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	• https://www.kali.org/tools/nmap/ • (Online GUI) https://nmap.online/
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	• https://www.kali.org/tools/netcat/
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

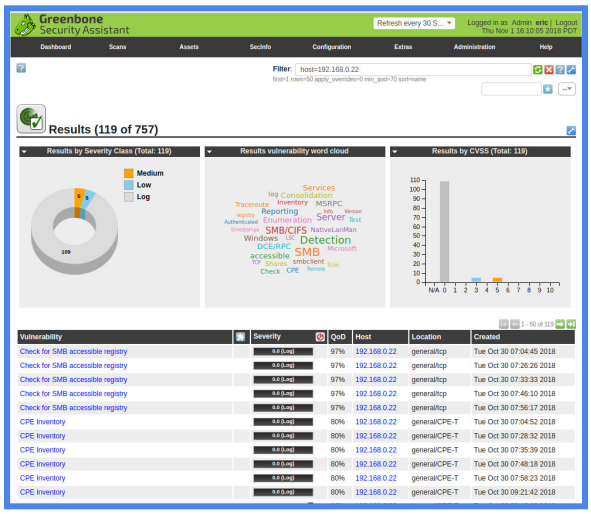
Perform banner grab. Inputs are domain name and port number. Port numbers obtained from Nmap tool.

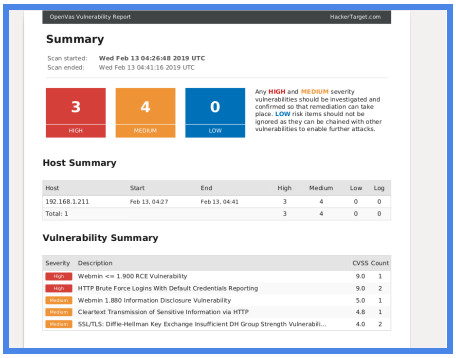
```
nc artemisenergypartners.com 80
```

OpenVAS

Source	• https://www.kali.org/tools/gvm/ • https://openvas.org/
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

