

Audit de Sécurité Technique

Chapter 2.4 Toolbox

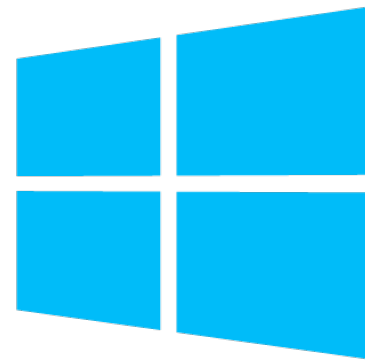
Jean-Marc Bost

jean-marc.bost@heig-vd.ch

Set of tools for technical security assessments

- What do you use?

- Windows
- Linux
- OS X



Linux



- Recommendation is to have all three of them, or at least Windows and Linux
 - Don't think of them as different operating systems
 - Thinks of them as set of tools
- Setup a virtualized environment on you machine (VMWare)
 - Deploy images of Windows and Linux boxes so that you can easily switch between
- Today's average Portable PC (quad-core)
 - Can easily run several OS in parallel
 - Images allow easily to backup, roll-back and deploy a fresh/clean version of the OS

Testing platform

- The Kali linux distribution which superseded historical BackTrack (BT) linux is seen as a de-facto standard platform to help you with your pentest tasks
 - Debian-based distribution
 - More than 300 tools for pentest and data forensics
 - Active online support community
 - Easy to install and start using



If you are an Arch Linux fan, you might want to give BlackArch a try

- Download from www.kali.org
 - Either an ISO from <http://www.kali.org/downloads/>
 - VMWare image from <http://www.offensive-security.com/kali-linux-vmware-arm-image-download/>
 - Download, unzip (7z x Kali-Linux-2019.3-vm-amd64.7z) and open the image in VMPlayer
 - default username and password: root/toor
 - remember to change the root password
 - `apt-get update && apt-get upgrade`
- In normal circumstances if running a WMPPlayer, ensure that you are using **Bridged network** option for your virtual network adapter
 - If you are on HEIG-VD WLAN — use NAT !

Non-root user

- When installed, Kali linux uses root user for all tasks
- It is a good security practice to add an additional user with non-root privileges
 - `useradd -m noroot`
`passwd noroot`
`usermod -a -G sudo noroot`
`chsh -s /bin/bash noroot`
 - Replace the `noroot` by whatever you prefer

Install MultiArchitecture support

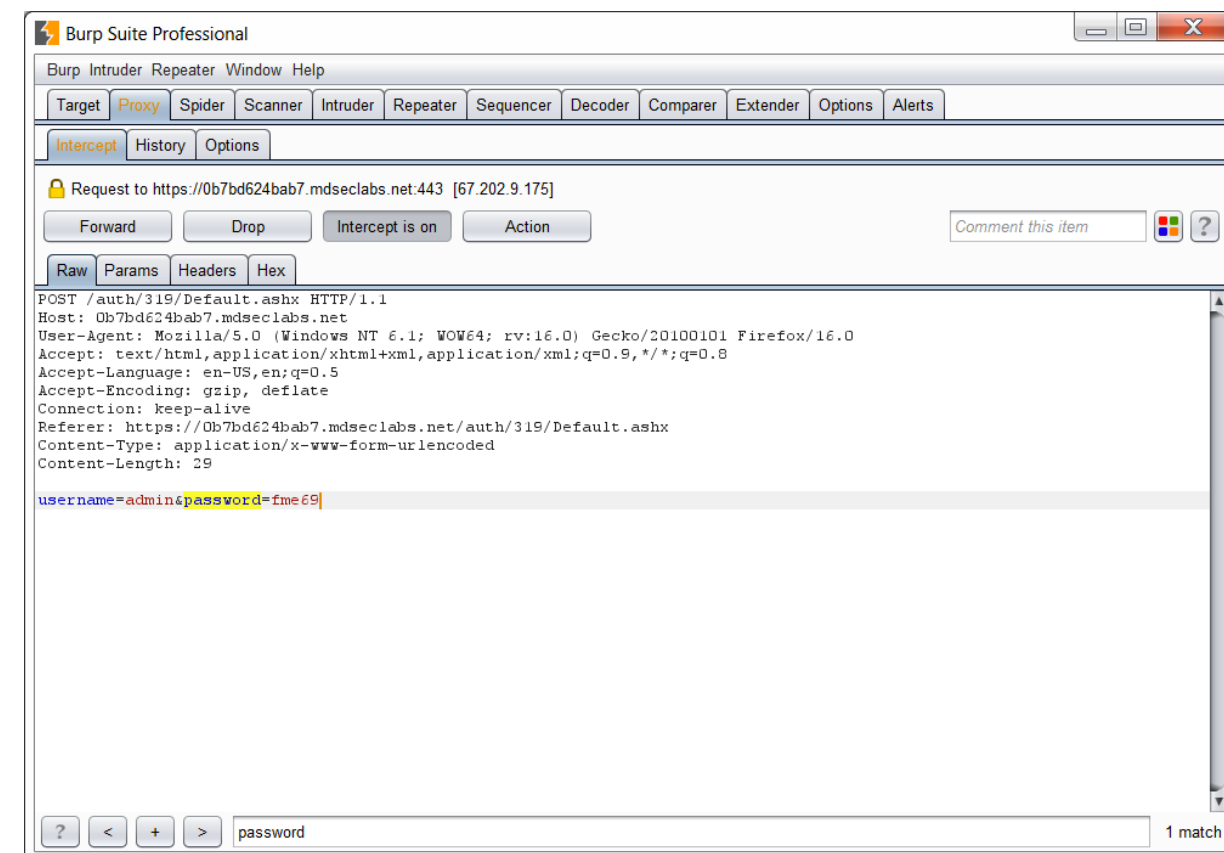
- By default Kali comes with 64 bit architecture
 - `sudo dpkg --add-architecture i386`
`sudo apt-get update`
`sudo apt-get upgrade`
 - Enables 32-bit support
 - Useful for applications supporting only 32-bit

Default repositories

- The default package repositories that should be present in `/etc/apt/sources.list` are listed as follows; if not present, edit the `sources.list` file to include them
 - `deb http://http.kali.org/kali kali-rolling main non-free contrib`

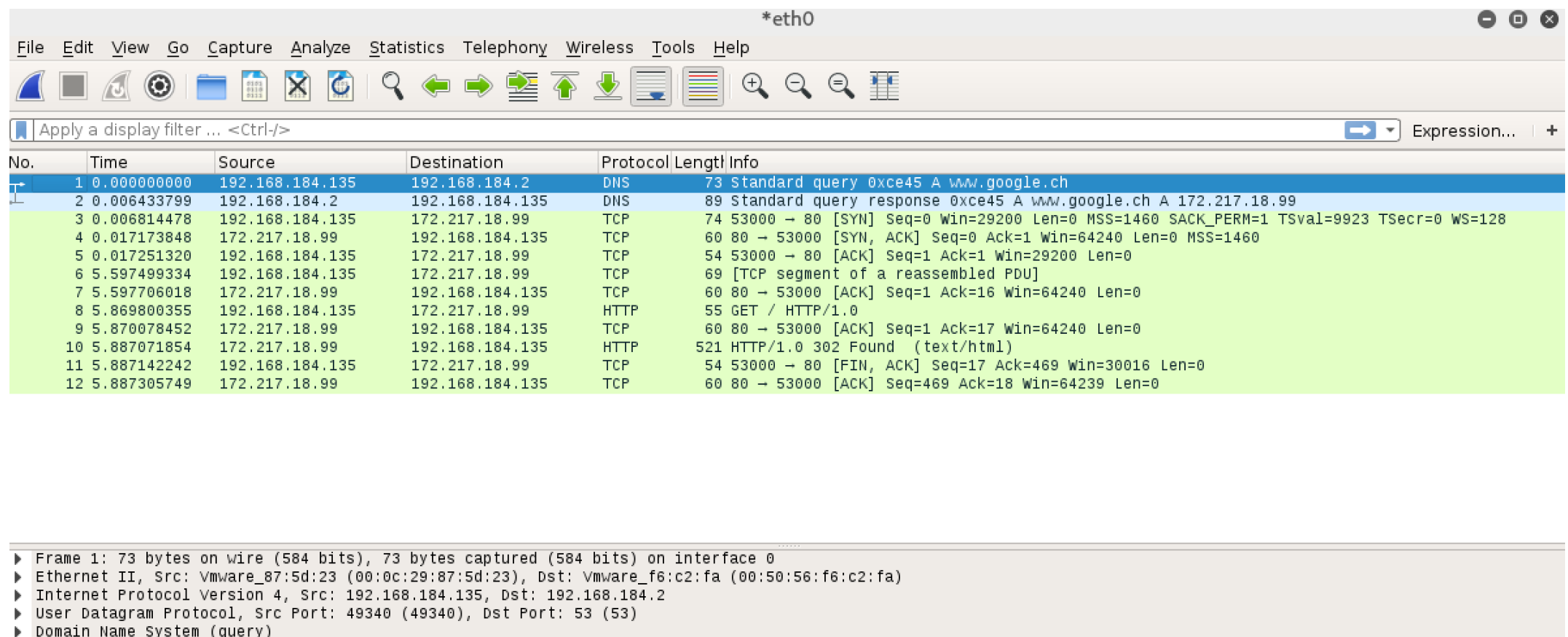
Burp Suite

- The most well-known toolbox for web hacking
- Comprises:
 - Proxy - intercept and modify requests
 - Spider - discover content
 - Scanner - vulnerabilities scanner
 - Intruder/repeater - attack tools
 - ...
- Free version available in Kali



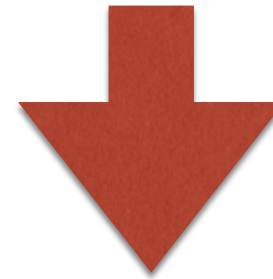
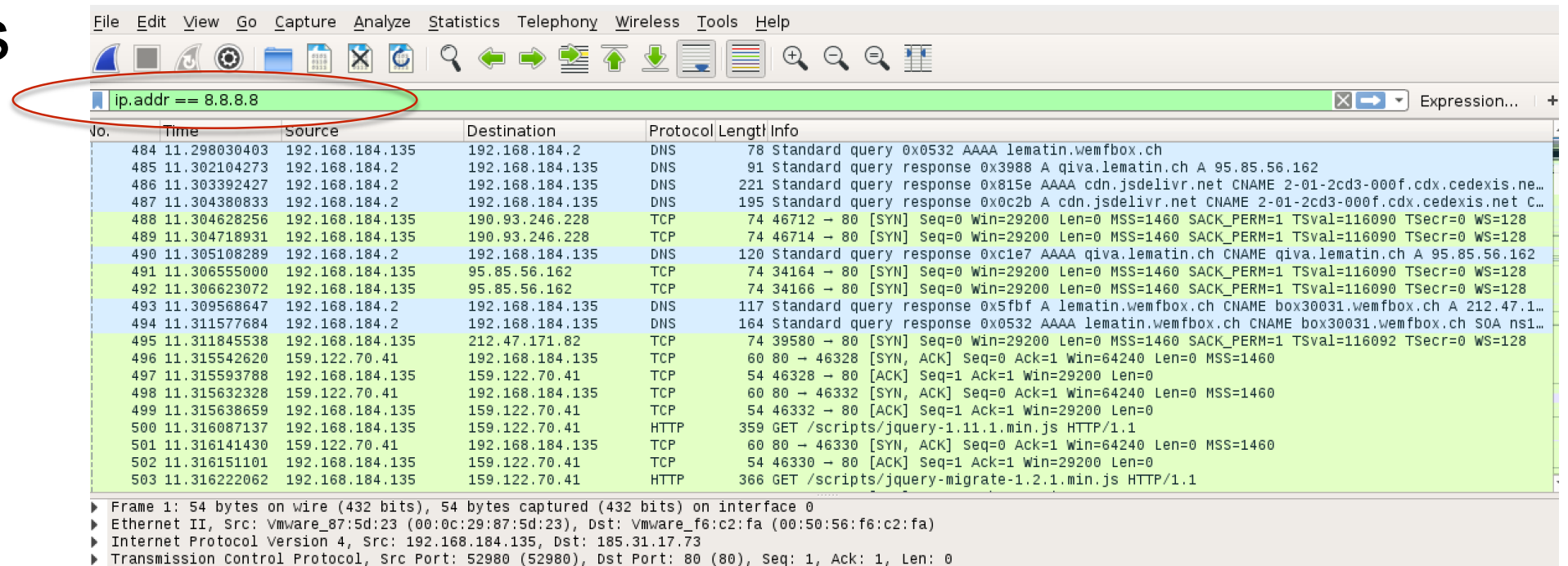
Wireshark

- The ultimate packet sniffer
 - Understanding/reverse engineering of protocols
 - Network debugging
 - Traffic analysis



Wireshark

- Capture filters
- Display filters



ip.addr == 8.8.8.8						
No.	Time	Source	Destination	Protocol	Length	Info
5284	18.780566823	192.168.184.135	8.8.8.8	ICMP	98	Echo (ping) request id=0x071d, seq=1/256, ttl=64 (reply in 5285)
5285	18.797334407	8.8.8.8	192.168.184.135	ICMP	98	Echo (ping) reply id=0x071d, seq=1/256, ttl=128 (request in 5284)
5325	19.782063285	192.168.184.135	8.8.8.8	ICMP	98	Echo (ping) request id=0x071d, seq=2/512, ttl=64 (reply in 5326)
5326	19.795635647	8.8.8.8	192.168.184.135	ICMP	98	Echo (ping) reply id=0x071d, seq=2/512, ttl=128 (request in 5325)
5376	20.783232524	192.168.184.135	8.8.8.8	ICMP	98	Echo (ping) request id=0x071d, seq=3/768, ttl=64 (reply in 5377)
5377	20.800344972	8.8.8.8	192.168.184.135	ICMP	98	Echo (ping) reply id=0x071d, seq=3/768, ttl=128 (request in 5376)
5421	21.784930698	192.168.184.135	8.8.8.8	ICMP	98	Echo (ping) request id=0x071d, seq=4/1024, ttl=64 (reply in 5422)
5422	21.798599708	8.8.8.8	192.168.184.135	ICMP	98	Echo (ping) reply id=0x071d, seq=4/1024, ttl=128 (request in 5421)
5462	22.786781076	192.168.184.135	8.8.8.8	ICMP	98	Echo (ping) request id=0x071d, seq=5/1280, ttl=64 (reply in 5463)
5463	22.801712675	8.8.8.8	192.168.184.135	ICMP	98	Echo (ping) reply id=0x071d, seq=5/1280, ttl=128 (request in 5462)

Wireshark

- Reconstructing streams

Applications ▾ Places ▾ Wireshark ▾ Wed 19:49

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
64	1.239102908	192.168.184.2	192.168.184.135	DNS	104	Standard query response 0xe12d A www.lematin.ch CNAME lematin.ch A 151.252.10.126
65	1.239394090	192.168.184.2	192.168.184.135	DNS	151	Standard query response 0x9c1f AAAA www.lematin.ch CNAME lematin.ch SOA ns1.netnames.net
66	1.278575963	151.252.10.126	192.168.184.135	TCP	60	80 → 55034 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
67	1.278618892	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
68	1.278928771	192.168.184.135	151.252.10.126	HTTP	976	GET / HTTP/1.1
69	1.279762885	151.252.10.126	192.168.184.135	TCP	60	80 → 55034 [ACK] Seq=1 Ack=923 Win=64240 Len=0
70	1.333576012	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
71	1.333606153	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=1449 Win=64240 Len=0
72	1.333671670	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
73	1.333679635	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=2897 Win=64240 Len=0
74	1.334100191	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
75	1.334109516	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=4345 Win=64240 Len=0
76	1.334386563	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
77	1.334413178	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=5793 Win=64240 Len=0
78	1.334767094	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
79	1.334793455	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=7241 Win=64240 Len=0
80	1.335185254	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
81	1.335195768	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=8689 Win=64240 Len=0
82	1.335532477	151.252.10.126	192.168.184.135	TCP	1502	[TCP segment of a reassembled PDU]
83	1.335542091	192.168.184.135	151.252.10.126	TCP	54	55034 → 80 [ACK] Seq=923 Ack=10137 Win=64240 Len=0

▶ Frame 68: 976 bytes on wire (7808 bits), 976 bytes captured (7808 bits) on interface 0

▶ Ethernet II, Src: Vmware_87:5d:23 (00:0c:29:87:5d:23), Dst: Vmware_f8:c2:fa (00:50:56:f8:c2:fa)

▶ Internet Protocol Version 4, Src: 192.168.184.135, Dst: 151.252.10.126

▶ Transmission Control Protocol, Src Port: 55034 (55034), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 922

▶ Hypertext Transfer Protocol

0000 00 50 56 f6 c2 fa 00 0c 29 87 5d 23 08 00 45 00 .PV....).]#..E.
0010 03 c2 5a f3 40 00 40 06 c0 98 c0 a8 b8 87 97 fc ..Z.@.
0020 0a 7e d6 fa 00 50 3f 6d f3 99 04 c5 16 a8 50 18PmP.

Wireshark - Follow TCP Stream (tcp.stream eq 18) - wireshark_pcapng_eth0_20160224194714_ed...

GET / HTTP/1.1
Host: www.lematin.ch
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:44.0) Gecko/20100101 Firefox/44.0 Iceweasel/44.0.2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: dtCookie=7169012F45091F08148BA3B0471C0150|RUN*Default+Application|1; __utma=35014588.459127341.1456360218.1456360218.1456360218.1; __utmb=35014588.2.10.1456360218; __utmc=35014588; __utmz=35014588.1456360218.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none); __utma=1.1911448580.1456360218.1456360218.1456360218.1; __utmb=1.2.10.1456360218; __utmc=1; __utmz=1.1456360218.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none); POPUPCHECK=1456446618461; ga=GA1.2.459127341.1456360218; _trouID=884c6f09-b10f-4a53-86fc-ccd6123e2ebc; __trouSYNC=1; _lo_no_track=1; _gat_UA-58327930-7=1; _gat=1
Connection: keep-alive
Cache-Control: max-age=0

HTTP/1.1 200 OK
Server: Apache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
X-Host-Backend: app10
Content-Encoding: gzip
Content-Length: 12599
Accept-Ranges: bytes
Date: Thu, 25 Feb 2016 00:47:16 GMT
X-Varnish: 2004431861 2004431589
Age: 6
Via: 1.1 varnish
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-Mx-ReqToken,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type
X-Varnish-Cache: HIT
X-Host-Varnish: proxy06

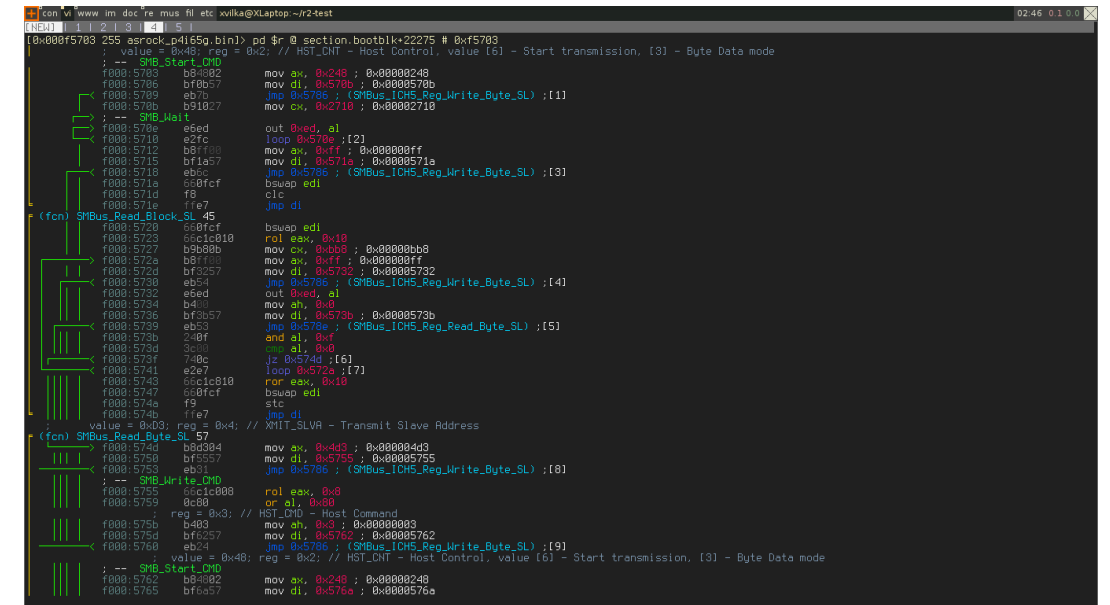
Last but not least

- Netcat
 - Hacker's Swiss Army Knife
 - Read and write tcp ports
 - Transferring files, remote administration, reverse shells,...
- Tcpdump
 - Command-line packet capture and analyser
 - When GUI is not available
 - Fast
 - To capture for further analysis with Wireshark:

```
$ tcpdump -i <interface> -s 65535 -w <some-file>
```

Binary reverse engineering

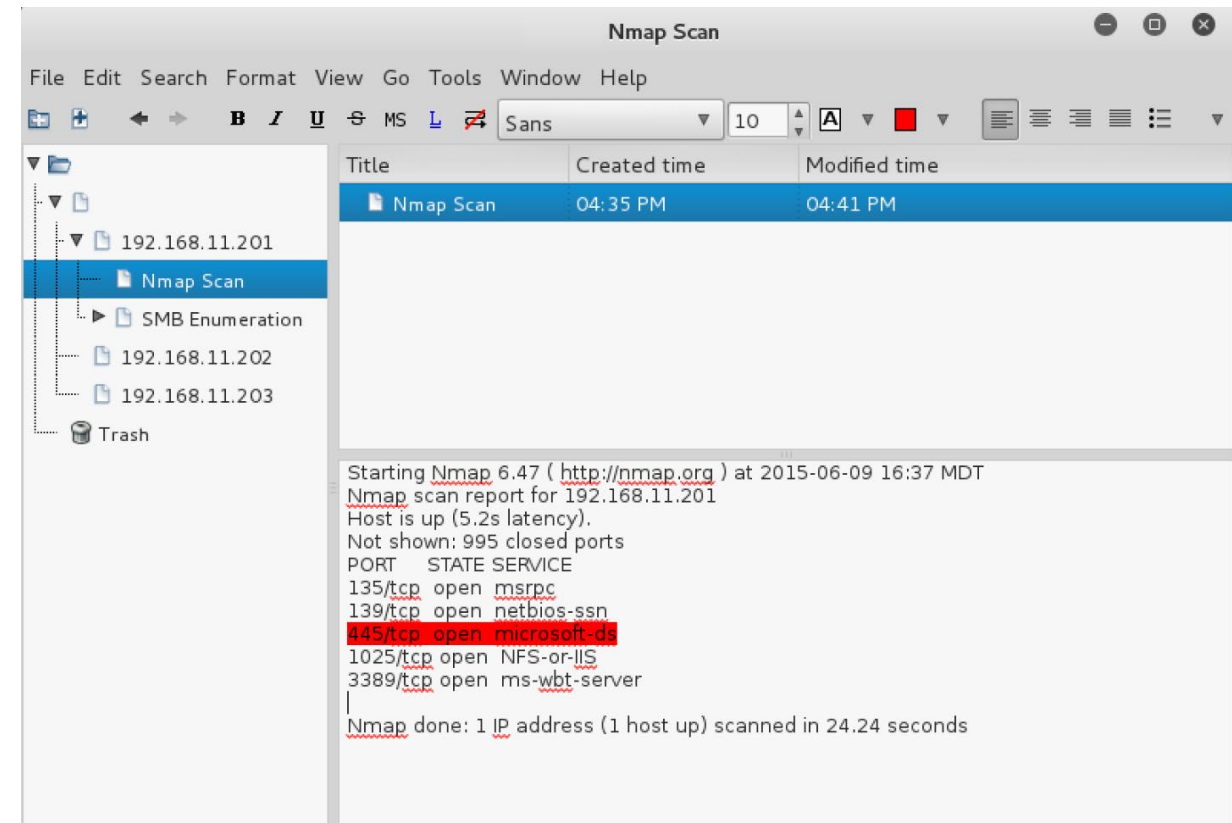
- IDA Pro - Fully Featured Disassembler
 - The weapon of choice when it comes to reverse engineer (any) binary
 - Quite expensive
 - Demo/free old version officially available from https://www.hex-rays.com/products/ida/support/download_freeware.shtml
- Ghidra
 - <https://ghidra-sre.org>
 - Developed by the NSA (Java/Swing)
 - Free, open source
- Radare2 is a free alternative
 - <https://www.radare.org>
 - Included in Kali



```
[0x000f5703] 255 asrock_p4155g.bin> pd $r @ section.bootblk+22275 # 0xf5703
; value = 0x48; reg = 0x2; // HST_CNT - Host Control, value {6} - Start transmission, {3} - Byte Data mode
; -- SMB_Start_CMD
r000:5705 b80002 mov ax, 0x248 ; 0x00000248
r000:5706 bf0057 mov di, 0x570b ; 0x0000570b
r000:5709 eb7b jmp 0x5706 ; (SMB_I2C5_Reg_Write_Byte_SL) ;{1}
r000:570b b91027 mov cx, 0x2710 ; 0x00002710
; -- SMB_Halt
r000:570e e6ed out 0xed, al
r000:5710 e2c5 loop 0x5706 ;{2}
r000:5712 b81f00 mov ax, 0xff ; 0x000000ff
r000:5715 bf1a57 mov di, 0x571a ; 0x0000571a
r000:5718 ebc5 jmp 0x5706 ; (SMB_I2C5_Reg_Write_Byte_SL) ;{3}
r000:571a 66fcaf bswap edi
r000:571d f8 cll
r000:571e ffe7 jmp di
; (fcn) SMBus_Read_Block_SL_45
r000:5720 66fcaf bswap edi
r000:5723 66c1010 rol eax, 0x10
r000:5727 b9000b mov cx, 0xb0b ; 0x00000bb0
r000:572a b81f00 mov ax, 0xff ; 0x000000ff
r000:572d bf5257 mov di, 0x572e ; 0x0000572e
r000:5730 ebc4 jmp 0x5706 ; (SMB_I2C5_Reg_Write_Byte_SL) ;{4}
r000:5732 e6ed out 0xed, al
r000:5734 b4 mov ah, 0
r000:5736 bf5b57 jmp 0x5706 ; 0x0000573b
r000:5739 ebc3 jmp 0x5706 ; (SMB_I2C5_Reg_Read_Byte_SL) ;{5}
r000:573b 24bf and al, 0xf
r000:573d 90 al, 0
r000:573f 740c jz 0x574d ;{6}
r000:5741 e2e7 loop 0x572a ;{7}
r000:5745 66c1010 rol eax, 0x10
r000:5747 66fcaf bswap edi
r000:574a f8 stc
r000:574b ffe7 jmp di
; value = 0x03; reg = 0x4; // XMIT_SLAVE - Transmit Slave Address
; (fcn) SMBus_Read_Byte_SL_57
r000:574d b80004 mov ax, 0x4d3 ; 0x000004d3
r000:5750 bf5257 mov di, 0x5755 ; 0x00005755
r000:5753 ebc1 jmp 0x5706 ; (SMB_I2C5_Reg_Write_Byte_SL) ;{8}
; -- SMB_Write_CMD
r000:5755 c1c1008 rol eax, 0x8
r000:5759 0c00 or al, 0x0
; reg = 0x3; // HST_CMD - Host Command
r000:575b b403 mov ah, 0x3 ; 0x00000003
r000:575d bf5257 mov di, 0x5762 ; 0x00005762
r000:5760 ebc4 jmp 0x5706 ; (SMB_I2C5_Reg_Write_Byte_SL) ;{9}
; value = 0x48; reg = 0x2; // HST_CNT - Host Control, value {6} - Start transmission, {3} - Byte Data mode
; -- SMB_Start_CMD
r000:5762 b80002 mov ax, 0x248 ; 0x00000248
r000:5765 bf0057 mov di, 0x570a ; 0x0000570a
```


Keeping notes through your work

- KeepNote available in Kali linux
- To organize the information gathered during your security project
- Can do screen grabbing and export to HTML
- You are of course free to use any application of your choice as long as you track and write down your findings.



Searching for exploits

- There are several source for public exploits
- A good and reliable source: Exploit-db (www.exploit-db.com)
 - Available in your kali distro with `searchsploit` command

<https://www.exploit-db.com>

EXPLOIT DATABASE Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security's Exploit Database Archive **35484**
Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).

The Exploit Database
The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database.
[Download the Exploit Database Archive](#)

EXPLOIT DATABASE
CVE Compliant 

Remote Exploits

This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2016-09-16	📄	-	🔒	Cisco ASA 9.2(3) - 'EXTRABACON' Authentication Bypass	Hardware	Sean Dillon
2016-09-14	📄	-	🔒	Apache Mina 2.0.13 - Remote Command Execution	Multiple	Gregory Draper.
2016-09-09	📄	📄	🔒	LamaHub 0.0.6.2 - Buffer Overflow	Linux	PI3rrot
2002-09-17	📄	-	🔒	Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG...	Unix	Solar Eclipse
2016-09-08	📄	-	🔒	Android - libutils UTF16 to UTF8 Conversion Heap Buffer Overflow	Android	Google Securit.
2016-09-07	📄	📄	🔒	SugarCRM 6.5.23 - REST PHP Object Injection Exploit (Metasploit)	PHP	Egidio Romano
2016-09-06	📄	-	🔒	glibc - getaddrinfo Stack Based Buffer Overflow (2)	Linux	Speedr00t