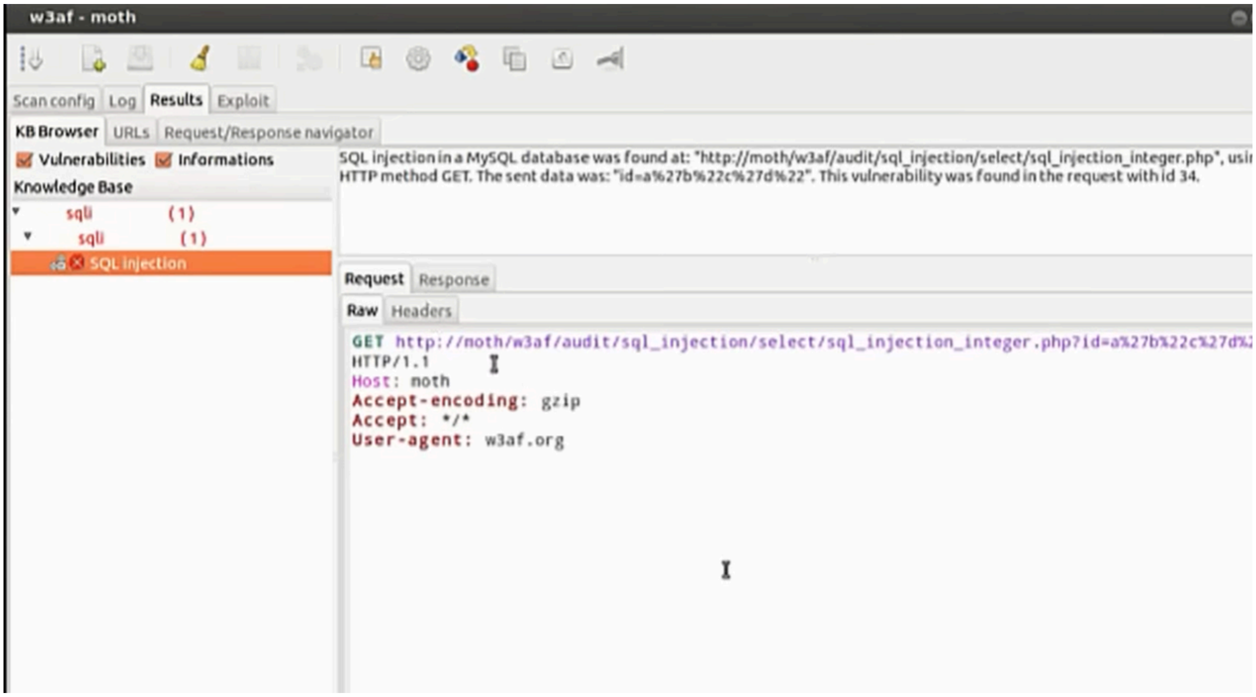
1. Wapiti does not have a GUI, which may make it difficult to understand results.
2. Many open-source tools have errors that need to be researched and fixed.

Benefits:

1. Generates vulnerability reports in various formats (HTML, XML, JSON, TXT, CSV)
2. Brute Force login form (using a dictionary list)
3. Can suspend and resume a scan or an attack
4. Check for TLS misconfiguration and vulnerabilities

W3af/W4af

Purpose: W3af is a Web Application Attack and Audit Framework that will identify vulnerabilities in web applications by sending specially crafted HTTP requests to them. It performs vulnerability testing and exploitation of vulnerabilities found.



SQL injection in a MySQL database was found at: "http://moth/w3af/audit/sql_injection/select/sql_injection_integer.php", usi
HTTP method GET. The sent data was: "id=a%27b%22c%27d%22". This vulnerability was found in the request with id 34.

```
GET http://moth/w3af/audit/sql_injection/select/sql_injection_integer.php?id=a%27b%22c%27d%2
HTTP/1.1
Host: moth
Accept-encoding: gzip
Accept: */*
User-agent: w3af.org
```

Challenges:

1. W3af runs on Python 2, which is deprecated. We will need to take additional steps to get it to run.
2. Attempted to run w4af, which is compatible with Python 3. Many dependencies were not part of the GitHub repo.

Benefits:

1. Based on all 5 tools for web app scanning, W3af has the best documentation available for users, which reduces the learning curve.
2. It has a simple GUI, making it user-friendly.

XSSPY

Purpose: XssPy is a Python tool for finding Cross-Site Scripting vulnerabilities in websites. This tool traverses the website and finds all the links and subdomains first. Next, it starts scanning each and every input on each and every page that it found during its traversal. It uses small yet effective payloads to search for XSS vulnerabilities. no image

No image

Challenges:

1. Running this program had errors with the way the code is written. The error source was print statements.
2. Unable to run the application on Windows or Kali because of dependency errors. As an example, libraries “lib” needed to be updated to “http.client.”

Benefits:

1. Short Scanning option available
2. Comprehensive Scanning
3. Finding subdomains
4. Checking every input on every page

Phase 4. Threat Assessment

Link to scenarios

Technical Report: Known Vulnerabilities and Remediation Actions

This technical report provides an overview of various known vulnerabilities and associated risks related to different scenarios. Each vulnerability is described along with the affected operating systems/versions, risks of exploitation, attack vectors, potential blocking mechanisms, and recommended remediation actions. Additionally, the Common Vulnerability Scoring System (CVSS) scores are included to assess the severity of each vulnerability.

Vulnerability: Unpatched RDP is exposed to the internet

Description: An Unpatched Remote Desktop Protocol (RDP) exposed to the internet poses a severe security risk. A notable vulnerability is CVE-2019-0708, also known as "BlueKeep," which allows attackers to execute arbitrary code by sending a specially crafted request to the RDP port (usually 3389).

Operating Systems/Versions Affected: Windows 7, XP, Vista, Server 2003, Server 2008.

Risks of Attempting to Exploit:

Exposing confidential information is not part of the project scope.
Potential damage to the system, including data corruption or deletion.
Denial of Service during exploitation.
Uncontrollable spread of Blue Keep due to its worm capabilities.
Attack Vectors: Using Metasploit to bypass authentication or social engineering to obtain credentials.

Potential Blocking Mechanisms: BlueKeep exploitation resembles a BlueKeep vulnerability scanner, which can be detected by network-level IDS/IPS if already able to detect the scanner sequence.

Remediation Action: Disable RDP if not needed. Block port 3389 using a firewall. Install the patch issued by Microsoft in 2019 to correct the vulnerability.

CVSS Score: 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Vulnerability: Web Application is Vulnerable to SQL Injection

Description: SQL Injection (SQLi) is a web security vulnerability that allows attackers to interfere with database queries. It can lead to unauthorized access, data exposure, and potential data modification. An example vulnerability is CVE-2013-0375 in the MySQL Server database.

Operating Systems/Versions Affected: Web applications using databases like Oracle, PostgreSQL, MySQL, and Microsoft. Applications using PHP and ASP are susceptible due to the prevalent older functional interfaces.

Risks of Attempting to Exploit:

Denial of Service.
Exposure of sensitive data.
Compromise of user privacy.
Attack Vectors: Inband, Out-of-band, or Inferential/Blind methods utilizing Union Operator, Boolean, Error-based, Out-of-band, and Time delay techniques.

Potential Blocking Mechanisms: Hardening databases and query structure, intrusion detection systems with SQLi detection capabilities.

Cracking Passwords: SQLi does not require passwords.

Remediation Action: Use parameterized queries (prepared statements) instead of string concatenation to prevent SQL injection. Employ intrusion detection systems and follow secure coding practices.

CVSS Score: 5.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N)

Vulnerability: Default Password on Cisco Admin Portal

Description: Cisco Network Registrar installations do not force users to change the default password, allowing potential unauthorized access and configuration changes. CVE-2011-2024 is an example vulnerability associated with the persistent default password.

Operating Systems/Versions Affected: Cisco Network Registrar Software Releases Before 7.2.

Risks of Attempting to Exploit:

Accidental reconfiguration of DNS, DHCP, and TFTP services.
Exposure of network structure.
Attack Vector: Internal network attack.

Potential Blocking Mechanisms: Possible Detection by Nessus Network Monitor.

Cracking Passwords: Detection of default password usage.

Remediation Action: Upgrade to Software Release 7.2 or apply the provided workaround to prevent exploitation.

CVSS Score: 10.0 (CVSS:2.0/AV:N/AC:L/Au:N/C:C/I:C/A:C)

Vulnerability: Apache Web Server Vulnerable to CVE-2019-0211

Description: The vulnerability allows a "worker" process to elevate its privileges, potentially enabling unauthorized code execution with root clearance. Exploitation can result in information disclosure, compromise of system integrity, or complete shutdown of the affected resource.

Operating Systems/Versions Affected: Apache web server releases for Unix systems, version 2.4.17 (Oct. 9, 2015) to version 2.4.38 (Apr. 1, 2019).

Risks of Attempting to Exploit:

Total information disclosure.
Total compromise of system integrity.
Total shutdown of the affected resource.
Attack Vectors: Local exploitation or running arbitrary scripts on the web server (PHP, CGI, etc.).

Potential Blocking Mechanisms: Possible Detection by Nessus Network Monitor.

Cracking Passwords: User password not required.

Remediation Action: Patch the flaw by updating servers to Apache httpd version 2.4.39. Apply the principle of least privilege to prevent potential related vulnerabilities.

CVSS Score: 7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Vulnerability: Web Server Exposing Sensitive Data

Description: A sensitive data exposure vulnerability allows unauthorized access to confidential information not intended to be publicly accessible. This includes passwords, credit card numbers, personally identifiable information (PII), or other confidential data. CVE-2019-2725 is an example vulnerability affecting Oracle WebLogic Server.

Operating Systems/Versions Affected: Oracle WebLogic Server versions 12.1.3.0.0 to 12.2.1.4.0.

Risks of Attempting to Exploit:

Exposure of sensitive data.
Invasion of user privacy.
Disruption of business operations.
Attack Vectors: Network-level vulnerabilities such as cross-site scripting (XSS), directory traversal, or SQL injection.

Potential Blocking Mechanisms: Possible Detection by Nessus Network Monitor.

Cracking Passwords: No password is required.

Remediation Action: Apply the patch provided by Oracle. Implement secure coding practices and conduct regular security assessments.

CVSS Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Vulnerability: Web Application with Broken Access Control

Description: Vulnerabilities with broken access control can lead to unauthorized access and potential remote code execution. An example vulnerability is CVE-2023-21996, a remote code execution vulnerability affecting Oracle WebLogic Server.

Operating Systems/Versions Affected: Oracle WebLogic Server versions 12.2.1.3.0, 12.2.1.4.0, and 14.1.1.0.0.

Risks of Attempting to Exploit:

Denial of Service.
Attack Vectors: Network-level Denial of Service attacks.

Potential Blocking Mechanisms: Detection by intrusion detection systems.

Cracking Passwords: No user interaction or passwords are needed.

Remediation Action: Oracle released a patch in April 2023 to address this vulnerability. Apply the patch to secure the system.

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Vulnerability: Oracle WebLogic Server Vulnerable to CVE-2020-14882

Description: CVE-2020-14882 is a remote code execution (RCE) vulnerability in the Console component of Oracle WebLogic Server. Successful exploitation allows an unauthenticated attacker to compromise the server and take complete control.

Operating Systems/Versions Affected: Oracle WebLogic Server versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0.

Risks of Attempting to Exploit:

A full takeover of the server, leading to a complete disruption of service.
Exposing sensitive data.
Attack Vectors: Network-level Denial of Service attacks.

Potential Blocking Mechanisms: Detection by vulnerability scanners capable of checking for this specific CVE.

Cracking Passwords: No user interaction or passwords are needed.

Remediation Action: Oracle made available a patch for supported, vulnerable instances. Apply the patch to mitigate the vulnerability.

CVSS Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Vulnerability: Misconfigured Cloud Storage (AWS Security Group Misconfiguration, Lack of Access Restrictions)

Description: Misconfigured cloud storage, such as AWS security group misconfiguration or lack of access restrictions, can lead to vulnerabilities and data breaches. Unauthorized access to resources in AWS accounts exposes them to potential attacks.

Operating Systems/Versions Affected: AWS EC2 and S3.

Risks of Attempting to Exploit:

Buckets are exposed to the public.
Exposing the root account because it is used as an everyday account.
Attack Vectors: Network-level vulnerabilities, like social engineering to obtain passwords or dictionary attacks.

Potential Blocking Mechanisms: Instructive security group rules to restrict resource access. Use AWS Security Hub and AWS GuardDuty for monitoring and automatic remediation.

Cracking Passwords: Brute force or social engineering attack on the root password.

Remediation Action: Implement security group rules to limit access to known IP addresses or known applications/networks. Utilize AWS Security Hub and AWS GuardDuty for monitoring AWS accounts and workloads.

CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Vulnerability: Microsoft Exchange Server is Vulnerable to CVE-2021-26855

Description: CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Microsoft Exchange Server, enabling unauthorized HTTP requests and authentication as the Exchange server. Exploitation exposes the network to denial-of-service attacks and potential data exposure.

Operating Systems/Versions Affected: Microsoft Exchange Server 2013, 2016, or 2019.

Risks of Attempting to Exploit: Exploitation could lead to denial of service, exposure of sensitive data, and network compromise.

Attack Vectors: Network-level active server-side request forgery.

Potential Blocking Mechanisms: Detection by vulnerability scanners capable of checking for this specific CVE. For example, ProxyLogon Scanner by Pentest-Tools.com and Nmap script Http-Vuln-cve2021-26855.nse by Microsoft.

Cracking Passwords: No user interaction or passwords are needed.

Remediation Action: Restrict untrusted connections and consider setting up a VPN to separate the Exchange server from external access. Apply additional security measures provided by Microsoft, such as security updates, security advisories, and guidance.

CVSS Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)