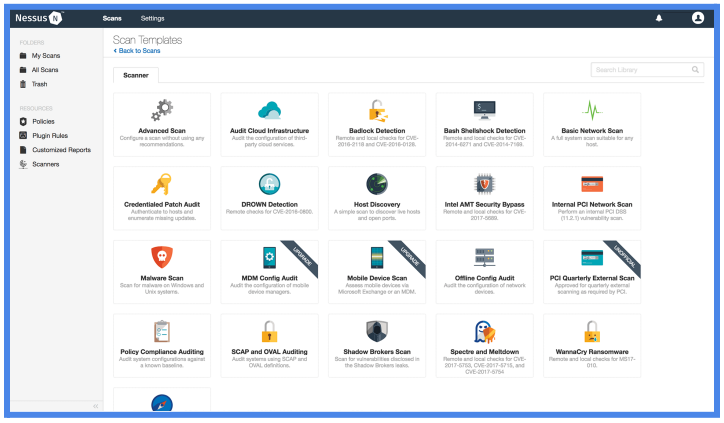


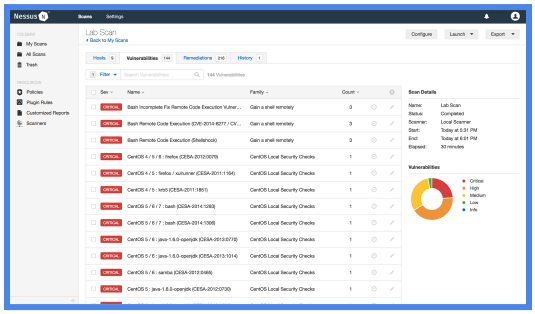


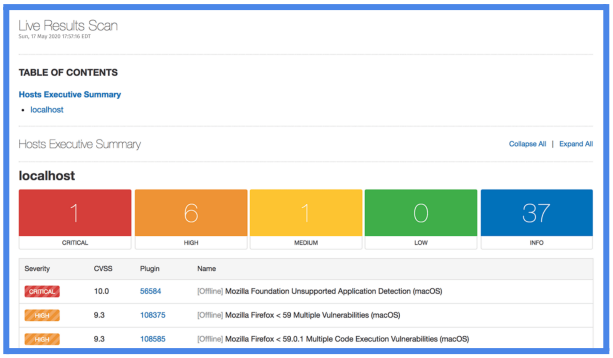
Nessus by Tenable

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

Process Notes







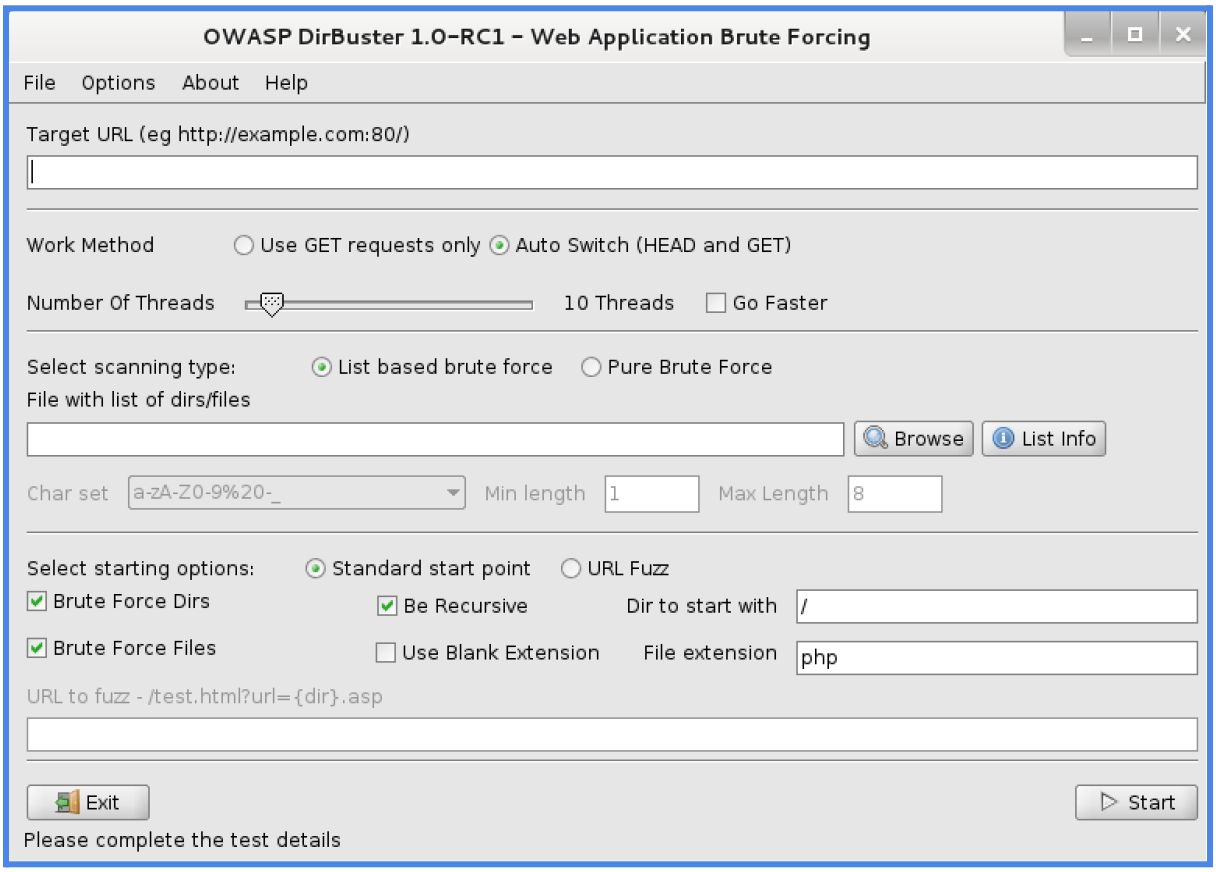
Dirbuster by OWASP

Source	• https://www.kali.org/tools/dirbuster/ • https://owasp.org/projects/
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
```



SQLmap

Source	• https://www.kali.org/tools/sqlmap/ • https://sqlmap.org/
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

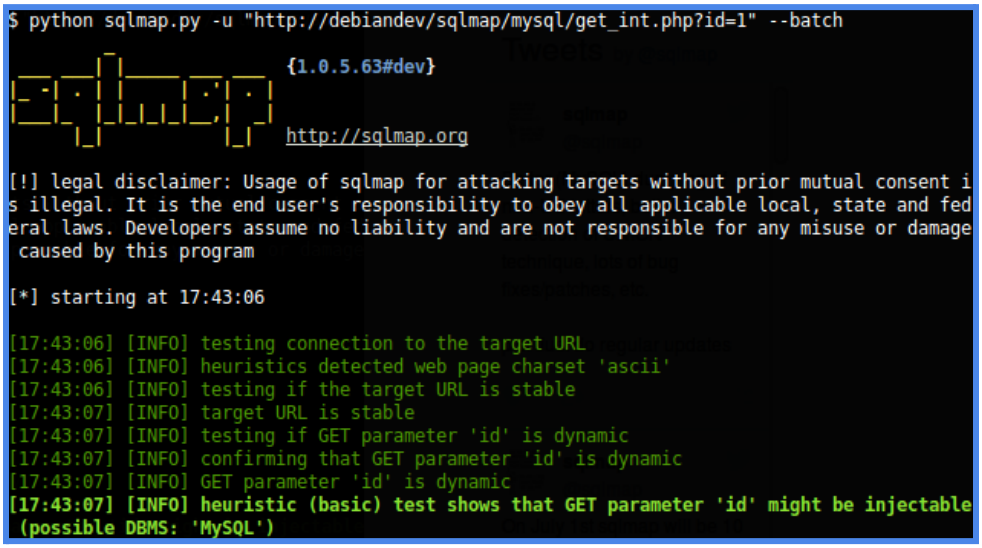
```
sqlmap -u "www.artesmisgas.com/data.php"
```

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
```



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: