



NETWORK SECURITY

“Introduzione al Corso”

Corso di Laurea Magistrale in Ingegneria Informatica

Prof. Simon Pietro Romano

sromano@unina.it



DI COSA SI TRATTA?

- Sicurezza di Rete...
- ...o, meglio, Sicurezza delle Applicazioni distribuite (in reti IP)*:
 - posta elettronica, applicazioni Web, sistemi VoIP, sistemi informativi, applicazioni per terminali mobili
- Alcuni argomenti legati alla sicurezza delle infrastrutture di rete:
 - Connattività da remoto
 - Reti wireless
 - Sistemi Hardware (cenni...)

*Applicazioni Telematiche (cfr. cuginetto di questo corso @ unina)!



SECURITY: UNA DEFINIZIONE INFORMALE

“Evitare che entità non autorizzate compiano azioni che non vogliamo che vengano compiute”



SECURITY: UNA DEFINIZIONE FORMALE

- La 'triade' della sicurezza:
 - Confidentiality
 - Integrity
 - Availability



CONFIDENTIALITY

*“The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].”**

* [definizione estratta da RFC 4949 – Internet Security Glossary]



CONFIDENTIALITY vs PRIVACY

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC 4949]

NB:

1. La *privacy* è una delle ragioni che giustificano l'esigenza di "confidentiality"
2. La *privacy* è (anche) strettamente legata all'anonimato (*anonymity*)
3. L'anonimato è (anche) il principale requisito perché un 'hacker' resti impunito
4. Come molte cose della vita, le proprietà della security hanno spesso un duplice risvolto...



A PROPOSITO DI PRIVACY

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say”

*Edward Snowden**

<http://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for>

*uno che di privacy se ne intende!



INTEGRITY [RFC 4949]

Data integrity:

“The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.”

System integrity:

“The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.”



AVAILABILITY [RFC 4949]

“The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.”

NB:

1. Se il mio server è spento, garantisco senz'altro la confidenzialità e l'integrità, ma fallisco completamente per quanto riguarda la disponibilità!
2. Gli attacchi di tipo “Denial Of Service” (DoS) mirano proprio a minare la disponibilità di un servizio...e sono tra i più ‘rognosi’!



ARGOMENTI DEL CORSO

- Sicurezza del protocollo IP
- Sicurezza della posta elettronica
- Sicurezza nel Web
 - ivi comprese le architetture web di nuovissima generazione:
 - *WebRTC* (Web Real Time Communication)
- Intrusioni in reti di calcolatori
- Software doloso
- Firewall
- Tecniche di "hacking":
 - Minacce e contromisure



“HACKING” IN RETI IP

- Fasi preliminari di un attacco:
 - *Footprinting, scanning, enumeration*
- Tecniche di attacco indirizzate a:
 - end-system & server;
 - Infrastruttura:
 - Reti VoIP (Voice over IP)
 - Reti Wireless
 - Sistemi hardware
 - Applicazioni e dati:
 - Web
 - Dispositivi mobili
 - Basi di dati



APPROCCIO MENTALE ALLA SICUREZZA

- I malintenzionati non seguono le regole
- Per capire come rendere un sistema più sicuro bisogna identificare gli attacchi a cui esso può andare soggetto
 - ...il che ovviamente non implica l'esigenza di sferrare realmente tali attacchi!
- Un host non può fidarsi di nessun dato che provenga dalla rete



SECURITY “BY DESIGN”

- Qualsiasi tipo desiderato di protezione deve essere progettato e realizzato in maniera esplicita
- Es: progettazione di protocolli sicuri →
 - Lasciare sempre spazio per crittografia ed autenticazione
 - Assicurarsi che tutti i campi sensibili siano proteggibili
 - Prevedere autenticazione da ambo le parti
 - Prevedere meccanismi di autorizzazione
 - Prevedere meccanismi di difesa da attività malevole quali:
 - “eavesdropping” (intercettazione), modifica selettiva, cancellazione, ‘replay’ e relative combinazioni



SICUREZZA E ‘BUGGY SOFTWARE’

- La maggior parte dei buchi di sicurezza è dovuta a codice ‘difettoso’
- Un programma difettoso che comunichi in rete è una seria minaccia alla sicurezza
- Le tecniche di correzione dei *bug* software rappresentano uno dei principali strumenti di prevenzione legati alla sicurezza dei sistemi



ATTEGGIAMENTI IMPRODUTTIVI

- “Ma perché qualcuno dovrebbe voler fare questo?”
- “Quell’attacco è troppo complicato per avere speranze di successo!”
- “Nessuno conosce come funziona questo sistema (perché è un sistema ‘chiuso’ [ndr]), quindi nessuno lo può attaccare!”

Ah, cett cett!





ATTEGGIAMENTI PRODUTTIVI

- “Programming Satan’s computer” (Ross Anderson & Roger Needham)
 - <http://www.cl.cam.ac.uk/~rja14/Papers/satan.pdf>

In effect, our task is to pro-

gram a computer which gives answers which are subtly and maliciously wrong at the most inconvenient possible moment. This is a fascinating problem; and we hope that the lessons learned from programming Satan’s computer may be helpful in tackling the more common problem of programming Murphy’s.

- “Assumi che il ‘numero seriale 1’ di qualsiasi dispositivo venga venduto al nemico”
- “Tutti i pacchetti che invii li passi al nemico; tutti i pacchetti che ricevi ti vengono consegnati dal nemico”

STRUMENTI PER LA SICUREZZA DELLE RETI

- Crittografia
 - “Out of Topic” per questo corso → cfr. corso di “Secure Systems Design”
- Network-based access control
 - ...ivi inclusi i Firewall
- Monitoraggio di rete
 - cfr. (anche) corso di “Analisi e Prestazioni di Internet”
- Impiego di tecniche cosiddette di “Paranoid Design”
 - cfr. slide precedente sugli atteggiamenti produttivi...

PROGRAMMA DEL CORSO (1/2)

- Principi di sicurezza delle reti
 - requisiti funzionali per la security
 - “threats”, attacchi, contromisure
- Sicurezza in reti wireless
- Sicurezza a livello rete
 - protocollo IPsec
- Sicurezza a livello trasporto
 - Transport Layer Security (TLS)
- Sicurezza al livello applicativo:
 - posta elettronica
 - Web
 - HTTPS
 - WebRTC Security Architecture
- Cloud Computing e sicurezza (cenni)



PROGRAMMA DEL CORSO (2/2)

- Software malevolo
 - Tassonomia
 - Advanced Persistent Threats (APTs)
 - Contromisure
- Attacchi di tipo “Denial of Service” (DoS) e “Distributed Denial of Service” (DDoS)
- Intrusion Detection Systems (IDS)
 - Tecniche “host-based”, “network-based” e ibride
- Firewall e Intrusion Prevention Systems (IPS)



PREREQUISITI e/o PROPEDEUTICITÀ

- Si tratta di un corso avanzato di reti di calcolatori, per cui:
 - Reti di Calcolatori
 - propedeutico
 - Computer Networks II
 - caldamente consigliato come prerequisito per il corso
 - Applicazioni Telematiche
 - utilissimo per le conoscenze approfondite sui protocolli applicativi di Internet (Web, applicazioni VoIP, applicazioni real-time multimediali)
- In realtà si parlerà molto anche di:
 - Software e tecniche di programmazione
 - Sistemi Operativi
 - Architettura dei calcolatori
 - ...che ci crediate o meno, un “buffer exploit”, se non conoscete un po’ di assembly e di tecniche per la chiamata di sottoprogrammi, non lo capirete mai!

MODALITÀ DI ACCERTAMENTO DEL PROFITTO

- **35%** del voto finale dipenderà dalla valutazione di un progetto pratico legato ad argomenti selezionati del corso e concordati con il docente
 - possibilità di svolgere progetti di gruppo
 - gruppi di max 4 persone
 - Elaborato consegnato al docente
 - almeno 7 giorni prima della prova orale
 - completo di documentazione e codice sorgente
- **65%** del voto finale dipenderà dall'esito di una prova orale
 - verifica degli argomenti trattati al corso
 - presentazione e discussione del progetto



A PROPOSITO DEI PROGETTI DI GRUPPO

- Cooperazione vs Disonestà
 - un gruppo si può definire tale se tutti i suoi membri apportano un contributo individuale
- Un progetto è valido se contiene contributi originali
 - lo scopo dei progetti è farvi approfondire alcuni argomenti e porvi dinanzi a problemi stimolanti e di non immediata soluzione
 - ...il “copia & incolla” (da Internet, da un amico, o da qualsiasi altra sorgente) si chiama plagio e non è un comportamento eticamente corretto
- Esempio di policy sull'onestà accademica:
 - <http://www.cs.columbia.edu/education/honesty>



LEZIONI FRONTALI

- Presentazione degli argomenti del corso mediante proiezione di slide
 - NB:
 - le slide NON sono mai esaustive (se lo fossero, sarebbero pessime slide)
 - le slide NON sostituiscono i libri di testo, gli articoli, o qualsiasi altro materiale didattico consigliato dal docente
 - Nei limiti del possibile (non si tratta di un corso che preveda esplicite attività di laboratorio ☺)
 - esempi pratici legati ad alcuni argomenti cruciali del corso
 - utili per illustrare con approccio ingegneristico i temi affrontati
 - da considerare come spunti per la definizione dei progetti pratici



HOMEWORK

- Una fase significativa dell'apprendimento si svolgerà in autonomia
 - sperimentare le tecniche e le metodologie illustrate a lezione
 - approfondire alcuni argomenti di interesse
 - prepararsi alla realizzazione del progetto pratico in vista dell'esame
- Tutti i problemi che incontrerete a casa, li possiamo discutere insieme a ricevimento



APPROCCIO PRATICO

- Come sempre, imparare dagli esempi, per un ingegnere, è fondamentale
- Impossibile arrivare ad avere una preparazione completa senza ‘sporcarsi le mani’
- Ma:
 - la pratica, da sola, non basta
 - sono le conoscenze teoriche approfondite che distinguono un ingegnere da uno ‘smanettone’...
 - ...e voi siete quasi ingegneri!
 - L’approccio giusto è:
 1. Studio
 2. Sperimento
 3. Capisco meglio quello che ho studiato!



ETICA DELLA SICUREZZA

- Seguire un corso di security NON è una scusa per comportarsi da “hacker”
- Nella sua accezione negativa, con il termine “hacking” intendiamo:
 - qualsiasi forma di accesso non autorizzato a risorse disponibili in rete, ivi incluse tecniche che prevedano l'abuso di permessi autorizzati
- Il semplice fatto che un file o un computer non sia opportunamente protetto non giustifica un accesso non autorizzato
 - ...se il legittimo proprietario di una risorsa vi ‘invita’ ad attaccarla, allora sì che siete autorizzati!
 - Mai sentito parlare di ‘penetration testing’?
- In questo corso non “prenderemo sotto gamba le cose serie”
 - Non diventeremo tristemente famosi per aver inventato e diffuso nuovi “Trojan Horses”, nuove “backdoor” o qualsiasi altra forma di codice malevolo



ASSUNZIONE DI RESPONSABILITÀ

- Siete tutti adulti
- Siete tutti responsabili delle vostre azioni
- Lo scopo di questo corso è quello di creare degli esperti di sicurezza...
- ...non degli 'skiddies'

Script kiddie

From Wikipedia, the free encyclopedia

In programming culture a **script kiddie** or **skiddie**^[1] (also known as *skid*, *script bunny*,^[2] *script kitty*)^[3] is an **unskilled** individual who uses **scripts** or programs developed by others to attack computer systems and networks, and **deface websites**. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities.^[4] However, the term does not relate to the actual age of the participant. The term is generally considered to be pejorative.



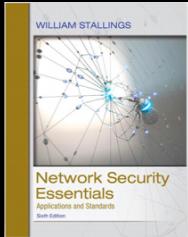
RIFERIMENTI DEL DOCENTE

- Simon Pietro Romano
 - Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI)
 - Ufficio:
 - Via Claudio 21, palazzina 3, quarto piano, stanza IV.08
 -  +39 0817683823
 -  spromano@unina.it
 -  @spromano
- Orario di ricevimento:
 - Mercoledì dalle 10:45 alle 12:45

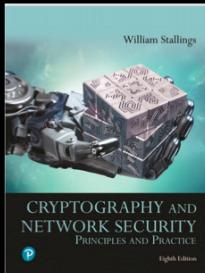


MATERIALE DIDATTICO (1/2)

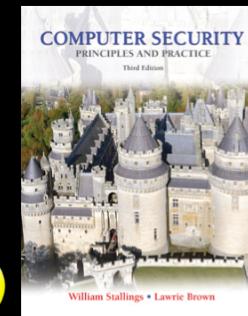
- Libri consigliati:
 - Il principale ‘evangelist’ accademico in ambito sicurezza:
 - William Stallings
 - Tre libri famosi e tutti adatti allo scopo



“Network Security Essentials Applications and Standards”, 6/E
William Stallings
ISBN-13: 9780134528038 - (e-book: 9780134527598)
©2017 • Pearson



“Cryptography and Network Security: Principles and Practice”, 8th Edition
William Stallings
ISBN-13: 9780135764039 (e-book: 9780135764268)
©2020 • Pearson



“Computer Security: Principles and Practice”, 4/E
William Stallings Lawrie Brown
ISBN-13: 9780134794334 – (e-book: 9780134794181)
©2018 • Pearson



MATERIALE DIDATTICO (2/2)

- Una bibbia per chi vuole sperimentare:



"Hacking Exposed", 7th Edition
by Stuart McClure, Joel Scambray and George Kurtz
Mc Graw Hill
ISBN-10: 0071780289, ISBN-13: 978-0071780285

- Materiale disponibile in rete
 - Riferimenti ‘formali’:
 - es: Request For Comments (RFC)
 - www.ietf.org
 - Riferimenti ‘informali’:
 - es: Phrack Magazine
 - www.phrack.org





A PROPOSITO DI SPERIMENTAZIONE

- *"The quieter you become, the more you are able to hear"*
- Kali Linux:
 - un progetto open source creato e gestito dal gruppo "Offensive Security", specializzato in attività di formazione in ambito sicurezza, con focus sui servizi cosiddetti di "penetration testing"
 - una distribuzione Linux 'preconfezionata' con una impressionante serie di tool per l'auditing della sicurezza





KALI LINUX TOOLS

- Information gathering
- Sniffing & spoofing
- Vulnerability analysis
- Exploitation
- Password attacks
- Wireless attacks
- Forensic analysis
- Hardware hacking
- Web applications attacks
- Reporting
- Stress testing
- Reverse engineering
- Social engineering
- ...

DOMANDE?

