Introduzione

Fondamenti di Cybersecurity 2022/2023

Davide Berardi <davide.berardi@unibo.it>

Il corso è diviso in 3 macro-parti:

- Parte Generale
- Crittografia
- Esercitazioni

Imparerete le basi della crittografia e della cybersecurity **infrastrutturale** e **applicativa**.
No Web! (qualche accenno, ne parleremo tra poco).

Esercitazioni: 8/30 del totale
Esame Scritto: 24/30 del totale.
Voto >30 = Lode!

Parte Generale: Davide Berardi <davide.berardi@unibo.it >
Crittografia: Riccardo Treglia <riccardo.treglia@unibo.it >
Tutor / Esercitazioni: Giacomo Gori <g.gori@unibo.it >

Davide Berardi

http://cs.unibo.it/~davide.berardi6
Founder of MON5 security startup (https://mon5.it)

Adjunct Professor & Research Fellow @ UniBo

Ph.D. in Computer Science & Engineering from 2022
Ex (from 2016 to 2018) Firmware Engineer @ T3LAB
Member of Ulisse (https://ulis.se)

Keywords: Network Security; System Administration; GNU/Linux; Embedded Systems; Industrial / Automotive / Satellite Security

Hacker 7.0


Stuart McClure – Joel Scambray – George Kurtz
HACKER
7.0
DA 13 ANNI IL BEST SELLER
SULLA SICUREZZA INFORMATICA
TRADOTTO IN 30 LINGUE
600.000 COPIE VENDUTE
"Un buon sistema di sicurezza si misura proprio con
'non succede niente'."
– Stuart McClure, Joel Scambray, George Kurtz
APOGEO

La cybersecurity è un processo. È trasversale agli argomenti.
E.g. sicurezza delle reti, sicurezza industriale, sicurezza web, sicurezza degli applicativi, sicurezza infrastrutturale, etc.

- Linux / VM
- TOR / Dark Web / OSINT
- Radio / SDR
- Cifrari simmetrici / asimmetrici
- Password
- Sicurezza Wifi
- Network Security
- Reverse engineering e pwning
- Hardware security e Hardware open source (accenni)

Essendo una materia estremamente ampia, esistono diversi corsi Unibo.

Possibili corsi a scelta dei vostri 12 CFU:

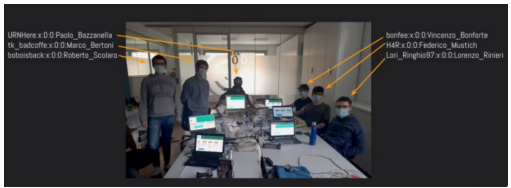
Triennale Informatica: questo corso (6CFU, hw / reverse engineering)

Triennale Ingegneria Informatica: Laboratorio Di Sicurezza Informatica T (6CFU, web / red teaming)

Attività extra:

Cyberchallenge: `https://cyberchallenge.it/`

- Percorso a numero chiuso di 12 Lezioni su temi avanzati di sicurezza (PWN, reverse engineering, Web security, crypto, sicurezza dei sistemi e delle reti).



1 Luglio 2019 Premi e riconoscimenti

Cyber challenge italiana, medaglia d'argento per i cyber-defender Unibo

Il team dell'Alma Mater ha sbaragliato le altre squadre, composte da studenti universitari provenienti da tutta Italia, in una sfida sulla gestione della sicurezza di sistemi informatici di tipo attacco-difesa

Attività extra:

- Ulisse, Unibo Laboratory of Information and System SEcurity, gruppo di studenti e dottorandi interessati alla sicurezza informatica. Facciamo:
  - Progetti (sicurezza di ALMAWIFI);
  - CTF (Competizioni di sicurezza informatica);
  - Seminari.
  - `ulis.se` oppure `ulisse.unibo.it`

SMBs typically spend around 10% of their annual budget on cybersecurity The amount of money that many businesses spend on cyber security services varies but usually falls around 10% of the yearly IT budget. Companies spend $250,000 on cybersecurity solutions and training with annual IT budgets of $2.5M. Each full-time employee costs a company $2,500 – $2,800 for solid cyber security protection.

https://imagineiti.com/
how-much-does-cybersecurity-cost-for-small-to-mid-sized-businesses/

If You Think Education Is Expensive, Try Ignorance

Derek Bok

Ransomware attacks grew and destructive attacks got costlier

The share of breaches caused by ransomware grew 41% in the last year and took 49 days longer than average to identify and contain. Additionally, destructive attacks increased in cost by over USD 430,000.

$4.54M

Average cost of a ransomware attack

$5.12M

Average cost of a destructive attack

https://www.ibm.com/reports/data-breach

Gli attacchi moderni si classificano principalmente per le seguenti tipologie:

- Ransomware
- Malicious Code
- Destructive Malware
- Rootkits and Botnets
- Trojan horses
- Corrupted Software Files
- Spyware
- Denial-of-Service Attacks
- Phishing
- Network Infrastructure Devices
- Website Security
- Securing Wireless Networks
- Mobile security

Gli hacker vengono generalmente classificati secondo tre categorie:

- White Hat, hacker “buoni”;
- Black Hat, hacker “cattivi”;
- Grey Hat.

Sono classificazioni che riguardano l’etica degli attaccanti.

Pensate alle CTF un po' come alle olimpiadi dell'informatica, con l'unica differenza che sono in gruppo e dovete bucare dei software!

How does it feels like

How it really is

Le CTF saranno parte integrante di questo percorso, le esercitazioni saranno strutturate allo stesso modo di una CTF semplice.

Un esempio di CTF (in realtà un wargame) è:
`https://overthewire.org/wargames/bandit/`.

Molto consigliato svolgerlo per prepararsi al corso!

Uno dei concetti più importanti e controintuitivi della sicurezza informatica.

Security by Obscurity è la segretezza di un sistema data dal fatto che non si conoscono i suoi funzionamenti interni.

La sicurezza di un sistema non deve mai dipendere dalla segretezza del suo funzionamento.

Esempio: Qual è la sicurezza di un sistema web che controlla la password lato client?

Nessuna! Potete creare un altro client copiando il codice e togliendo il controllo della password.

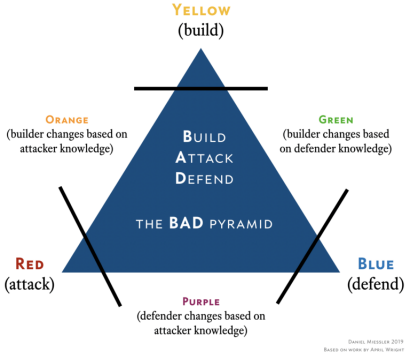
La sicurezza in questo caso sta nel fatto che credete che nessuno sia in grado di riscrivere il client togliendo quel controllo.

È esattamente quello che succede con le crack dei videogiochi.

Il mondo dell'hacking Etico (white hat) si divide in diversi team.

- Red Team – Team "d'attacco" (e.g. penetration tester)
- Blue Team – Team "di difesa" (e.g. sysadmin)

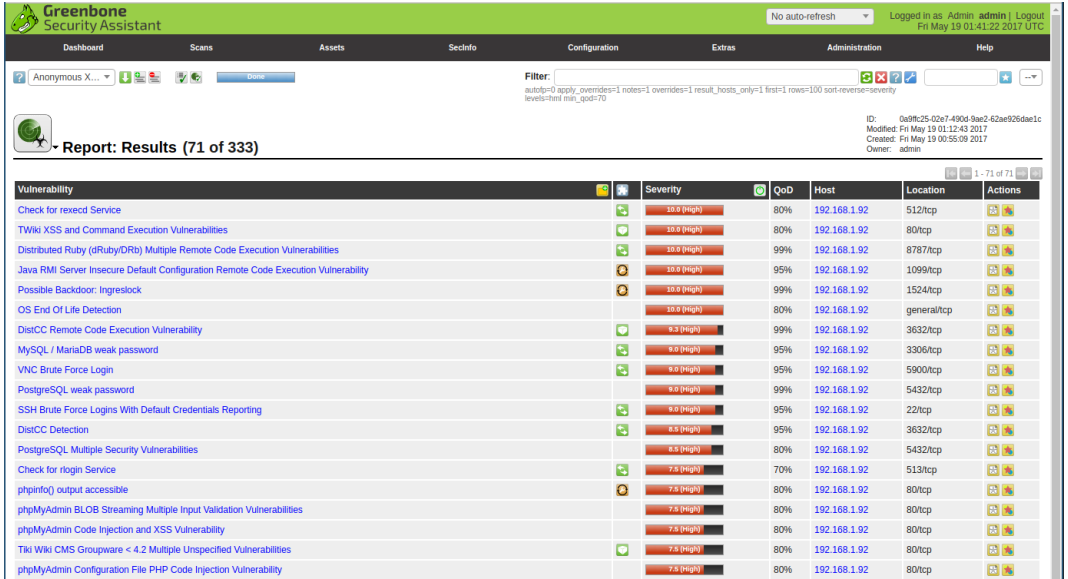
Mix di questi team e altri team sono presenti sul mercato!



Un'azienda potrebbe richiedere una certificazione del proprio livello di sicurezza (infrastrutturale o di un suo prodotto). Per questo scopo esistono due procedure:

- Vulnerability Assessment
- Penetration Test

Il primo espone al cliente la lista di **possibili** Vulnerabilità presenti, il secondo dove un hacker può arrivare sfruttando certe vulnerabilità



Greenbone Security Assistant

No auto-refresh | Logged in as Admin admin | Logout
Fri May 19 01:41:22 2017 UTC

Dashboard | Scans | Assets | SecInfo | Configuration | Extras | Administration | Help

Anonymous X... | Done

Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (71 of 333)

ID: 0a9ffc25-02e7-490d-9ae2-62ae926dae1c
Modified: Fri May 19 01:12:43 2017
Created: Fri May 19 00:55:09 2017
Owner: admin

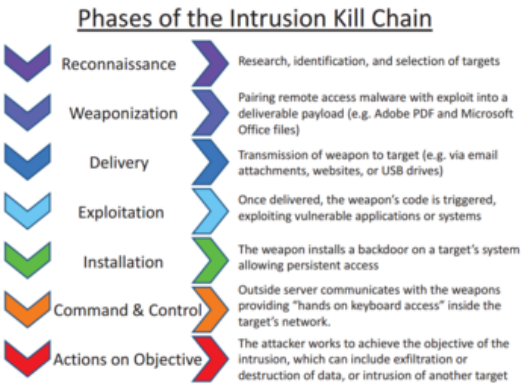
1 - 71 of 71

Vulnerability	Severity	QoD	Host	Location	Actions
Check for rexecd Service	10.0 (High)	80%	192.168.1.92	512/tcp	
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.92	80/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.92	8787/tcp	
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95%	192.168.1.92	1099/tcp	
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.92	1524/tcp	
OS End Of Life Detection	10.0 (High)	80%	192.168.1.92	general/tcp	
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.92	3632/tcp	
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.1.92	3306/tcp	
VNC Brute Force Login	9.0 (High)	95%	192.168.1.92	5900/tcp	
PostgreSQL weak password	9.0 (High)	99%	192.168.1.92	5432/tcp	
SSH Brute Force Logins With Default Credentials Reporting	9.0 (High)	95%	192.168.1.92	22/tcp	
DistCC Detection	8.5 (High)	95%	192.168.1.92	3632/tcp	
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	192.168.1.92	5432/tcp	
Check for rlogin Service	7.5 (High)	70%	192.168.1.92	513/tcp	
phpinfo() output accessible	7.5 (High)	80%	192.168.1.92	80/tcp	
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities	7.5 (High)	80%	192.168.1.92	80/tcp	
phpMyAdmin Code Injection and XSS Vulnerability	7.5 (High)	80%	192.168.1.92	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.1.92	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	80%	192.168.1.92	80/tcp	

Esempio di Penetration Test a MON5:

1. Vengono ricercati online i profili delle persone che lavorano in MON5 (OSINT);
2. Viene creato un finto ransomware da inviare ai dipendenti;
3. Viene mandata una mail di phishing contenente un exploit e il ransomware;
4. Viene infettata l'azienda.

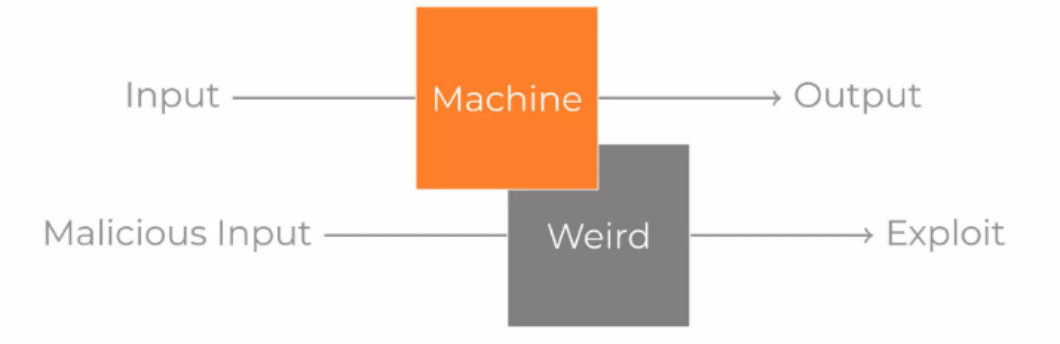
L'azienda era carente quindi di formazione di personale, viene creato un report per spiegare i passi da effettuare per correggere queste mancanze.



La kill chain è un processo messo in atto dagli attaccanti e ricalcato da chi si vuole mettere nei panni di un attaccante.

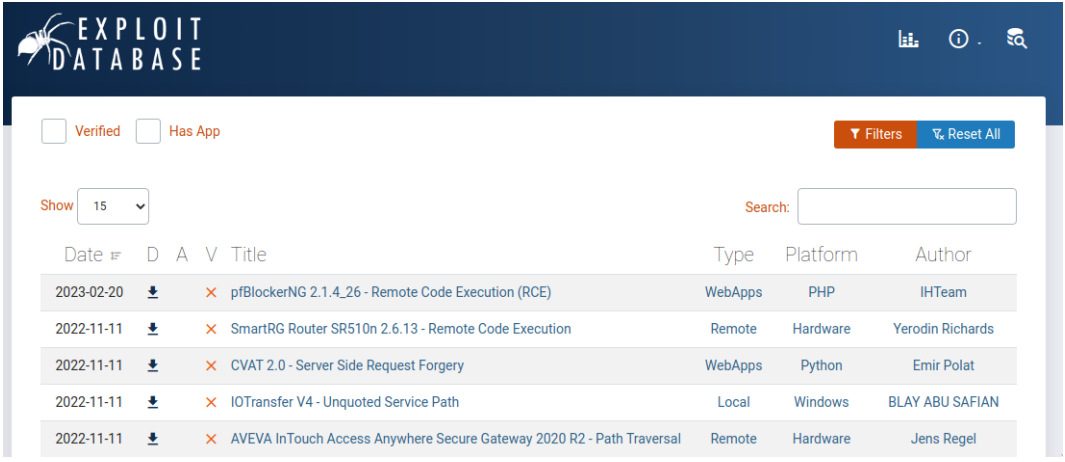
Una debolezza in un sistema informatico che può essere sfruttata da una fonte terza.

Esempio: Weird Machine



Un exploit è un programma o uno script o un comando in grado di sfruttare una specifica vulnerabilità per ottenere un risultato (e.g. installare un malware o ottenere una shell).
Esempio: Shellshock

curl -H "User-Agent: () { :; }; /bin/eject" http://example.com/


EXPLOIT DATABASE
Verified
Has App
Filters
Reset All
Show 15
Search:
Date D A V Title Type Platform Author
2023-02-20 pfBlockerNG 2.1.4_26 - Remote Code Execution (RCE) WebApps PHP IHTeam
2022-11-11 SmartRG Router SR510n 2.6.13 - Remote Code Execution Remote Hardware Yerodin Richards
2022-11-11 CVAT 2.0 - Server Side Request Forgery WebApps Python Emir Polat
2022-11-11 IOTransfer V4 - Unquoted Service Path Local Windows BLAY ABU SAFIAN
2022-11-11 AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal Remote Hardware Jens Regel

Un CVE (Common Vulnerability Exposure) è un programma di classificazione delle vulnerabilità.

A molte vulnerabilità note è associato un identificativo CVE con il relativo livello di minaccia.

zeroday

Uno Zero Day è una vulnerabilità precedentemente ignota a chi è interessato alla sua risoluzione

Uno script kiddie (skid) è un Hacker che si limita ad eseguire (o modificare leggermente ed eseguire) exploit senza capirne il funzionamento interno.

Sono generalmente bistrattati dalla community hacker ma costituiscono una minaccia alla stregua black hat malevoli (se non peggio).

Uno skid potrebbe lanciare un exploit in grado di generare un Denial of Service di una linea di produzione, anche come danno collaterale.

Domande?