[Utility Provider] Penetration Test Phase 3: Identify Vulnerabilities

Nathan Tendido
Cybersecurity Career Track, Springboard
Penetration Test Capstone
August 17, 2023

Phase 3 Introduction

Phase 3 will use input from Phase 1 and 2 in order to run vulnerability assessments and identify vulnerabilities in the target network. Client provided information should continue to be limited in order to maintain external perspective.

Activities conducted during Phase 3 may 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

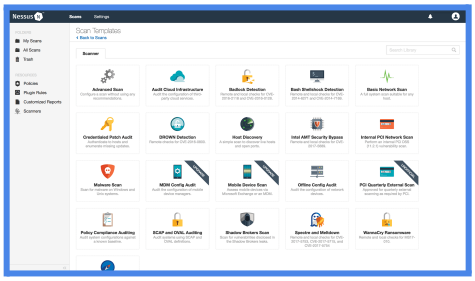
- Perform comprehensive vulnerability assessment scans to identify security weaknesses, misconfigurations, and security gaps in target systems

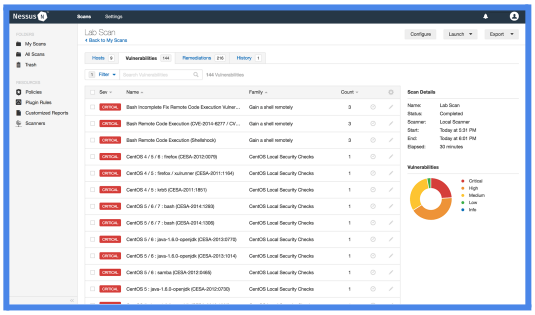
Vulnerability assessment tools to be used are:

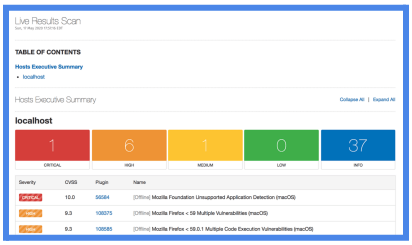
1. Nessus by Tenable *(Network and Web)*
2. GVM *(Network and Web)*
3. BurpSuite *(Application)*
4. ZAP Zed Attack Proxy *(Network and Web)*
5. OpenSCAP *(Compliance)*

Nessus by Tenable

Source	• https://www.tenable.com/products/nessus
Objective	• In Scans, define a target using IP, IP range, or domain • Select External Network Scan • Select Critical Systems Scan • Select Zero-Day Scan • In Scans, review Vulnerabilities to see found vulnerabilities with severity ratings • Choose Export to export reports for review
Pros	• Provides extensive vulnerability coverage • Paid version includes customer support
Cons	• Advanced features are locked in the paid Professional subscription • Higher learning curve for new Nessus users than compared to OpenVAS

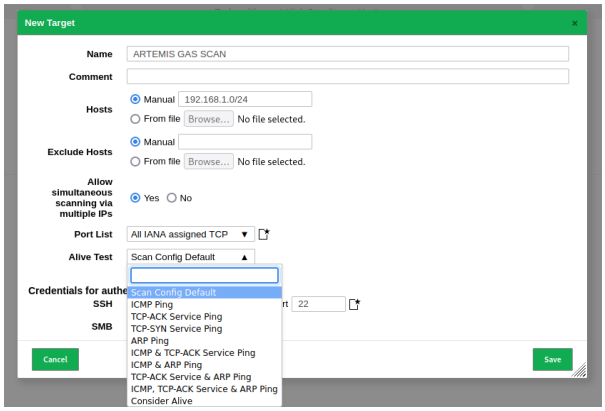


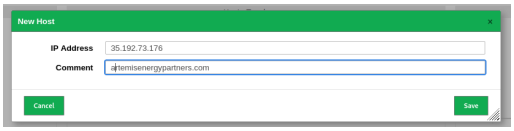




GVM (OpenVAS)

