Network penetration testing

Marek Kumpošt

Penetration testing

> Authorized attempt to violate specific constraints defined in a form of a policy

> Technique to discover, understand, and document all security holes found in a system

    > Not restricted to network only

> Penetration testing can prove presence of a security flaw

    > But not their total absence

Penetration study

> Complex process to evaluate (through penetration testing) the strength of all security controls within the system/network

> + suggestions how to fix them

> The goal of a penetration study is also finding interpretations (causes) of discovered vulnerabilities and to suggest how to remove/close them

> Not intrusive - detects/enumerate potential vulnerabilities but does not exploit them

Lifecycle of penetration testing

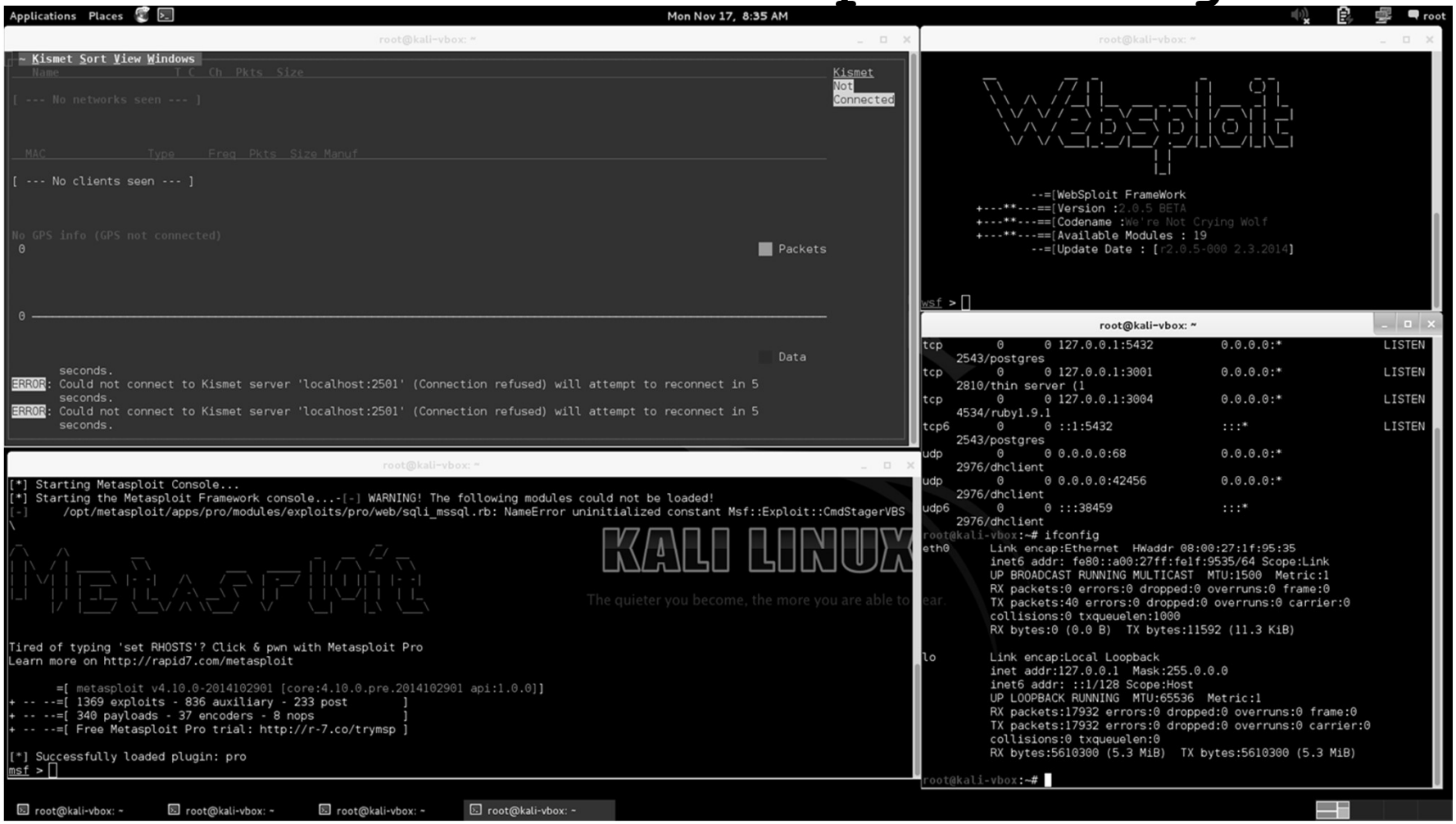
> Phase 1: Information gathering about tested environment

> Phase 2: Scanning, enumeration, fingerprinting, ...

> Phase 3: Exploitation, vulnerability testing, ...

> Phase 4: Report and evaluation

Recommended tools and pentesting arsenal



Types of penetration testing

> **Black-box pentesting**

  > Tester knows no details about tested environment

  > Simulation of an external attacker with no internal knowledge

> **Grey-box pentesting**

  > Tester might have some arch. details, credentials, etc...

> **White-box pentesting**

  > Nothing is hidden from the tester in this scenario

  > Arch. details, credentials, source code of tested application

Determining scope of a pentest (1/2)

> Who has the authority to authorize testing?

> What is the purpose and what is the timeframe for the testing?

> Who is authorized to know about the pentesting (IT, mngmt, ITsec.)?

> What documentation will you have (IP ranges, applications, DB, ...)?

Determining scope of a pentest (2/2)

> What are the conditions for the test to be immediately stopped?

> Will additional permissions be required for exploiting vulnerabilities?

> Are there any legal implications you should be aware of?

> Is social engineering (or physical security) also part of the pentest?

Most important part of any pentest?

> Take good notes!!! ;-)

> Of your setup, testing procedures, used tools, results, follow-ups

> Tips for tools: Dradis, MagicTree, ThreadFix or just Notepad ...

Information gathering

> Name servers, IP ranges, banners, running services

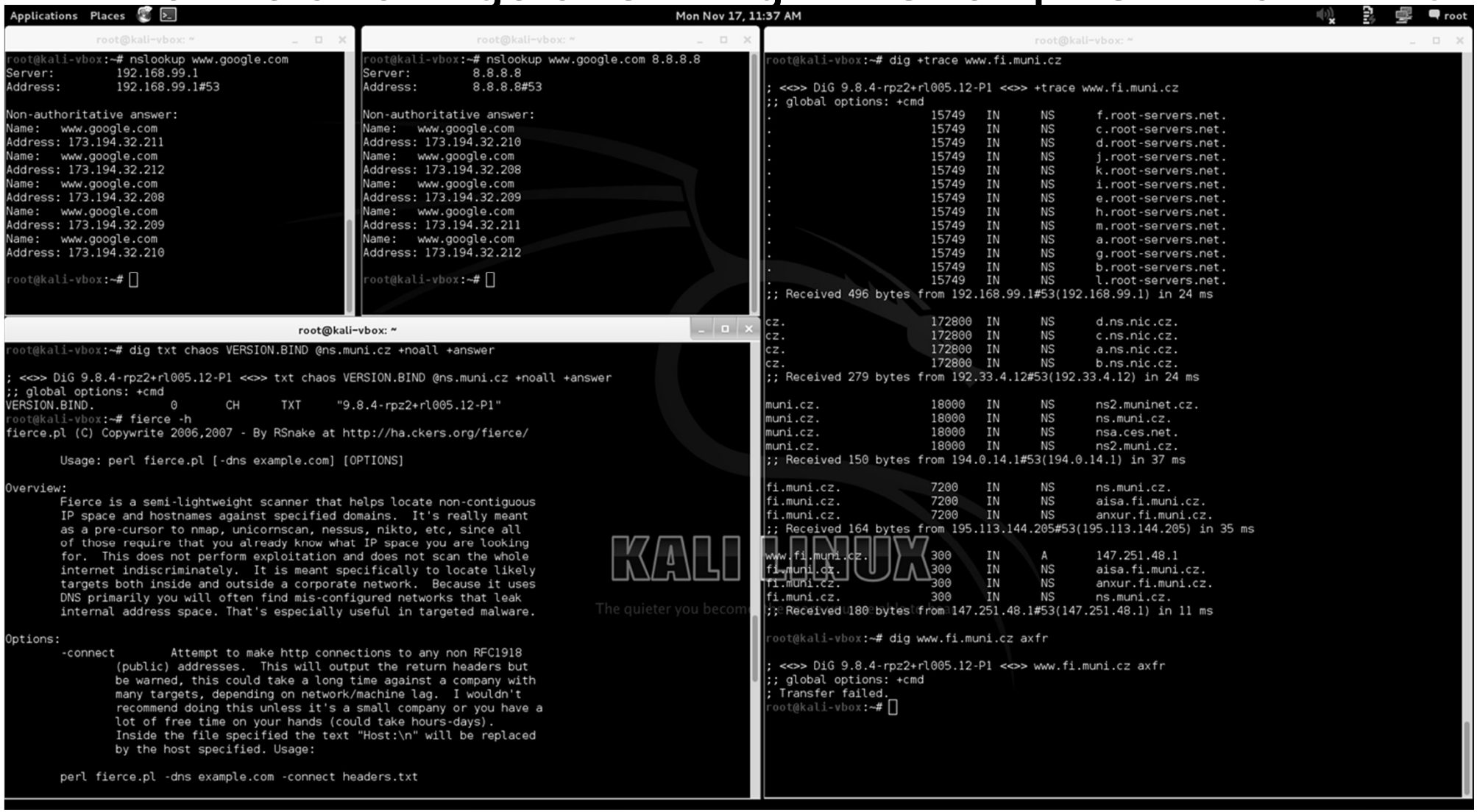
> Operating systems, IDS/IPS presence

> Technology used, network device types

> Google for anything, that might help you to build knowledge

> Find everything that you can -> prioritize, remove misleading data -> use gathered data to develop a pentest plan

Information gathering – example with DNS



How do you get info you want?

> Network scanning – typical approach in the beginning

  > List of live IP addresses – PING scan

  > Information from WHOIS database – DNS name, A, MX records, geolocation, reputation of an IP, SPAM db lookups, etc.

www.tcpiputils.com

How do you get info you want?

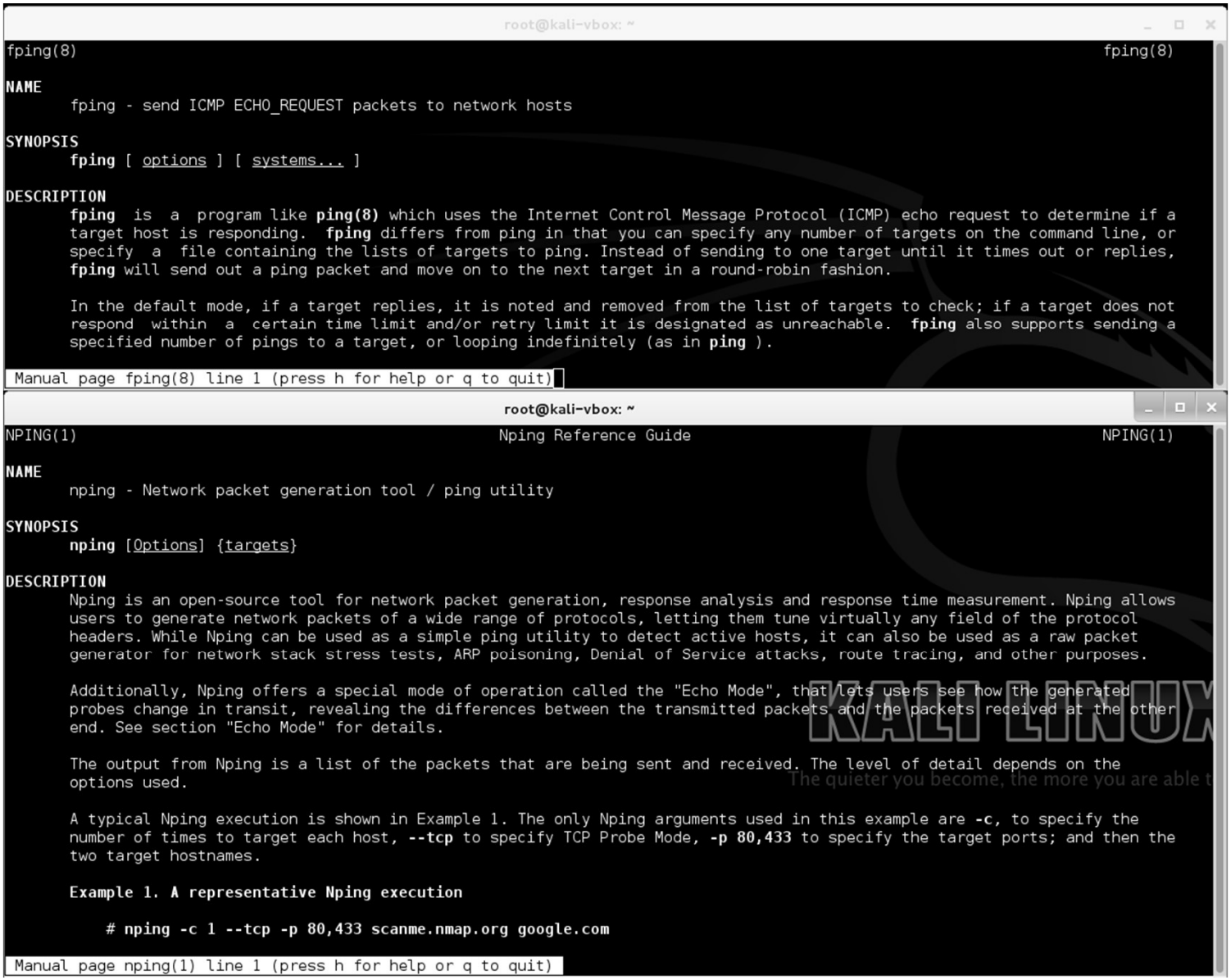
> Service scanning

- > Basic portscan – slower scan with nmap
- > Gives us information about running services
- > Services fingerprinting
  - - possible versions of services
  - - used to identify vulnerabilities and help us finding relevant exploits

PING scan of a network

> What is this technique good for?

- > Get a list of live IP addresses
- > Get a list of your targets, understand IP addressing structure
- > Basic PING scan can be easily detected


root@kali-vbox: ~
fping(8) fping(8)
NAME
fping - send ICMP ECHO_REQUEST packets to network hosts
SYNOPSIS
fping [options] [systems...]
DESCRIPTION
fping is a program like ping(8) which uses the Internet Control Message Protocol (ICMP) echo request to determine if a target host is responding. fping differs from ping in that you can specify any number of targets on the command line, or specify a file containing the lists of targets to ping. Instead of sending to one target until it times out or replies, fping will send out a ping packet and move on to the next target in a round-robin fashion.
In the default mode, if a target replies, it is noted and removed from the list of targets to check; if a target does not respond within a certain time limit and/or retry limit it is designated as unreachable. fping also supports sending a specified number of pings to a target, or looping indefinitely (as in ping).
Manual page fping(8) line 1 (press h for help or q to quit)
root@kali-vbox: ~
NPING(1) Nping Reference Guide NPING(1)
NAME
nping - Network packet generation tool / ping utility
SYNOPSIS
nping [Options] {targets}
DESCRIPTION
Nping is an open-source tool for network packet generation, response analysis and response time measurement. Nping allows users to generate network packets of a wide range of protocols, letting them tune virtually any field of the protocol headers. While Nping can be used as a simple ping utility to detect active hosts, it can also be used as a raw packet generator for network stack stress tests, ARP poisoning, Denial of Service attacks, route tracing, and other purposes.
Additionally, Nping offers a special mode of operation called the "Echo Mode", that lets users see how the generated probes change in transit, revealing the differences between the transmitted packets and the packets received at the other end. See section "Echo Mode" for details.
The output from Nping is a list of the packets that are being sent and received. The level of detail depends on the options used.
A typical Nping execution is shown in Example 1. The only Nping arguments used in this example are -c, to specify the number of times to target each host, --tcp to specify TCP Probe Mode, -p 80,433 to specify the target ports; and then the two target hostnames.
Example 1. A representative Nping execution
nping -c 1 --tcp -p 80,433 scanme.nmap.org google.com
Manual page nping(1) line 1 (press h for help or q to quit)

Getting more info about targets?

> Services scanning – fingerprinting and service banners

> Get info about running services

  > Versions of services

  > Operating system of a server and its possible version

  > Patches of a service or operating system

  > Enabled modules, internal service name, ...

Service scanning with NMAP

```
root@kali-vbox:~# nmap -A 192.168.99.10

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-30 07:05 EST
Nmap scan report for SIP_tel (192.168.99.10)
Host is up (0.0028s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE    VERSION
80/tcp open  tcpwrapped
|_http-title: Sipura SPA Configuration
MAC Address: 00:0E:08:DC:68:80 (Cisco Linksys)
Device type: VoIP phone
Running: Linksys embedded
OS CPE: cpe:/h:linksys:spa901_1-line_ip_phone cpe:/h:linksys:spa921_1-line_ip_phone_with_1-port_ethernet cpe:/h:linksys:spa941_4-line_ip_phone_with_1-port_ethernet
OS details: Linksys SPA901, SPA921, or SPA 941 SIP VoIP phone
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   2.83 ms SIP_tel (192.168.99.10)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.42 seconds
root@kali-vbox:~#
```

> nmap –A is very noisy and easy to discover scan

> -sS – half-open scan, more stealthy

Basic nmap options for scanning

> --open – report only open ports of a target

> -Pn – skip host discovery (if i.e. firewall drops ping)

> T0-5 – aggressiveness of a scan 0-slowest, 5-insane

> -sA/P/X/S/T/U/M/I/C – different scan types

> -oA/G/X/N – output from nmap scan – good for import to msf

Usage of nmap scripts

> Make sure you **fully** understand any script that you run! ;-)

> nmap –sC <target> - runs about 50 basic set of nmap scripts, but is very loud on the network...

```
root@kali-vbox:/usr/share/nmap/scripts# l |wc -l
475
root@kali-vbox:/usr/share/nmap/scripts# l |grep -i -E "ssl|ssh|smb"
-rw-r--r-- 1 root root  3809 Aug 23 06:47 rmi-vuln-classloader.nse
-rw-r--r-- 1 root root 46084 Aug 23 06:47 smb-brute.nse
-rw-r--r-- 1 root root 28215 Aug 23 06:47 smb-check-vulns.nse
-rw-r--r-- 1 root root  4890 Aug 23 06:47 smb-enum-domains.nse
-rw-r--r-- 1 root root  3606 Aug 23 06:47 smb-enum-groups.nse
-rw-r--r-- 1 root root  8320 Aug 23 06:47 smb-enum-processes.nse
-rw-r--r-- 1 root root 12820 Aug 23 06:47 smb-enum-sessions.nse
-rw-r--r-- 1 root root  6271 Aug 23 06:47 smb-enum-shares.nse
-rw-r--r-- 1 root root 12546 Aug 23 06:47 smb-enum-users.nse
-rw-r--r-- 1 root root  1743 Aug 23 06:47 smb-flood.nse
-rw-r--r-- 1 root root  4789 Aug 23 06:47 smb-ls.nse
-rw-r--r-- 1 root root  8793 Aug 23 06:47 smb-mbenum.nse
-rw-r--r-- 1 root root  6863 Aug 23 06:47 smb-os-discovery.nse
-rw-r--r-- 1 root root  5127 Aug 23 06:47 smb-print-text.nse
-rw-r--r-- 1 root root 64768 Aug 23 06:47 smb-psexec.nse
-rw-r--r-- 1 root root  4582 Aug 23 06:47 smb-security-mode.nse
-rw-r--r-- 1 root root  2423 Aug 23 06:47 smb-server-stats.nse
-rw-r--r-- 1 root root 14149 Aug 23 06:47 smb-system-info.nse
-rw-r--r-- 1 root root  1557 Aug 23 06:47 smbv2-enabled.nse
-rw-r--r-- 1 root root  5635 Aug 23 06:47 smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root  7342 Aug 23 06:47 smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root  5658 Aug 23 06:47 ssh2-enum-algos.nse
-rw-r--r-- 1 root root 14815 Aug 23 06:47 ssh-hostkey.nse
-rw-r--r-- 1 root root  1445 Aug 23 06:47 sshv1.nse
-rw-r--r-- 1 root root  8596 Jun 30 14:33 ssl-ccs-injection.nse
-rw-r--r-- 1 root root  7560 Aug 23 06:47 ssl-cert.nse
-rw-r--r-- 1 root root  3807 Aug 23 06:47 ssl-date.nse
-rw-r--r-- 1 root root 15235 Aug 23 06:47 ssl-enum-ciphers.nse
-rw-r--r-- 1 root root  2051 Aug 23 06:47 ssl-google-cert-catalog.nse
-rw-r--r-- 1 root root  8069 Aug 23 06:47 ssl-heartbleed.nse
-rw-r--r-- 1 root root  4220 Aug 23 06:47 ssl-known-key.nse
-rw-r--r-- 1 root root  6821 Aug 23 06:47 sslv2.nse
root@kali-vbox:/usr/share/nmap/scripts# nmap --script-help "ssl-heartbleed.nse"

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-30 12:43 EST

ssl-heartbleed
Categories: vuln safe
http://nmap.org/nsedoc/scripts/ssl-heartbleed.html
  Detects whether a server is vulnerable to the OpenSSL Heartbleed bug (CVE-2014-0160).
  The code is based on the Python script ssltest.py authored by Jared Stafford (jspenguin@jspenguin.org)
root@kali-vbox:/usr/share/nmap/scripts#
```

Getting information from SNMP

> Commonly misconfigured service by admins

> Great source of various information about your targets

  > Default public string; non-encrypted versions, open ports on fw

  > Tools in kali: SNMPenum, SNMPcheck, onesixtyone

  > You get a lot of info by sending just one packet!

```
root@kali-vbox:/usr/share/nmap/scripts# snmpcheck -t 192.168.99.11
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

 [*] Try to connect to 192.168.99.11
 [*] Connected to 192.168.99.11
 [*] Starting enumeration at 2014-11-30 13:13:29

 [*] System information
 -----------------------------------------------------------------------------------------

 Hostname               : DiskStation
 Description            : Linux DiskStation 2.6.32.12 #5004 Sat Nov 29 01:34:57 CST 2014 armv5tel
 Uptime system          : 22 hours, 47:50.92
 Uptime SNMP daemon     : 22 hours, 46:28.90
 Contact                : admin@diskstation
 Location               : Unknown
 Motd                   : -

 [*] Devices information
 -----------------------------------------------------------------------------------------

    Id                Type   Status  Description

  1025             Network  Running  network interface lo
  1026             Network  Running  network interface eth0
  1027             Network     Down  network interface sit0
  1028             Network  Running  network interface tun0
  1536        Disk Storage  Unknown  WDC WD20EARS-00MVWB0
  1552        Disk Storage  Unknown  SCSI disk (/dev/sda)
  1553        Disk Storage  Unknown  SCSI disk (/dev/sdb)
  1568        Disk Storage  Unknown  RAID disk (/dev/md0)
  1569        Disk Storage  Unknown  RAID disk (/dev/md1)
  1570        Disk Storage  Unknown  RAID disk (/dev/md2)
  3072         Coprocessor  Unknown  Guessing that there's a floating point co-processor
   768           Processor  Unknown

 [*] Storage information
 -----------------------------------------------------------------------------------------
```

```
[*] Processes
--------------------------------------------------------------------------------------------

Total processes : 80

Process type    : 1 unknown, 2 operating system, 3 device driver, 4 application
Process status  : 1 running, 2 runnable, 3 not runnable, 4 invalid

Process id             Process name  Process type  Process status  Process path

         1                     init             4               2  /sbin/init
      1004                synoconfd             4               2  /usr/syno/sbin/synoconfd
     10146             photostationd             4               2  /usr/syno/bin/photostationd
     10209                      dms             4               2  /var/packages/MediaServer/target/sbin/dms
      1023              synologarchd             4               2  /usr/syno/sbin/synologarchd
     10235                  lighttpd             4               2  /var/packages/MediaServer/target/sbin/lighttpd
      1033                     udevd             4               2  udevd
      1043                  synonetd             4               2  /usr/syno/sbin/synonetd
     10444                mysqld_safe             4               2  /bin/sh
     10758                     mysqld             4               2  /usr/bin/mysqld
     11026                    php-fpm             4               2  php-fpm: master process (/etc/php/php-fpm.conf)
     11042                      nginx             4               2  nginx: master process /usr/bin/nginx -g pid /run/nginx.pi
d; daemon on; master_process on;
     11043                      nginx             4               2  nginx: worker process
     11045                    php-fpm             4               2  php-fpm: pool www
     11046                    php-fpm             4               2  php-fpm: pool www
     11063                      httpd             4               2  /usr/bin/httpd
     11066                      httpd             4               2  /usr/bin/httpd
     11067                      httpd             4               2  /usr/bin/fcgi-
     11178                      httpd             4               2  /usr/bin/httpd
     11260                      httpd             4               2  /usr/bin/httpd
     11297                      httpd             4               2  /usr/bin/httpd
     11349          synoindexworker             4               2  /usr/syno/sbin/synoindexworkerd
     11350          synoindexplugin             4               2  /usr/syno/sbin/synoindexplugind
     11351          synomediaparser             4               2  /usr/syno/sbin/synomediaparserd
     11361                 postgres             4               2  postgres: postgres mediaserver [local] idle
     11366                 postgres             4               2  postgres: postgres photo [local] idle
     11367           synoindexscand             4               2  /usr/syno/sbin/synoindexscand
      2784           synologrotated             4               2  /usr/syno/bin/synologrotated
      3556                findhostd             4               2  /usr/syno/bin/findhostd
      3581                    ntpd             4               2  /usr/sbin/ntpd
      3733          SYNO.Core.Secur             4               2  entry.cgi_SYNO.Core.Security.Firewall.Rules[1].save_start
      3738           S01iptables.sh             4               2  /bin/sh
      3754          SYNO.Core.Exter             4               1  entry.cgi_SYNO.Core.ExternalDevice.Storage.USB[1].list
      3776             iptablestool             4               1  /usr/syno/bin/iptablestool
      3782                    httpd             4               2  /usr/bin/httpd
      3918                     sshd             4               2  /usr/bin/sshd
      5185             synostoraged             4               2  /usr/syno/sbin/synostoraged
      5209                    scemd             4               2  scemd
      5579                hotplugd              4               2  /usr/syno/sbin/hotplugd
      5612                   getty              4               2  /sbin/getty
      6416                   inetd              4               2  /usr/sbin/inetd
      6602                    nmbd              4               2  /usr/bin/nmbd
```

```
[*] Routing information
-------------------------------------------------------------------------------------------

     Destination         Next Hop             Mask     Metric

         0.0.0.0     192.168.99.1          0.0.0.0        1
        10.0.0.0         10.0.0.2    255.255.255.0        1
        10.0.0.2          0.0.0.0  255.255.255.255        -

[*] Listening TCP ports and connections
-------------------------------------------------------------------------------------------

  Local Address   Port      Remote Address   Port       State

        0.0.0.0    139            0.0.0.0      -       Listening
        0.0.0.0    161            0.0.0.0      -       Listening
        0.0.0.0     21            0.0.0.0      -       Listening
        0.0.0.0     22            0.0.0.0      -       Listening
        0.0.0.0   3306            0.0.0.0      -       Listening
        0.0.0.0    445            0.0.0.0      -       Listening
        0.0.0.0  49170            0.0.0.0      -       Listening
        0.0.0.0  50001            0.0.0.0      -       Listening
        0.0.0.0  50002            0.0.0.0      -       Listening
        0.0.0.0    514            0.0.0.0      -       Listening
        0.0.0.0   6690            0.0.0.0      -       Listening
      127.0.0.1   1195            0.0.0.0      -       Listening
      127.0.0.1    412            0.0.0.0      -       Listening
      127.0.0.1   5432            0.0.0.0      -       Listening
  192.168.99.11  37960       192.168.99.11    514     Established
  192.168.99.11    514       192.168.99.11  37960     Established
  192.168.99.11   6690        192.168.99.1  50050     Established
  192.168.99.11   6690        192.168.99.1  51223     Established
  192.168.99.11   6690        192.168.99.1  55239     Established
  192.168.99.11   6690        192.168.99.1  61231     Established
```

Metasploit – Swiss army knife for pentesting

> Previous manual work done effectively from one framework

> Great source of various information about your targets

> Results of your activities are stored in a database

> All configured (db, msf, web server) in Kali Linux


root@kali-vbox:~# msfconsole
[*] Starting the Metasploit Framework console...-
METASPLOIT CYBER MISSILE COMMAND V
WAVE 4 ######## SCORE 31337 ################################ HIGH FFFFFFFF
http://metasploit.pro
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.10.2-2014111901 [core:4.10.2.pre.2014111901 api:1.0.0]]
+ -- --=[1379 exploits - 850 auxiliary - 233 post]
+ -- --=[340 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >
auxiliary/scanner/snmp/ubee_ddw3611 normal Ubee DDW3611b Cable Modem
auxiliary/scanner/snmp/xerox_workcentre_enumusers normal Xerox WorkCentre User Enu
auxiliary/scanner/ssh/cerberus_sftp_enumusers 2014-05-27 normal Cerberus FTP Server SFTP
auxiliary/scanner/ssh/ssh_enumusers normal SSH Username Enumeration
auxiliary/scanner/ssh/ssh_identify_pubkeys normal SSH Public Key Acceptance
auxiliary/scanner/ssh/ssh_login normal SSH Login Check Scanner
auxiliary/scanner/ssh/ssh_login_pubkey normal SSH Public Key Login Scan
auxiliary/scanner/ssh/ssh_version normal SSH Version Scanner
auxiliary/scanner/ssl/openssl_ccs 2014-06-05 normal OpenSSL Server-Side Chang
auxiliary/scanner/ssl/openssl_heartbleed 2014-04-07 normal OpenSSL Heartbeat (Heartb
auxiliary/scanner/telephony/wardial normal Wardialer
auxiliary/scanner/telnet/lantronix_telnet_password normal Lantronix Telnet Password
auxiliary/scanner/telnet/lantronix_telnet_version normal Lantronix Telnet Service
auxiliary/scanner/telnet/telnet_encrypt_overflow normal Telnet Service Encyption
auxiliary/scanner/telnet/telnet_login normal Telnet Login Check Scanne
auxiliary/scanner/telnet/telnet_ruggedcom normal RuggedCom Telnet Password
auxiliary/scanner/telnet/telnet_version normal Telnet Service Banner Det
auxiliary/scanner/tftp/ipswitch_whatsupgold_tftp 2011-12-12 normal IpSwitch WhatsUp Gold TFT
auxiliary/scanner/tftp/netdecision_tftp 2009-05-16 normal NetDecision 4.2 TFTP Dire
auxiliary/scanner/tftp/tftpbrute normal TFTP Brute Forcer
auxiliary/scanner/udp_scanner_template 2014-03-15 normal UDP Scanner Example
auxiliary/scanner/upnp/ssdp_amp normal SSDP ssdp:all M-SEARCH Am
auxiliary/scanner/upnp/ssdp_msearch normal UPnP SSDP M-SEARCH Inform
auxiliary/scanner/vmware/esx_fingerprint
auxiliary/scanner/vmware/vmauthd_login
msf > workspace
* default
home
msf > hosts
Hosts
address mac name os_name os_flavor os_sp purpose
37.187.134.197
67.18.187.172
176.9.123.43
204.77.3.50
msf > services
Services
host port proto name state info
37.187.134.197 443 tcp
67.18.187.172 443 tcp
176.9.123.43 443 tcp
204.77.3.50 443 tcp

Metasploit – Swiss army knife for pentesting

> Workspaces for storing different project in msf

> Metasploit can import result from nmap

  > Or you can run nmap directly from Metasploit!

  > db_nmap with options you would use with standard nmap

> Metasploit prompt accepts standard Linux commands

```
msf > db_nmap -A 192.168.99.11
[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-08 15:54 EST
[*] Nmap: Nmap scan report for 192.168.99.11
[*] Nmap: Host is up (0.00082s latency).
[*] Nmap: Not shown: 993 filtered ports
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         Synology DiskStation NAS ftpd
[*] Nmap: | ssl-cert: Subject: commonName=h          ost r      et/organizationName=Home/stateOrProvinceName=CZ/countryName=CZ
[*] Nmap: | Not valid before: 2014-04-19T13:20:35+00:00
[*] Nmap: |_Not valid after:  2024-04-16T13:20:35+00:00
[*] Nmap: |_ssl-date: 2088-01-23T02:54:38+00:00; +73y45d5h59m35s from local time.
[*] Nmap: 22/tcp   open  ssh         OpenSSH 6.6p2-hpn14v4 (protocol 2.0)
[*] Nmap: |_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
[*] Nmap: 80/tcp   open  http        Apache httpd
[*] Nmap: |_http-generator: ERROR: Script execution failed (use -d to debug)
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 302)
[*] Nmap: |_http-title: Did not follow redirect to http://192.168.99.11:5000/
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: MSHOME)
[*] Nmap: 443/tcp  open  ssl/http    Apache httpd
[*] Nmap: |_http-generator: ERROR: Script execution failed (use -d to debug)
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 302)
[*] Nmap: |_http-title: Did not follow redirect to https://192.168.99.11:5001/
[*] Nmap: | ssl-cert: Subject: commonName=h          ost r      t/organizationName=Home/stateOrProvinceName=CZ/countryName=CZ
[*] Nmap: | Not valid before: 2014-04-19T13:20:35+00:00
[*] Nmap: |_Not valid after:  2024-04-16T13:20:35+00:00
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: MSHOME)
[*] Nmap: 5001/tcp open  ssl/http    Apache httpd
[*] Nmap: |_http-generator: ERROR: Script execution failed (use -d to debug)
[*] Nmap: |_http-methods: No Allow or Public header in OPTIONS response (status code 301)
[*] Nmap: | http-robots.txt: 1 disallowed entry
[*] Nmap: |_/
[*] Nmap: |_http-title: Did not follow redirect to https://192.168.99.11/webman/index.cgi
[*] Nmap: | ssl-cert: Subject: commonName=h          ost r      t/organizationName=Home/stateOrProvinceName=CZ/countryName=CZ
[*] Nmap: | Not valid before: 2014-04-19T13:20:35+00:00
[*] Nmap: |_Not valid after:  2024-04-16T13:20:35+00:00
[*] Nmap: MAC Address: 00:11:32:0B:A0:B4 (Synology Incorporated)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: storage-misc|general purpose
[*] Nmap: Running: LaCie Linux 2.6.X, Linux 2.6.X
```

```
msf > vulns
[*] Time: 2014-10-23 11:01:06 UTC Vuln: host=37.187.134.197 name=OpenSSL Heartbeat (Heartbleed) Information Leak refs=CVE-2014-0160,US-CERT-VU-720951,URL-https://www.us-
ert.gov/ncas/alerts/TA14-098A,URL-http://heartbleed.com/,URL-https://github.com/FiloSottile/Heartbleed,URL-https://gist.github.com/takeshixx/10107280,URL-http://filippo.
o/Heartbleed/
[*] Time: 2014-10-23 11:22:27 UTC Vuln: host=67.18.187.172 name=OpenSSL Server-Side ChangeCipherSpec Injection Scanner refs=CVE-2014-0224,URL-http://ccsinjection.lepidum
co.jp/,URL-http://ccsinjection.lepidum.co.jp/blog/2014-06-05/CCS-Injection-en/index.html,URL-http://www.tripwire.com/state-of-security/incident-detection/detection-scrip
-for-cve-2014-0224-openssl-cipher-change-spec-injection/,URL-https://www.imperialviolet.org/2014/06/05/earlyccs.html
[*] Time: 2014-11-16 17:40:44 UTC Vuln: host=176.9.123.43 name=OpenSSL Heartbeat (Heartbleed) Information Leak refs=CVE-2014-0160,US-CERT-VU-720951,URL-https://www.us-ce
t.gov/ncas/alerts/TA14-098A,URL-http://heartbleed.com/,URL-https://github.com/FiloSottile/Heartbleed,URL-https://gist.github.com/takeshixx/10107280,URL-http://filippo.io
Heartbleed/
[*] Time: 2014-10-23 11:03:42 UTC Vuln: host=204.77.3.50 name=OpenSSL Heartbeat (Heartbleed) Information Leak refs=CVE-2014-0160,US-CERT-VU-720951,URL-https://www.us-cer
.gov/ncas/alerts/TA14-098A,URL-http://heartbleed.com/,URL-https://github.com/FiloSottile/Heartbleed,URL-https://gist.github.com/takeshixx/10107280,URL-http://filippo.io/
eartbleed/
```

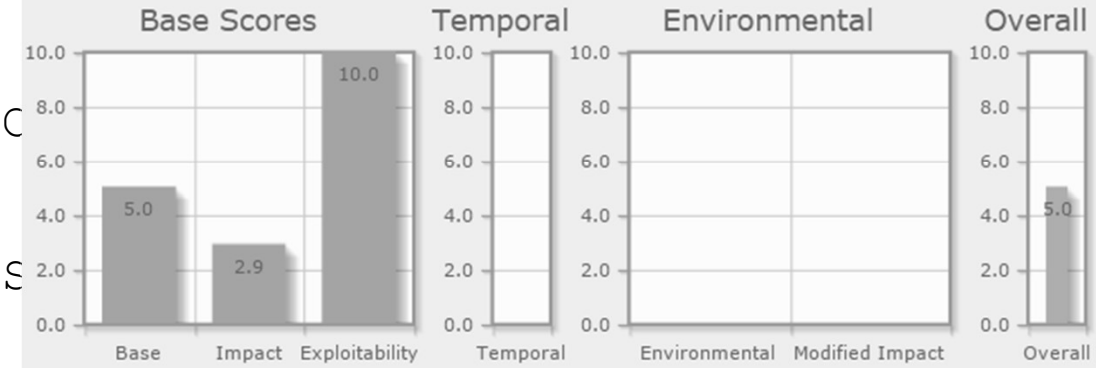
```
msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > show options

Module options (auxiliary/scanner/ssl/openssl_heartbleed):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   DUMPFILTER                         no        Pattern to filter leaked memory before storing
   MAX_KEYTRIES      50               yes       Max tries to dump key
   RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server response
   RHOSTS            192.168.99.11    yes       The target address range or CIDR identifier
   RPORT             5001             yes       The target port
   STATUS_EVERY      5                yes       How many retries until status
   THREADS           1                yes       The number of concurrent threads
   TLS_CALLBACK      None             yes       Protocol to use, "None" to use raw TLS sockets (accepted: None, SMTP, IMAP,
   TLS_VERSION       1.0              yes       TLS/SSL version to use (accepted: SSLv3, 1.0, 1.1, 1.2)


Auxiliary action:

   Name  Description
   ----  -----------
   SCAN  Check hosts for vulnerability


msf auxiliary(openssl_heartbleed) > set RHOSTS 192.168.99.11
RHOSTS => 192.168.99.11
msf auxiliary(openssl_heartbleed) > set RPORT 5001
RPORT => 5001
msf auxiliary(openssl_heartbleed) > set ACTION
set ACTION DUMP  set ACTION KEYS  set ACTION SCAN
msf auxiliary(openssl_heartbleed) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) >
```

```
msf > info auxiliary/scanner/ssl/openssl_heartbleed

       Name: OpenSSL Heartbeat (Heartbleed) Information Leak
     Module: auxiliary/scanner/ssl/openssl_heartbleed
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2014-04-07

Provided by:
  Neel Mehta
  Riku
  Antti
  Matti
  Jared Stafford <jspenguin@jspenguin.org>
  FiloSottile
  Christian Mehlmauer <FireFart@gmail.com>
  wvu <wvu@metasploit.com>
  juan vazquez <juan.vazquez@metasploit.com>
  Sebastiano Di Paola
  Tom Sellers
  jjarmoc
  Ben Buchanan
  herself

Available actions:
  Name  Description
  ----  -----------
  DUMP  Dump memory contents
  KEYS  Recover private keys from memory
  SCAN  Check hosts for vulnerability

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  DUMPFILTER                         no        Pattern to filter leaked memory before storing
  MAX_KEYTRIES      50               yes       Max tries to dump key
  RESPONSE_TIMEOUT  10               yes       Number of seconds to wait for a server response
  RHOSTS                             yes       The target address range or CIDR identifier
  RPORT             443              yes       The target port
  STATUS_EVERY      5                yes       How many retries until status
  THREADS           1                yes       The number of concurrent threads
  TLS_CALLBACK      None             yes       Protocol to use, "None" to use raw TLS sockets (accepted: None, SMTP, IMAP, JABBER, P
OP3, FTP, POSTGRES)
  TLS_VERSION       1.0              yes       TLS/SSL version to use (accepted: SSLv3, 1.0, 1.1, 1.2)

Description:
  This module implements the OpenSSL Heartbleed attack. The problem
  exists in the handling of heartbeat requests, where a fake length
  can be used to leak memory data in the response. Services that
  support STARTTLS may also be vulnerable. The module supports several
```

CV

Common Vulnerability Scoring System Version 2 Calculator - CVE-2014-0160

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to
are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmer



CVSS Base Score	**5**
Impact Subscore	2.9
Exploitability Subscore	10
CVSS Temporal Score	**Not Defined**
CVSS Environmental Score	**Not Defined**
Modified Impact Subscore	Not Defined
Overall CVSS Score	**5**

Show Equations

CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:N/A:N)

> C

> S

> H

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L) | **Adjacent Network (AV:A)** | **Network (AV:N)**

Access Complexity (AC)*

High (AC:H) | **Medium (AC:M)** | **Low (AC:L)**

Authentication (Au)*

Multiple (Au:M) | **Single (Au:S)** | **None (Au:N)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | **Partial (C:P)** | **Complete (C:C)**

Integrity Impact (I)*

None (I:N) | **Partial (I:P)** | **Complete (I:C)**

Availability Impact (A)*

None (A:N) | **Partial (A:P)** | **Complete (A:C)**

* - All base metrics are required to generate a base score.

```
auxiliary/scanner/ssl/openssl_heartbleed          2014-04-07       normal  OpenSSL Heartbeat (Heartbleed) Information Leak
auxiliary/server/openssl_heartbeat_client_memory  2014-04-07       normal  OpenSSL Heartbeat (Heartbleed) Client Memory Exposure
```

Pentest reporting – general guidelines

> Scope of the pentest (what/when/why/how/who)

  > What is scanned, what is the goal, what is excluded, ...

> For each discovered vulnerability

  > Discuss risk, impact, attacker’s skill, affected hosts

  > Provide description/evidence, recommendation and references

Useful pointers

> OWASP testing guide

- https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

> OWASP reporting guide

- https://www.owasp.org/index.php/Reporting

- Certified Ethical Hacker (CEH) certification

Questions?

Thx…