

## **ARTEMIS GAS, INC Penetration Test Phase 2: Identify Targets and Run Scans**

Nathan Tendido

Cybersecurity Career Track, Springboard

Penetration Test Capstone

August 13, 2023

## Phase 2 Introduction

Phase 2 will use input from Phase 1's Reconnaissance in order to perform host discovery and enumerate the target's network. Client provided information should continue to be limited in order to maintain external perspective.

Activities conducted during Phase 2 are expected to alert client's monitoring systems. Effort will be made by the testers in order to minimize disruptive traffic to client network/s. The client should continue to follow regular security protocols when systems are alerted. Findings and activities will be disclosed at the end of penetration testing activities in a final report.

### Objective

- Run scans to perform host discovery and enumerate the target's network.

Scanning and enumerative tools and techniques to be used are:

1. [Nmap](#) (*Network Scanning*)
2. [Netcat](#) (*Network Tool*)
3. [OpenVAS](#) (*Vulnerability Assessment*)
4. [Nessus by Tenable](#) (*Vulnerability Assessment*)
5. [Dirbuster by OWASP](#) (*Web Application Testing*)
6. [SQLmap](#) (*Web Application Testing*)

## Nmap

Source	<ul style="list-style-type: none"><li>• <a href="https://www.kali.org/tools/nmap/">https://www.kali.org/tools/nmap/</a></li><li>• (Online GUI) <a href="https://nmap.online/">https://nmap.online/</a></li></ul>
Objective	Comprehensively scan the target network and identify active hosts, open ports, services, and operating systems being used. Notable ports would include 21 ftp, 23 telnet, 25 smtp, 80 http, 110 pop3, and 443 https. Scan results will help determine potential entry points.
Limitations	Nmap may be limited by client's active firewall configurations and any action taken by client in response to activities performed by client's security team in response to Phase 2 activities.

### Process Notes

Perform a host discovery scan for live hosts using ICMP.

```
nmap -sn artemisenergypartners.com
```

Perform a scan to check for all hosts, including hosts with active firewalls blocking ICMP.

```
nmap -Pn artemisenergypartners.com
```

Perform OS fingerprinting scan.

```
nmap -O artemisenergypartners.com
```

Scan for open ports and services. Inputs are domain name or IP address.

```
nmap artemisenergypartners.com
```

Scan for port service version information and run nmap default enumerative scripts on the target port. Input is domain and port. -sV determines port service/version info and -sC runs nmap's default enumerative scripts.

```
nmap -sV -sC artemisenergypartners.com -p 21
```

## Netcat

Source	<ul style="list-style-type: none"><li>• <a href="https://www.kali.org/tools/netcat/">https://www.kali.org/tools/netcat/</a></li></ul>
Objective	Obtain information on target host, ports, and services using service banner grabbing.
Limitations	Firewalls, IDS/IPS systems can block traffic on Netcat ports. Netcat can potentially trigger port scanning detection mechanisms if they are in place, causing IP address blacklisting.

### Process Notes

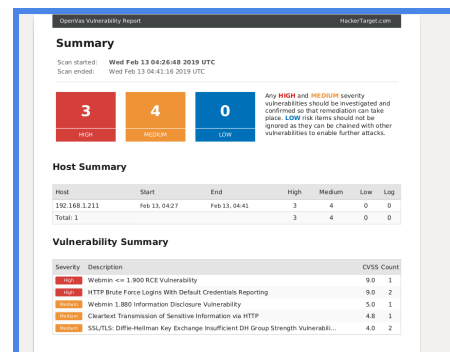
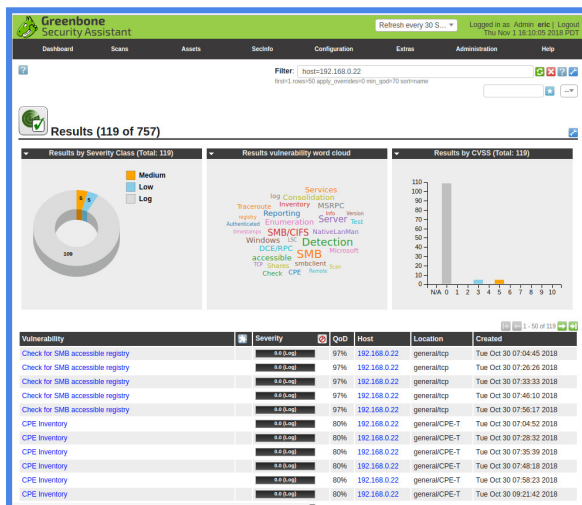
Perform banner grab. Inputs are domain name and port number. Port numbers obtained from Nmap tool.

```
nc artemisenergypartners.com 80
```

## OpenVAS

Source	<ul style="list-style-type: none"> <li>• <a href="https://www.kali.org/tools/gvm/">https://www.kali.org/tools/gvm/</a></li> <li>• <a href="https://openvas.org/">https://openvas.org/</a></li> </ul>
Objective	Perform vulnerability assessments on target systems to identify security weaknesses, misconfigurations, and potential entry points.
Limitations	OpenVAS processes can be resource intensive and may require particular time management in order to keep testing on schedule. Some networks configurations block usage of vulnerability assessment tools like OpenVAS.

## Process Notes



Source	<ul style="list-style-type: none"> <li>• <a href="https://www.tenable.com/products/nessus">https://www.tenable.com/products/nessus</a></li> </ul>
Objective	Perform vulnerability scanning to identify potential security gaps and entry points into the target network.
Limitations	Advanced features have licensing restrictions. Can also have resource-intensive processes like OpenVAS.