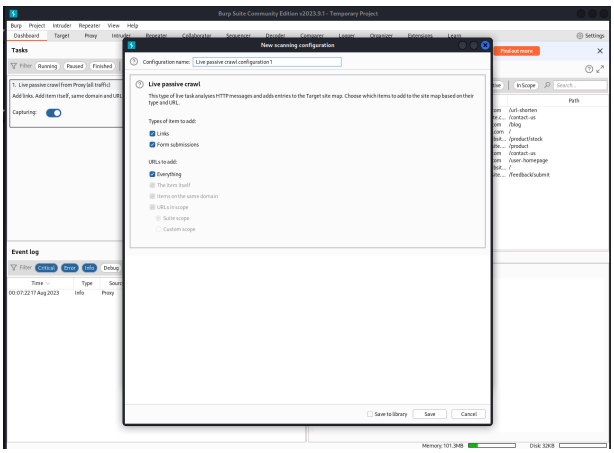
Source	• https://www.kali.org/tools/gvm/ • https://openvas.org/
Objective	• In Targets, define (or import) target ip address range • In Assets, perform Asset Discovery to discover all assets in the network • In Scans, begin scan and select scan configuration • In Configurations, define and customize scan configurations • Review scan results in Results and comb through any false positives • Generate a comprehensive report in Reports • If any credentials are in possession, configure a scan to perform authenticated scan
Pros	• Open-source • Comprehensive and customizable scanning
Cons	• Uses a lot of computing resources • False positives and negatives need to be manually identified

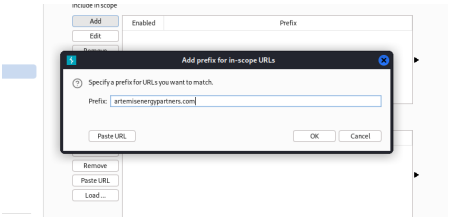




Burpsuite by PortSwigger Security

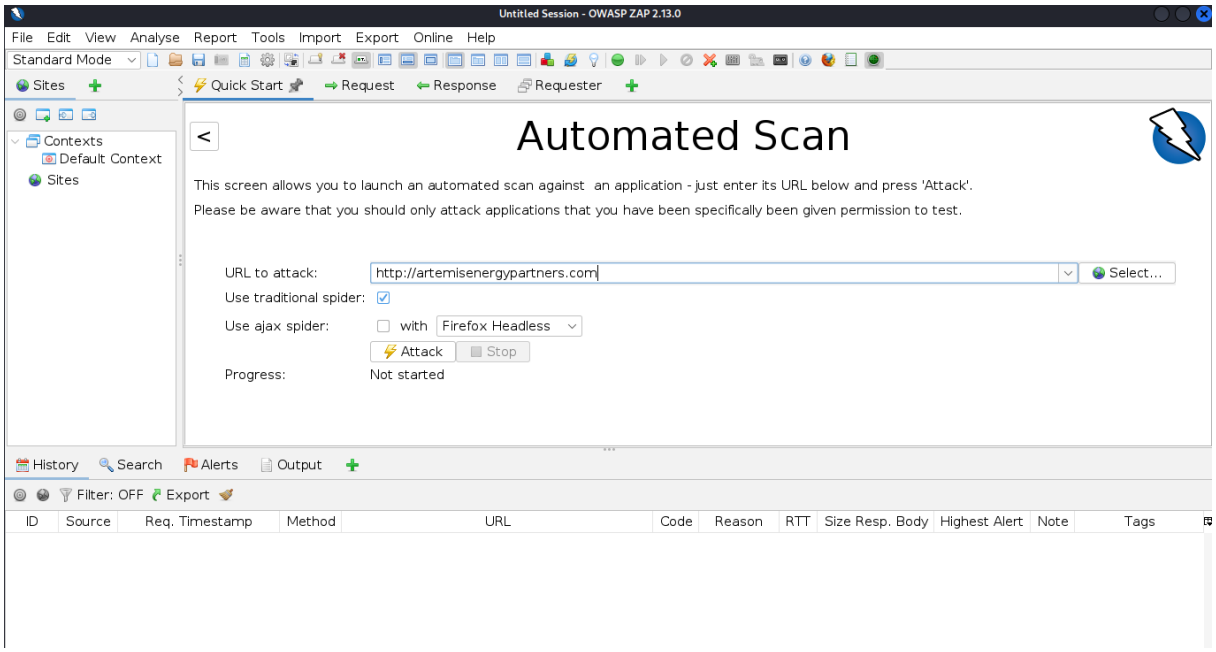
Source	• https://www.kali.org/tools/burpsuite/ • https://portswigger.net/
Objective	• Use Spider to crawl web application for SQL injection vulnerabilities • Use Scanner to scan for XSS, CSRF, command injection, path traversal, file inclusion, SSRF, RCE, header injection, and sensitive data exposure vulnerabilities • User Intruder to test for authentication bypass and input validation bypass vulnerabilities
Pros	• Automation of detection of common web vulnerabilities • Supports use of extensions and is updated frequently
Cons	• Advanced tools are locked in the Professional edition • Focuses on application-level testing, may not be best option for testing for network-level vulnerabilities





