

LAB 09

Thầy Mai Hoàng Đình
Trường đại học FPT

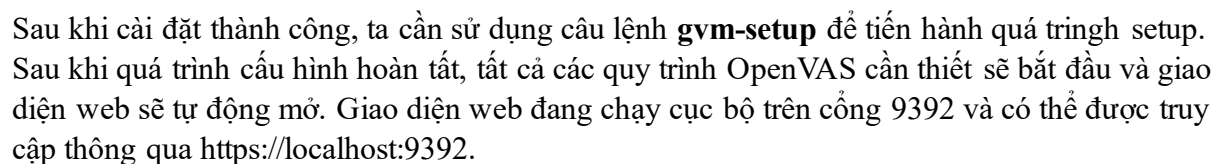
Người thực hiện
Đặng Hoàng Nguyên

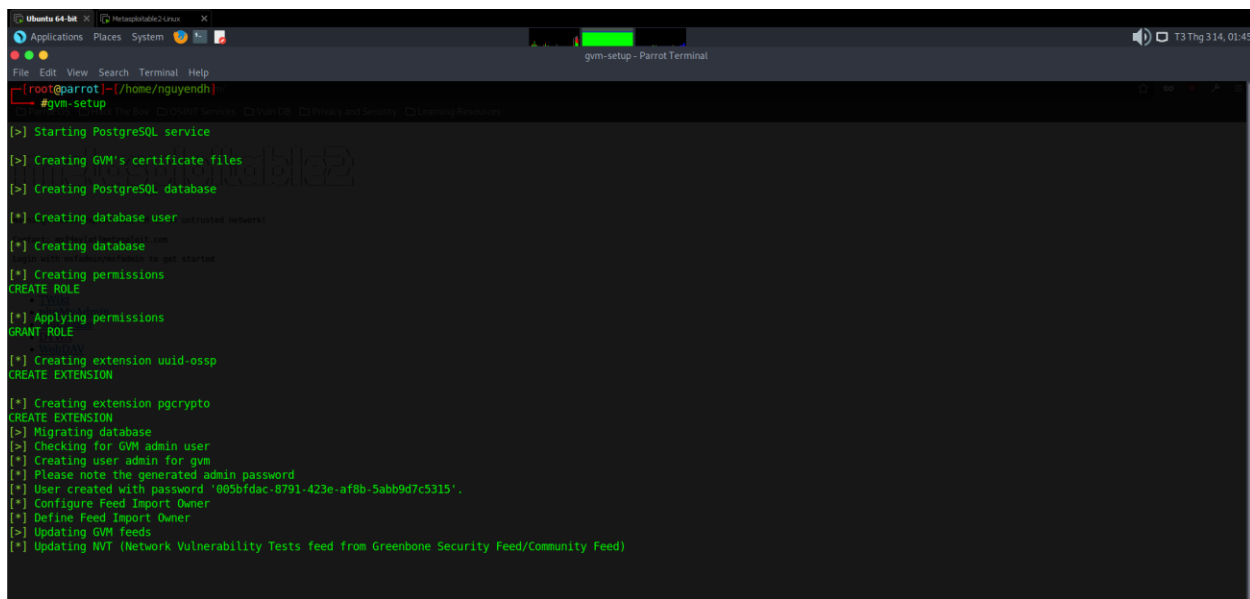
Chạy câu lệnh apt update để cập nhật lên phiên bản mới nhất

Chạy câu lệnh apt update để cập nhật lên phiên bản mới nhất



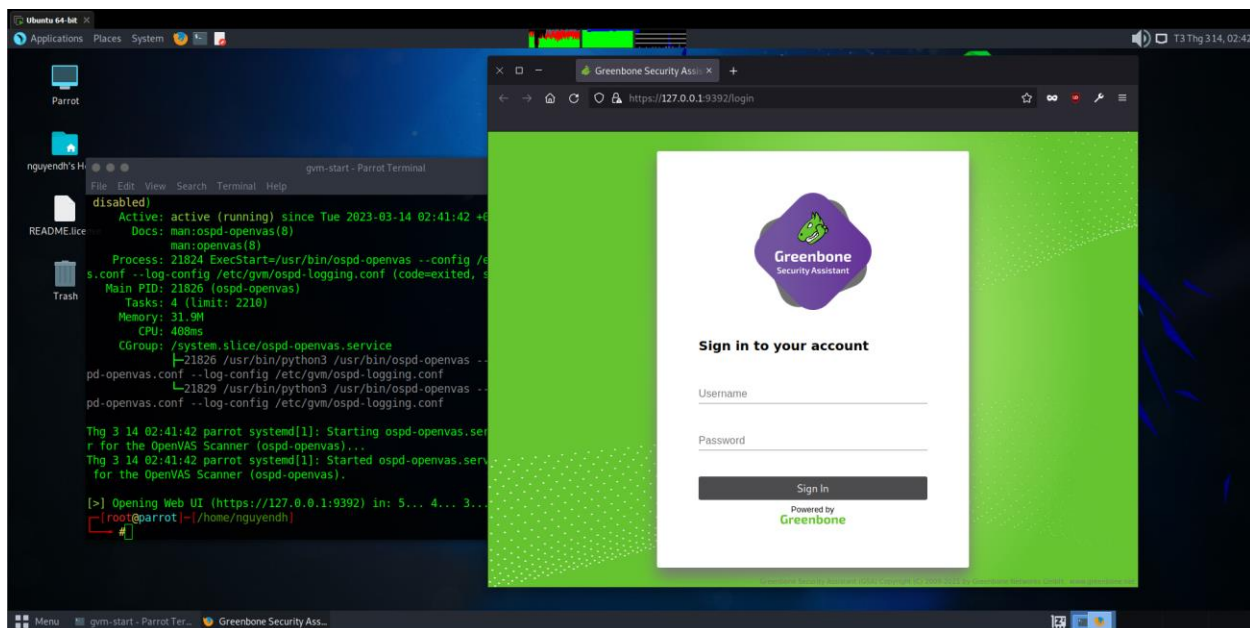
Bắt đầu tiến hành cài đặt openvas thông qua câu lệnh **apt install openvas**





```
[root@parrot:~]# gvm-setup
[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
[*] Creating database user
[*] Creating database
[*] Creating permissions
CREATE ROLE
[*] Applying permissions
GRANT ROLE
[*] Creating extension uuid-ossdp
CREATE EXTENSION
[*] Creating extension pgcrypto
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '005bf0ac-b791-423e-af8b-5abb9d7c5315'
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[>] Updating GVM Feeds
[*] Updating NVT (Network Vulnerability Tests feed from Greenbone Security Feed/Community Feed)
```

Sau khi cài đặt xong, ta có openvas ở trong phần application. Nhấn start để có thể vào bên trong trình duyệt hoặc có thể dùng gvm start



Trong lúc làm sẽ có những lỗi sau khi setup, mọi người có thể tham khảo lỗi ở một số trang sau:

<https://askubuntu.com/questions/1409379/openvas-scanner-is-not-found-error-for-gvm-check-setup-how-to-solve-it>

https://www.reddit.com/r/Kalilinux/comments/lkingw/error_on_gvmstart/

Vì thằng openvas không có default username và password nên chúng ta phải tạo username thông qua câu lệnh `sudo runuser -u _gvm -- gvmcmd --create-user=admin2 --new-password=12345` và nó sẽ trả về một cái password cho sẵn

Ubuntu 64-bit - VMware Workstation

Applications Places System

Greenbone Security Assistant

Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

Greenbone Security Assistant

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML

Filter: `auth=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort=reverse-severity level=info min_qod=70`

ID: 4b0e40eb-3a86-4ef8-8a83-c9268ffc4663
Modified: Tue Mar 14 00:49:02 2023
Created: Tue Mar 14 00:19:26 2023
Owner: admin

Report: Results (56 of 386)

Vulnerability	Severity	QoD	Host	Location	Actions
TWiki XSS and Command Execution Vulnerabilities	10.0 (high)	80%	192.168.154.129	80/tcp	
OS End Of Life Detection	10.0 (high)	80%	192.168.154.129	general/tcp	
rsync Passwordless / Unencrypted Cleartext Login	10.0 (high)	80%	192.168.154.129	512/tcp	
Distributed Ruby (Druby/Drb) Multiple Remote Code Execution Vulnerabilities	10.0 (high)	99%	192.168.154.129	8787/tcp	
Possible Backdoor: Ingreslock	10.0 (high)	99%	192.168.154.129	1524/tcp	
DistCC Remote Code Execution Vulnerability	9.9 (high)	99%	192.168.154.129	3632/tcp	
MySQL / MariaDB weak password	9.9 (high)	95%	192.168.154.129	3306/tcp	
VNC Brute Force Login	9.9 (high)	95%	192.168.154.129	5900/tcp	
PostgreSQL weak password	9.9 (high)	99%	192.168.154.129	5432/tcp	
rsh Unencrypted Cleartext Login	7.5 (high)	80%	192.168.154.129	514/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (high)	80%	192.168.154.129	80/tcp	
phpinfo() output Reporting	7.5 (high)	80%	192.168.154.129	80/tcp	
rsync Passwordless / Unencrypted Cleartext Login	7.5 (high)	70%	192.168.154.129	513/tcp	
Test HTTP dangerous methods	7.5 (high)	99%	192.168.154.129	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (high)	99%	192.168.154.129	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (high)	99%	192.168.154.129	21/tcp	
Check for Backdoor in UnrarRCd	7.5 (high)	70%	192.168.154.129	6667/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (high)	95%	192.168.154.129	80/tcp	
SSH Brute Force Logins With Default Credentials BruteForce	7.5 (high)	95%	192.168.154.129	22/tcp	

Nếu muốn xem một lỗ hổng nào đó, ta chỉ cần click vào để xem. Như lỗ hổng với mức nghiêm trọng là 10, ta có thể thực hiện được một cuộc tấn công XSS vào hệ thống

Applications Places System

Greenbone Security Assistant

Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resources

Greenbone Security Assistant

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

ID: 6b9c5f68-2aa3-46bf-9588-41d52d517931
Created: Tue Mar 14 00:39:30 2023
Modified: Tue Mar 14 00:39:30 2023
Owner: admin

Result: TWiki XSS and Command Execution Vulnerabilities

Vulnerability	Severity	QoD	Host	Location	Actions
TWiki XSS and Command Execution Vulnerabilities	10.0 (high)	80%	192.168.154.129	80/tcp	

Summary
The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 4.2.4

Impact
Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution
Solution type: ☐ Vendorfix
Upgrade to version 4.2.4 or later.

Affected Software/OS
TWiki, TWiki version prior to 4.2.4.

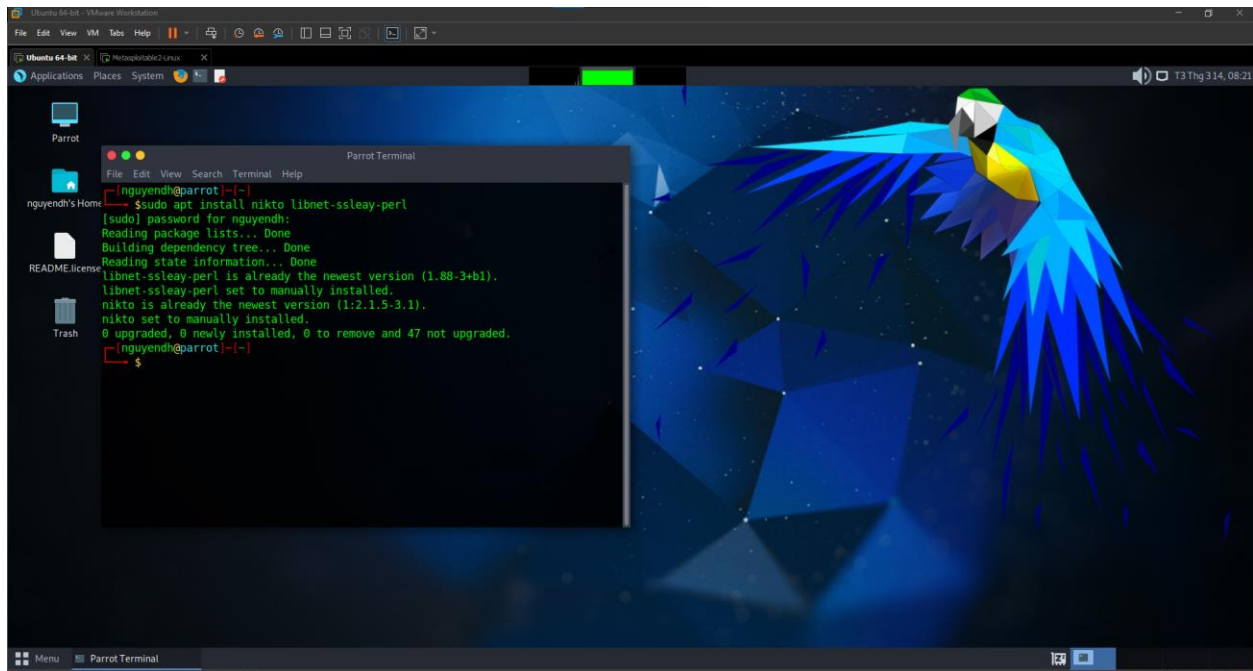
Vulnerability Insight
The flaws are due to:
- %URLPARAM()% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.
- %SEARCH()% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method
Details: TWiki XSS and Command Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800320)
Version used: \$Revision: 12952 \$

Product Detection Result

Installing and updating Nikto on Linux

Cài đặt Nikto trên Parrot



Sử dụng câu lệnh **nikto -h địa chỉ** ta có thể scan được những lỗ hổng được scan bởi nikto. Tại đây ta có thể thấy được những thông số cơ bản như hostname, địa chỉ ip, thời gian bắt đầu. Dịch vụ và những thức khác.

Trong kết quả của Nikto, các thông tin về máy chủ như phiên bản Apache và PHP được hiển thị, cùng với đó là các lỗ hổng có thể xảy ra. Cụ thể, trong phần kết quả trên, Nikto đã tìm thấy nhiều lỗ hổng tiềm ẩn, bao gồm phiên bản Apache đã cũ và khả năng bị tấn công XST. Ngoài ra, Nikto cũng đã phát hiện một số thư mục có thể được duyệt qua, cùng với việc tiết lộ các thông tin nhạy cảm về PHP. Cuối cùng, Nikto cũng đã tìm thấy các trang web quản lý MySQL như phpMyAdmin không được bảo vệ đầy đủ, cũng như các cookie không an toàn.

```
Ubuntu 64-bit - VMware Workstation
File Edit View VM Tools Help
Ubuntu 64-bit X ParrotOS962 Linux X
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
nikto set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 47 not upgraded.
[nguyendh@parrot]~$
$ nikto -h 192.168.154.129
- Nikto v2.1.5
-----
+ Target IP: 192.168.154.129
+ Target Hostname: 192.168.154.129
+ Target Port: 80
+ Start Time: 2023-03-14 08:23:16 (GMT7)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8201xdh28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?PHPBB5F2A0-3C92-11d3-A3A9-4C7B88C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Cookie phpMyAdmin created without the httponly flag
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server Leaks inodes via ETags, header found with file /icons/README, inode: 412190, size: 5108, mtime: 0x438c0358aae00
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 18 item(s) reported on remote host
+ End Time: 2023-03-14 08:23:31 (GMT7) (15 seconds)
-----
+ 1 host(s) tested
[nguyendh@parrot]~$
```