

Laboratorio di Internet, Reti e Sicurezza

Introduzione + Wireshark

Fabrizio Ippoliti - A.A. 2015-2016



Contatti

- Fabrizio Ippoliti, PhD
mail [fabrizio.ippoliti \[AT\] unicom.it](mailto:fabrizio.ippoliti@unicam.it)
web www.cs.unicam.it/marcantoni/
- Ricevimento studenti
sempre (appuntamento via mail)
primo piano, Polo Tecnologico @Battibocca

Obiettivi

A fianco delle nozioni teoriche, sviluppo capacità pratiche

- Progettazione reti
- Amministrazione della rete
- Network/port scanning
- Vulnerability scanning
- Vulnerability exploitation
- Firewall

Partecipazione ATTIVA

Esame

L'esame non è lo scopo di questo corso
(superare gli esami non è lo scopo della laurea).

Per la parte di laboratorio:

- Sezione nell'esame scritto del prof. Marcantoni
- **Tesina ...**

Esame

Già sostenuto l'esame con il prof Polzonetti/Reti degli elaboratori 6 CFU?
Internet, Reti e Sicurezza è un altro corso, quindi ci sono **2 opzioni**:

- 1) sostenere il nuovo esame da 12 CFU.
- 2) ripristinare «Reti degli elaboratori + Laboratorio»
Cisco → prof. Maccari
prof. Marcantoni verbalizzerà Reti + Lab (12 CFU).

Tesina

Tutti gli argomenti dove il concetto di sicurezza informatica ha un ruolo fondamentale.

Materiale da realizzare (?):

- Relazione – solo PDF, no carta!
- Discussione (presentazione/video/demo)

Scelta entro 1 dicembre 2015
Discussa entro 30 gennaio 2016

Tesina

Vostre proposte discusse:

- prima/dopo lezione
- mail
- ricevimento

Presto, già dalle prossime settimane...

Esempio: "Bad USB" MITM Attack

<https://github.com/adamcaudill/Psychson>
<http://vimeo.com/106065667>

[Link tesine proposte](#)

Sicurezza informatica?

Processo di prevenzione e individuazione dell'uso non autorizzato di un sistema informatico.

- Host
- Dati
- Rete
- → Persone ←

Sicurezza informatica?



A seconda del proprio *core business* (e delle risorse a disposizione), si potrà definire un **livello di sicurezza** target.

Eventi dolosi → buona amministrazione sistemi, ...

Eventi accidentali → backup, disaster recovery, ...

Business continuity (plan)

Insieme di attività per assicurare che le funzioni principali di una infrastruttura possano **continuare ad operare** nonostante il verificarsi di **gravi incidenti** o **disastri** che potrebbero interromperle, o che comunque possano essere ripristinate in un ragionevolmente **breve periodo**.

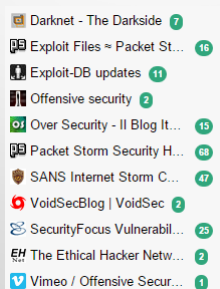
Ci si diverte?



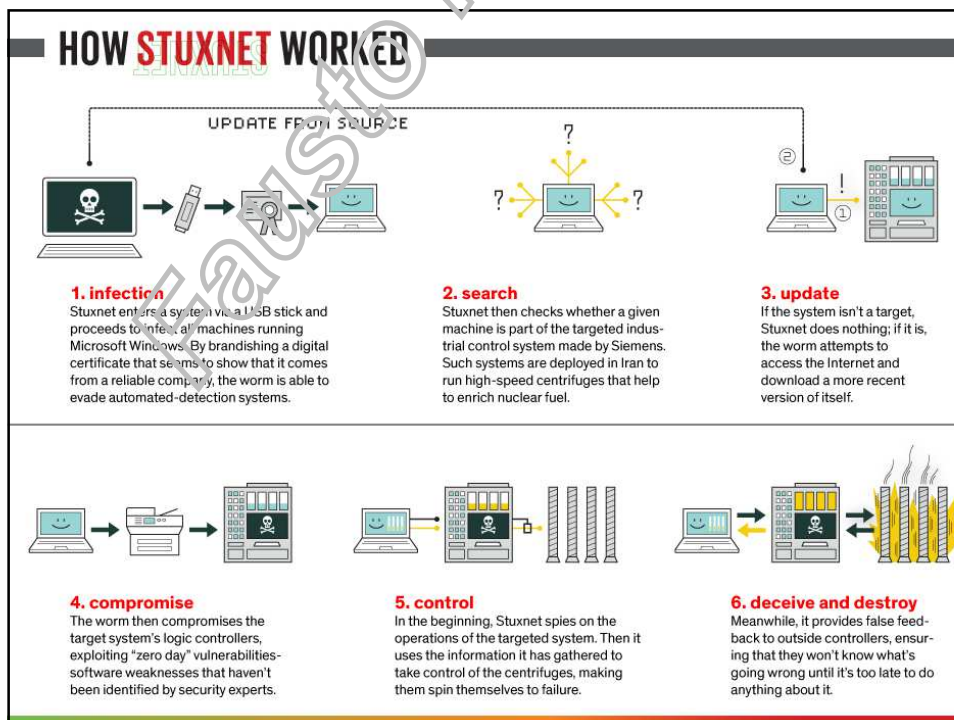
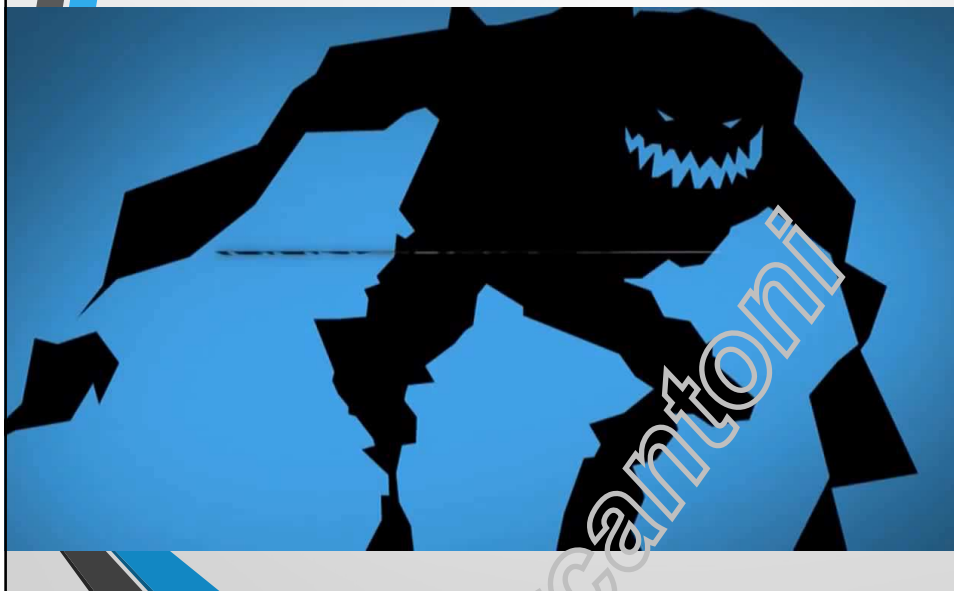
- <https://www.securitysummit.it/>
- <http://www.craccaaltesoro.it/>
- <http://www.hackinbo.it/>

Per saperne di più

- Tantissimi siti di informazione/discussione
- Iscrizione feed RSS...



Una storia...