ZAP Zed Attack Proxy

Source	• https://www.kali.org/tools/zaproxy/ • https://www.zaproxy.org/
Objective	• In automated scan, enter URL to perform spidering and identify all related pages and components • In Proxy, use Proxy Mode to manually intercept and manipulate requests on [Utility Provider] website's forms, logins, etc checking for potential manipulatable URL variables • In Reports, generate reports with findings
Pros	• Open-source • Customizable scans, automation, and scripting
Cons	• Can be resource intensive • Results will need to be analyzed for false positives and false negatives (will still require manual effort and also require manual effort in manual testing features)



OpenSCAP

Source	• https://www.open-scap.org/
Objective	• Obtain a XCCDF XML file with defined benchmarks to assess compliance against • Check NIST Checklist Program, SCAP Security Guide, CIS Benchmarks • Run oscap xccdf eval --profile selected_profile --results-arf arf.xml --report report.html [[PATH TO CXXDF BENCHMARKFILE.XML]]
Pros	• Automated compliance checks can reveal potential focus areas for infiltration • Generated reports can be immediately useful 'action items' for client in later reports
Cons	• Not as comprehensive for vulnerability scanning as other tools • May require authentication credentials for scanning • Vulnerabilities may need to be inferred based on non-compliance findings

```
# oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_rht-ccp --results-arf arf.xml --report report.html /usr/share/xml/sc
ap/ssg/content/ssg-rhel6-ds.xml
Title   Ensure /tmp Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_tmp
Ident   CCE-26435-8
Result  fail

Title   Ensure /var Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_var
Ident   CCE-26639-5
Result  fail

Title   Ensure /var/log Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_var_log
Ident   CCE-26215-4
Result  fail

Title   Ensure /var/log/audit Located On Separate Partition
Rule    xccdf_org.ssgproject.content_rule_partition_for_var_log_audit
Ident   CCE-26436-6
Result  fail

Title   Ensure Red Hat GPG Key Installed
Rule    xccdf_org.ssgproject.content_rule_ensure_redhat_gpgkey_installed
Ident   CCE-26506-6
Result  fail

Title   Ensure gpgcheck Enabled In Main Yum Configuration
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Ident   CCE-26709-6
Result  pass

Title   Ensure gpgcheck Enabled For All Yum Package Repositories
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled
Ident   CCE-26647-8
Result  fail

Title   Ensure Software Patches Installed
Rule    xccdf_org.ssgproject.content_rule_security_patches_up_to_date
Ident   CCE-27635-2
Result  notchecked
```

Phase 3 Conclusion

Phase 3 will require most time spent in system set-up and configuration. In a case where the tester is not already familiarized with a tool, additional time should be taken into consideration when scheduling.

Preparer Approval

Signature:

Name:

Date:

Client Approval

Signature:

Name:

Date: