KEAMANAN SISTEM DAN JARINGAN

ENUMERASI

RINANZA ZULMY ALHAMRI, S.Kom., M.Kom
PSDKU POLINEMA DI KOTA KEDIRI

Kode : KIF195004
Kredit : 3 SKS
Semester : 5

MENU

- Konsep Enumerasi
- Enumerasi Jaringan Lokal
- Enumerasi Spesifikasi Jaringan dan Sistem
- Enumerasi Layanan

Konsep Enumerasi

- Enumerasi bertujuan untuk mendaftar, mengkaji, memeriksa, mengalisis secara satu persatu informasi yang diperoleh untuk nantinya diujicoba pada tahap selanjutnya dalam melakukan penyerangan target
- Bila footprinting sekedar memperoleh informasi personal/administratif, jaringan, dan sistem. Kemudian scanning/probing memeriksa secara lebih spesifik dan teknis pada kerentanan target. Maka enumerasi mencoba untuk memastikan mengumpulkan informasi yang didapat saat footprinting dan scanning/probing.
- Sebenarnya dalam Certified Ethical Hacker (CEH), reconnaissance/recon merupakan tahap pre-testing (tahap sebelum uji coba penyerangan) dimana tahap recon ini terdiri dari 3 sub-tahap footprinting, scanning/probing, dan enumerasi
- Tahap recon merupakan tahap aksi pasif dimana hanya mengumpulkan informasi dan data

Tipe Enumerasi

- Enumerasi jaringan lokal – mengumpulkan informasi perangkat yang terhubung pada jaringan lokal
- Enumerasi informasi administratif / personal – mengumpulkan informasi personal, akun, administratif target melalui search engine atau social media
- Enumerasi kondisi jaringan yang digunakan – mengumpulkan informasi kondisi target dalam menggunakan jaringan internet
- Enumerasi kondisi sistem – mengumpulkan informasi kondisi sistem pada target
- Enumerasi layanan – mengumpulkan informasi kondisi layanan yang diberikan oleh target

ENUMERASI JARINGAN LOKAL

Bisa dilakukan apabila berada pada suatu jaringan seperti hotspot atau jaringan LAN. Target merupakan sistem komputer personal yang terhubung pada jaringan

Advanced IP Scanner

- Aplikasi berbasis Windows yang mudah digunakan, instan, dan gratis
- Download aplikasi pada advanced-ip-scanner.com kemudian install
- Fitur:
    1. Scanning jaringan → tentukan range IP kemudian klik scan, maka akan muncul hasil PC yang aktif, hostname, alamat IP, manufacturer, alamat MAC pada jaringan lokal
    2. Penggunaan tools jaringan → ping, traceroute, telnet, ssh
    3. Penggunaan aplikasi → HTTP, HTTPS, FTP
    4. Remote Desktop
    5. Output report berupa xls /csv
- Tutorial bisa dibaca secara jelas dan mudah di advanced-ip-scanner.com/help
- Jika PC target memiliki celah keamanan seperti sharing folder, allow privilege, kesalahan setting firewall maka dengan mudah interfensi dilakukan dengan advanced IP scanner ini

ENUMERASI INFORMASI ADMINISTRATIF SERTA KONDISI JARINGAN DAN SISTEM

Target merupakan sistem komputer berbasis server / client yang terhubung pada jaringan internet / lokal. Telah dilakukan saat melakukan footprinting tapi belum terdokumentasi secara baik sebagai langkah enumerasi

Enumerasi dengan Melakukan Listing

- Mendokumentasikan hasil footprinting dan scanning/probing sebagai langkah enumerasi jaringan dan sistem selengkap-lengkapnya
- Listing baik informasi dari segi jaringan, sistem, maupun administratif
- Contoh:

No	Objek	Jumlah	Hasil
1	Nama Domain	1	polinema.ac.id
2	Domain Id	1	PANDI-D01261
3	Aktivasi	3	Created: 8/6/2011 Updated: 16/4/2018 Expired: 10/6/2027
4	Registrar	8	PANDI id: indosat m2 organisasi: PT Indosat Mega Media kota: Jakarta Selatan provinsi: DKI Jakarta kodepos: 12550 negara: Indonesia telepon: 02178546969 email: optech@indosat.net.id
5	Alamat IP Server	1	114.6.41.77
6	Nameserver	1	ns1.polinema.ac.id
7	Mailserver	5	ALT2.ASPMX.L.GOOGLE.COM. ALT3.ASPMX.L.GOOGLE.COM. ALT4.ASPMX.L.GOOGLE.COM. ASPMX.L.GOOGLE.COM. ALT1.ASPMX.L.GOOGLE.COM.
8	Route	2	_gateway(10.0.2.2) _gateway(10.0.2.2)
9	Round Trip Time	4	min: 283ms avg: 403ms max: 503ms mdev: 90ms
10	Operating System	1	Ubuntu Linu
11	Web Server	1	Apache 2.4.18
12	Web CMS	1	Wordpress
13	TCP Open Port	6	21, 22, 53, 80, 443, 3306
14	UDP Open Port	4	53, 67, 520, 4500
15	..... DST	...DST	....DST

ENUMERASI LAYANAN
Target polinema.ac.id

Melakukan enumerasi pada port yang terbuka pada target semaksimal mungkin menggunakan tools NMAP. Layanan yang rentan meliputi FTP, Web File, dan MySQL.

NMAP – Advance
Enumerasi FTP via NMap

1. **Pastikan port FTP terbuka**
2. **Gunakan script FTP anonymous, system, enumeration, backdoor, serta default**
3. **Analisis hasil enumerasi**

Daftar script default untuk ftp

```
root@kali-nanza:~# ls /usr/share/nmap/scripts/ | grep -e "ftp"
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
tftp-enum.nse
```

CATATAN:
Dengan optional –d akan jelas tertera penggunaan script danscript sudah bekerja
Hasil analisis FTP open tapi upload tidak ada pada website jadi hasil tidak ada informasi yang menarik

Pastikan port ftp open dimana menggunakan versi vsftpd

```
root@kali-nanza:~# nmap -sV -p21 polinema.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 06:16 EDT
Nmap scan report for polinema.ac.id (114.6.41.77)
Host is up (0.015s latency).
rDNS record for 114.6.41.77: 114-6-41-77.resources.indosat.com

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix
```

Pilih script yang berkaitan dengan port, namun hasil tidak keluar

```
root@kali-nanza:~# nmap --script=ftp-anon.nse,ftp-syst.nse,ftp-vsftpd-backdoor.nse,tftp
-enum.nse -p21 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 07:50 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.00066s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
```

Dicoba dengan script default yang artinya menggunakan seluruh script ftp tetap saja tidak ada informasi yang keluar… artinya FTP target disetting Aman

```
root@kali-nanza:~# nmap --script=default -p21 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 08:27 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0015s latency).

PORT   STATE SERVICE
21/tcp open  ftp
```

NMAP – Advance
Enumerasi Web File via NMAP

1. **Pastikan port HTTP terbuka**
2. **Gunakan script HTTP enum**
3. **Analisis hasil enumerasi**

List script http sangat banyak

```
root@kali-nanza:~# ls /usr/share/nmap/scripts/ | grep -e "http"
http-adobe-coldfusion-apsa1301.nse
http-affiliate-id.nse
http-apache-negotiation.nse
http-apache-server-status.nse
http-aspnet-debug.nse
http-auth-finder.nse
http-auth.nse
```

Script http-enum mencoba menggali informasi dengan mentok informasi versi apache

```
root@kali-nanza:~# nmap -p 80 --script=http-enum.nse 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 07:44 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0013s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|_  /: Root directory w/ listing on 'apache/2.4.18 (ubuntu)'

Nmap done: 1 IP address (1 host up) scanned in 8.51 seconds
```

```
root@kali-nanza:~# nmap -p 80 --script=default 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 07:58 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0019s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-title: Index of /
```

Dicoba script default terlihat informasi bahwa target bisa dibua index of lewat browser

HTTP open dengan versi Apache httpd

```
root@kali-nanza:~# nmap -sV -p80 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 07:57 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0066s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18
Service Info: Host: hasil1.polinema.ac.id
```

Meskipun tidak keluar informasi file yang ada namun dengan terbukanya Index of menjadi awal yang baik untuk penetrasi sehingga web kurang aman

NMAP – Advance
Enumerasi Database via NMap

1. **Pastikan port MySQL terbuka**
2. **Gunakan script MySQL enum dan empty-password**
3. **Analisis hasil enumerasi**

Daftar script mysql

```
root@kali-nanza:~# ls /usr/share/nmap/scripts/ | grep -e "mysql"
mysql-audit.nse
mysql-brute.nse
mysql-databases.nse
mysql-dump-hashes.nse
mysql-empty-password.nse
mysql-enum.nse
mysql-info.nse
mysql-query.nse
mysql-users.nse
mysql-variables.nse
mysql-vuln-cve2012-2122.nse
```

MySQL open dengan versi MySQL 5.7

```
root@kali-nanza:~# nmap -sV -p3306 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 08:39 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0021s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.25-0ubuntu0.16.04.2
```

Script default memberikan informasi umum mengenai kemampuan MySQL target

```
root@kali-nanza:~# nmap -p 3306 --script=default 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 08:06 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0012s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.7.25-0ubuntu0.16.04.2
|   Thread ID: 274176
|   Capabilities flags: 63487
|   Some Capabilities: SupportsTransactions, InteractiveClient, ConnectWithDatabase, Lo
ngPassword, DontAllowDatabaseTableColumn, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis,
 Speaks41ProtocolOld, FoundRows, SupportsLoadDataLocal, Speaks41ProtocolNew, ODBCClient
, Support41Auth, SupportsCompression, LongColumnFlag, SupportsAuthPlugins, SupportsMult
ipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x1Bm:6,m-%(e?"
| \x1A\x7Fo7#mu
|_  Auth Plugin Name: 96
```

```
root@kali-nanza:~# nmap -p3306 --script=mysql-enum.nse,mysql-empty-password.nse 114.6.4
1.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 08:41 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0019s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
```

Dicoba script custom keluar username dan pass dimana misal user root pass-nya kosong, disini merupakan informasi menarik dan bisa diperdalam

NMAP – Advance
Enumerasi Database via NMap

```
root@kali-nanza:~# mysql -u root -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'114.5.99.222' (using password: NO)
root@kali-nanza:~# mysql -u test -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'test'@'114.5.99.222' (using password: NO)
root@kali-nanza:~# mysql -u netadmin -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'netadmin'@'114.5.99.222' (using password: N
O)
root@kali-nanza:~# mysql -u user -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'user'@'114.5.99.222' (using password: NO)
root@kali-nanza:~# mysql -u guest -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'guest'@'114.5.99.222' (using password: NO)
root@kali-nanza:~# mysql -u sysadmin -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'sysadmin'@'114.5.99.222' (using password: N
O)
root@kali-nanza:~# mysql -u administrator -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'administrator'@'114.5.99.222' (using passwo
rd: NO)
root@kali-nanza:~# mysql -u webadmin -h 114.6.41.77 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'webadmin'@'114.5.99.222' (using password: N
```

Mencoba masuk mysql target dengan username yang telah terdaftar dan pass kosong → tidak ada yang berhasil. Namun paing tidak telah diperoleh enumerasi username MySQL dimana tinggal mencari password… artinya DB kurang aman

```
root@kali-nanza:~# nmap -p3306 --script=mysql-brute.nse --script-args=mysql-brute.threa
ds=100 114.6.41.77

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-17 08:54 EDT
Nmap scan report for 114-6-41-77.resources.indosat.com (114.6.41.77)
Host is up (0.0014s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 50009 guesses in 456 seconds, average tps: 115.9
```

Menggunakan MySQL brute dengan mengirimkan percobaan 100 kali tetap saja nihil tidak bisa masuk. Overall informasi menarik tetap didapat

ENUMERASI LAYANAN
Target unpkediri.ac.id

Selain mendata, menghitung, memeriksa hasil footprinting, scanning, & probing satu-persatu, dianalisis juga bagian mana yang kerentanan tinggi (vulnerability) terhadap celah keamanan

Ganti unpkediri.ac.id karena saat membuat modul ini polinema.ac.id sedangn down

Memastikan port terbuka

```
root@kali-nanza:~# nmap -sS -p 21,22,80,443,3306 unpkediri.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 11:37 EDT
Nmap scan report for unpkediri.ac.id (117.102.75.90)
Host is up (0.020s latency).

PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
```

Enumerasi FTP: PORT 21

```
root@kali-nanza:~# nmap -p 21 --script ftp-anon,ftp-syst,tftp-enum 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 12:34 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0057s latency).

PORT   STATE SERVICE
21/tcp open  ftp
```

```
root@kali-nanza:~# nmap -p 21 --script default 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 12:35 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0070s latency).

PORT   STATE SERVICE
21/tcp open  ftp
```

Lagi-lagi ftp script nse tidak bekerja… gk masalah tetap semangatttt
Bila perlu coba semua nse yang ada pada FTP

Enumerasi SSH: PORT 22

```
root@kali-nanza:~# ls /usr/share/nmap/scripts/ | grep -e "ssh"
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse
```

Metode otentikasi ssh

Hostkey yang terenkripsi

Algoritma2 yang digunakan pada ssh

```
root@kali-nanza:~# nmap -p22 --script ssh2-enum-algos,ssh-auth-methods,ssh-hostk
ey,ssh-run,sshv1 unpkediri.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 11:55 EDT
NSE: [ssh-run] Failed to specify credentials and command to run.
Nmap scan report for unpkediri.ac.id (117.102.75.90)
Host is up (0.0078s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|_    password
| ssh-hostkey:
|   1024 e3:74:c2:27:07:2f:dd:96:ba:85:bb:18:34:39:ba:36 (DSA)
|   2048 8f:a7:a9:aa:3d:d2:be:b2:60:f2:a1:47:52:0d:c0:45 (RSA)
|_  256 97:0c:fe:28:5e:a6:14:ae:66:e7:9e:e8:42:a4:e3:2c (ECDSA)
|_ssh-run: Failed to specify credentials and command to run.
| ssh2-enum-algos:
|   kex_algorithms: (7)
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
```

Enumerasi HTTP: PORT 80

```
root@kali-nanza:~# nmap -p 80 --script http-methods --script-args http-methods.t
est=all 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 12:38 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0067s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
```

Metode yang digunakan pada port HTTP ada GET, HEAD, POST, dan OPTION

```
root@kali-nanza:~# nmap -p 80 --script http-waf-detect,http-waf-fingerprint 117.
102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 12:43 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0062s latency).

PORT   STATE SERVICE
80/tcp open  http
```

Tidak terdeteksi web application firewall (waf)

```
root@kali-nanza:~# nmap -p 80 --script default 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 12:47 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0054s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-title: Server Hangup
```

Info gak penting, intinya server aktif

```
root@kali-nanza:~# nmap -p 80 --script http-enum,http-userdir-enum,http-wordpres
s-enum,http-svn-enum 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 12:49 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0054s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /robots.txt: Robots file
|_  ..%2f..%2f..%2f..%2f..%2f..%2f..%2f/var/mobile/Library/AddressBook/Addr
essBook.sqlitedb: Possible iPhone/iPod/iPad generic file sharing app Directory T
raversal (iOS)
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   plugins
|     akismet
|     contact-form-7
|     wordpress-seo
|     jetpack
```

http-enum terdapat /robots.txt

Plugin yang dipakai pada wordpress

Enumerasi HTTPS: PORT 443 menggunakan nse yang hampir sama dengan HTTP

```
root@kali-nanza:~# ls /usr/share/nmap/scripts/ | grep -e "https"
ip-https-discover.nse
```

```
root@kali-nanza:~# nmap -p 443 --script ip-https-discover 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:02 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0059s latency).

PORT    STATE SERVICE
443/tcp open  https
```

HTTPS IP discover tidak bekerja dan tidak ada hasil

```
root@kali-nanza:~# nmap -p 443 --script default 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:03 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0049s latency).

PORT    STATE SERVICE
443/tcp open  https
|_http-title: UN PGRI Kediri
| ssl-cert: Subject: commonName=unpkediri.ac.id
| Subject Alternative Name: DNS:unpkediri.ac.id
| Not valid before: 2020-08-17T05:34:35
|_Not valid after:  2020-11-15T05:34:35
```

Script default muncul informasi sertifikat SSL

```
root@kali-nanza:~# nmap -p 443 --script http-methods --script-args http-methods.
test=all 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:07 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0082s latency).

PORT    STATE SERVICE
443/tcp open  https
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
```

Metode yang digunakan pada port HTTPS ada GET, HEAD, POST, dan OPTION

```
root@kali-nanza:~# nmap -p 443 --script http-waf-detect,http-waf-fingerprint unp
kediri.ac.id

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:09 EDT
Nmap scan report for unpkediri.ac.id (117.102.75.90)
Host is up (0.0076s latency).

PORT    STATE SERVICE
443/tcp open  https
```

Tidak terdeteksi web application firewall (waf)? Atau nse tidak bekerja dengan baik??? Tp memang website tidak menggunakan https

```
root@kali-nanza:~# nmap -p 443 --script http-enum,http-userdir-enum,http-wordpre
ss-enum,http-svn-enum 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:12 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0051s latency).

PORT    STATE SERVICE
443/tcp open  https
| http-enum:
|_  /robots.txt: Robots file
| http-wordpress-enum:
| Search limited to top 100 themes/plugins
|   themes
|     twentyeleven
|     twentytwelve
```

Info sama seperti enumerasi HTTP

Enumerasi MySQL: PORT 3306

```
root@kali-nanza:~# nmap -p 3306 --script default 117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:30 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0073s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
|_mysql-info: ERROR: Script execution failed (use -d to debug)
```

Error berarti sistem menolak script nse

```
root@kali-nanza:~# nmap -p 3306 --script mysql-audit,mysql-databases,mysql-info
117.102.75.90

Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-24 13:32 EDT
Nmap scan report for 117.102.75.90
Host is up (0.0041s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
|_mysql-info: ERROR: Script execution failed (use -d to debug)
```

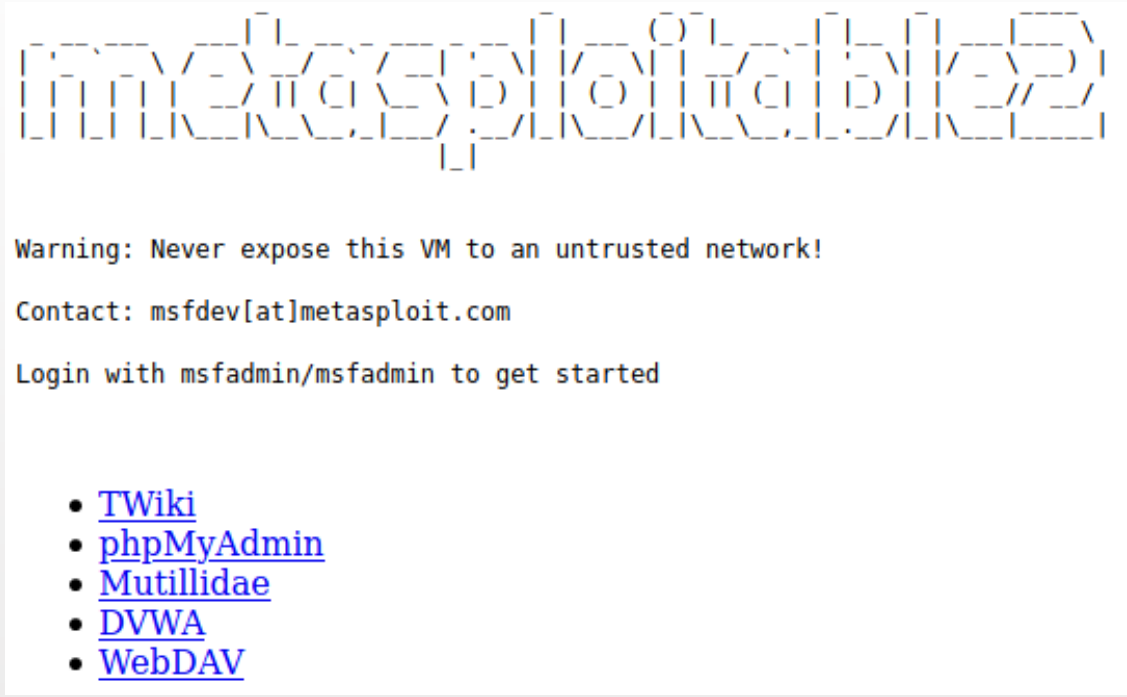
Error juga berarti sistem menolak script nse… we r not lucky

```
root@kali-nanza:~# ls /usr/share/nmap/scripts/ | grep -e "mysql"
mysql-audit.nse
mysql-brute.nse
mysql-databases.nse
mysql-dump-hashes.nse
mysql-empty-password.nse
mysql-enum.nse
mysql-info.nse
mysql-query.nse
mysql-users.nse
mysql-variables.nse
mysql-vuln-cve2012-2122.nse
```

TIDAK ADA YANG BERHASIL,
BEDA TARGET BEDA HASIL SEMANGATT

TUGAS

- Lakukan Enumerasi secara detail dengan target



Buat video screen record Enumerasi pada SO Metasploitable 2

- Enumerasi layanan port 21, 22, 80, dan 3306 dengan menggunakan sebuah script saja seperti yang telah dipraktikkan
- Jelaskan apa yang menarik pada feedback / hasil yangditemukan, referensi hasil ada nmap.org dan sumber internet lainnya

TERIMAKASIH