Alcuni tool, base e non

<http://gexos.github.io/Hacking-Tools-Repository/>

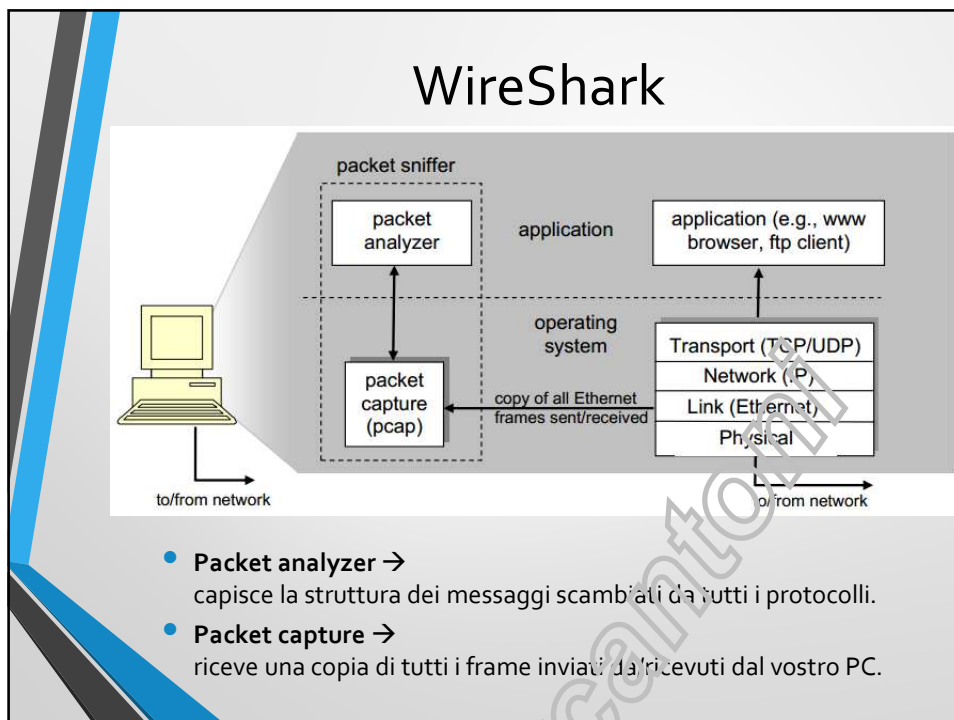
<https://technet.microsoft.com/it-it/sysinternals/bb545027>

<http://www.nirsoft.net/>

WireShark

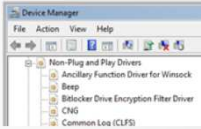
- Strumento base e potente di **troubleshooting***.
- **Sniffer di pacchetti** → Osservazione e analisi messaggi scambiati tra i vari protocolli.
- Messaggi inviati/ricevuti da/a vostro computer.

* Ricerca sistematica delle possibili cause di un certo problema.
Debug: Programmazione=Troubleshooting: Reti



WinPCAP

Possibile cambiare le impostazioni di avvio...



- **Da Device Manager** → View → Show hidden devices, poi aprire *Non-Plug and Play Drivers*, poi tasto destro su *NetGroup Packet Filter Driver*.
- **cmd.** → config npf start= auto (come amministratore...)
- **Cambiando la chiave di registro**
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NPF\Start
 - 0x3 (SERVICE_DEMAND_START)
 - 0x2 (SERVICE_AUTO_START)
 - 0x1 (SERVICE_SYSTEM_START)

Oppure avviarlo manualmente

- **Avvio del driver NPF:** cmd come Administrator → net start npf
 - **cmd** → runas /u:USER "net start npf"
- **Stop del driver NPF:** cmd come Administrator → net stop npf
 - **cmd** → runas /u:USER "net stop npf"

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
306	20.0102270	108.160.166.141	193.205.92.186	TLSv1	91	Encrypted Alert
307	20.0102280	108.160.166.141	193.205.92.186	TCP	60	49672-49672 [FIN, ACK] Seq=1
308	20.0104520	193.205.92.186	108.160.166.141	TCP	54	49672-443 [ACK] Seq=1
309	20.2410600	193.205.92.163	255.255.255.255	DB-LSP-	341	Dropbox LAN sync Discov
310	20.2415680	193.205.92.163	193.205.92.255	DB-LSP-	341	Dropbox LAN sync Discov
311	20.2620460	Hewlett-7a:1c:bc	Broadcast	ARP	60	who has 193.205.92.6?
312	20.2689520	193.205.92.153	255.255.255.255	DB-LSP-	288	Dropbox LAN sync Discov
313	20.2764560	193.205.92.153	255.255.255.255	DB-LSP-	288	Dropbox LAN sync Discov
314	20.2765210	193.205.92.153	255.255.255.255	DB-LSP-	288	Dropbox LAN sync Discov
315	20.2766880	193.205.92.153	193.205.92.255	DB-LSP-	288	Dropbox LAN sync Discov
316	20.2766890	193.205.92.153	255.255.255.255	DB-LSP-	288	Dropbox LAN sync Discov
317	20.3961070	193.205.92.249	255.255.255.255	Admin c	134	
318	20.5070810	193.205.92.153	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
319	20.6147680	193.205.92.31	224.0.0.251	MDNS	87	Standard query 0x0000
320	21.1791900	193.205.92.214	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1
321	21.2549860	Vmware_6a:44:34	Broadcast	ARP	60	who has 193.205.92.4?
322	21.6174550	193.205.92.31	224.0.0.251	MDNS	87	Standard query 0x0000
323	21.6587060	fe80::6030:b6ae:e06ff02:1:3		LLMNR	95	Standard query 0x7b49
324	21.6599920	193.205.92.25	224.0.0.252	LLMNR	75	Standard query 0x7b49

Frame 316: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0
 Ethernet II, Src: Apple_46:eb:09 (c8:2a:14:46:eb:09), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 Source: Apple_46:eb:09 (c8:2a:14:46:eb:09)
 Type: IP (0x0800)
 Internet Protocol Version 4, Src: 193.205.92.153 (193.205.92.153), Dst: 255.255.255.255 (255.255.255.255)
 User Datagram Protocol, Src Port: 17500 (17500), Dst Port: 17500 (17500)

0000 ff ff ff ff ff ff c8 2a 14 46 eb 09 08 00 45 00E.
 0010 01 12 2d 63 00 00 80 11 ee 11 c1 cd 5c 99 ff ff
 0020 ff ff 44 5c 44 5c 00 fe f6 03 7b 22 68 6f 77 74host
 0030 5f 69 6e 74 22 3a 20 33 33 33 36 35 39 39 30 33: 3 33659908
 0040 2c 20 22 76 65 72 73 69 6f 6e 22 3a 20 5b 11 7cversion: 11

Filtering query → https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

WireShark

- Wiki
<http://wiki.wireshark.org/>
- FAQ
<https://www.wireshark.org/faq.html>
- User guide
https://www.wireshark.org/docs/wsug_html_chunked/

Lab. 1

1. Lanciare un browser e avviare lo sniffing Wireshark sulla corretta interfaccia.

Device	Description	IP	Packets	Packets/s	
<input checked="" type="checkbox"/> Ethernet	USB3.0 to Gigabit Ethernet Adapt	193.205.92.186	485	9	Details
<input type="checkbox"/> Wi-Fi	Microsoft	90.147.43.131	0	0	Details
<input type="checkbox"/> Connessione alla rete locale (LAN)* 2	Microsoft	fe80::41da:72c1:d734:d4b5	0	0	Details

2. Navigare su www.unicam.it
3. Fermare lo sniffing
4. Quale informazioni si possono ricavare?
 - HTTP GET
 - Tempo intercorso tra il messaggio HTTP GET e la risposta HTTP OK
 - IP del sito Unicam, IP del vostro PC
 - Porte?
 - ...

Lab. 2

PING → tool per verificare se un host sia UP o DOWN
(Pacchetti ping sono pacchetti del protocollo ICMP)

1. Ping hostname
2. Quale informazioni si possono ricavare?
 - IP source host, destination host
 - Porte?
 - Type e code numbers della richiesta?
 - Type e code numbers della risposta?
 - ...