**Nessus**

Scores Settings

## Scan Templates

[Back to Scores](#)

VULNERABILITIES

- My Scores
- All Scores
- Traffic

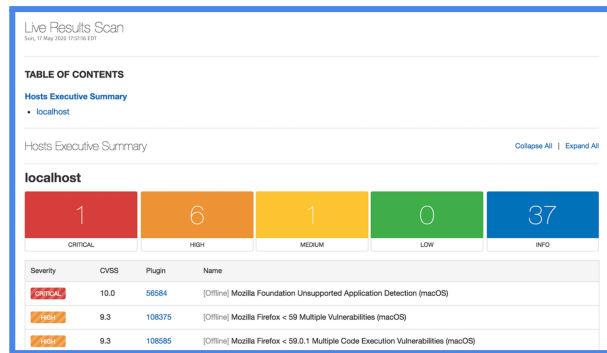
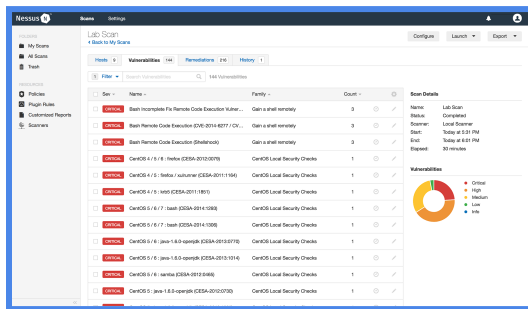
RECOMMENDATIONS

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Search Library

Scanner

<b>Advanced Scan</b> Perform a full system scan with any recommendations.	<b>Audit Cloud Infrastructure</b> Audit the configuration of third-party cloud services.	<b>Badlock Detection</b> Permissions and lock checks for CVE-2016-0118 and CVE-2016-0126.	<b>Bash Shellcheck Detection</b> Permissions and lock checks for CVE-2014-0121 and CVE-2014-7185.	<b>Basic Network Scan</b> A fast network scan suitable for any host.
<b>Credentialized Patch Audit</b> Push updates to hosts and reevaluate missing updates.	<b>CROWN Detection</b> Performs checks for CVE-2016-0800.	<b>Host Discovery</b> A simple scan to discover live hosts and open ports.	<b>Intel AMT Security Bypass</b> Permissions and lock checks for CVE-2017-0885.	<b>Internal PCI Network Scan</b> Perform an internal PCI DSS v2.1.3 vulnerability scan.
<b>Malware Scan</b> Scan for malware on Windows and Unix systems.	<b>MDM Config Audit</b> Audit the configuration of mobile device managers.	<b>Mobile Device Scan</b> Assess whether devices are on Microsoft Exchange or an MDM.	<b>Offline Config Audit</b> Audit the configuration of network devices.	<b>PCI Quarterly External Scan</b> Perform an external quarterly scanning as required by PCI.
<b>Policy Compliance Auditing</b> Audit system configurations against a known standard.	<b>SCAP and OVAL Auditing</b> Audit systems using SCAP and OVAL definitions.	<b>Shadow Broker Scan</b> Scan for vulnerabilities disclosed in the Shadow Broker leaks.	<b>Specfile and Mailboxes</b> Permissions and lock checks for CVE-2017-0755, CVE-2017-0756, and CVE-2017-0754.	<b>Warmcopy Passwords</b> Remote user login checks for KR01-750.



## Dirbuster by OWASP

Source	<ul style="list-style-type: none"> <li>• <a href="https://www.kali.org/tools/dirbuster/">https://www.kali.org/tools/dirbuster/</a></li> <li>• <a href="https://owasp.org/projects/">https://owasp.org/projects/</a></li> </ul>
Objective	Enumerate hidden or unprotected web directories and web files. Dirbuster can be run either in CLI or in GUI. Use -H option to run in CLI.
Limitations	DirBuster's brute force activity will alert client systems and may result in a security response to limit additional penetration testing activity.

### Process Notes

#### Run DirBuster

```
dirbuster
```

**OWASP DirBuster 1.0-RC1 – Web Application Brute Forcing**

File Options About Help

Target URL (eg http://example.com:80/)

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads  10 Threads ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

Char set  Min length  Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

## SQLmap

Source	<ul style="list-style-type: none"> <li>• <a href="https://www.kali.org/tools/sqlmap/">https://www.kali.org/tools/sqlmap/</a></li> <li>• <a href="https://sqlmap.org/">https://sqlmap.org/</a></li> </ul>
Objective	Automate detection of SQL injection vulnerabilities and enumerate database tables and obtain information of database structure.
Limitations	SQLmap usage can generate large volumes of network traffic and lead to degradation of database performance and even database crashing.

## Process Notes

## Run SQLmap and check for SQL injection vulnerabilities

```
sqlmap -u "www.artesmisgas.com/data.php"
```

Enumerate databases using target database

```
sqlmap -u "www.artesmisgas.com/datab.php" -D
```

## Open an interactive shell

```
sqlmap -u "www.artesmisgas.com/data.php" --os-shell
```

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch

[1.0.5.63#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```



## **Phase 2 Conclusion**

Activities during Phase 2 are likely to trigger IDS/IPS/Firewall port scanner alerts and other security mechanisms. The tester will run tests cautiously as to not result in client system downtime. If possible, a separate testing environment similar to the production environment can be used for traffic intensive processes.

### **Preparer Approval**

Signature:

Name:

Date:

### **Client Approval**

Signature:

Name:

Date: