UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SERLAB
Software Engineering Research

DIPARTIMENTO DI INFORMATICA
CORSO DI LAUREA IN INFORMATICA E TECNOLOGIE PER LA PRODUZIONE DEL SOFTWARE

TESI DI LAUREA IN
INTEGRAZIONE E TEST DI SISTEMI SOFTWARE

A CYBER RANGE FOR CYBER ATTACK AND DEFENSE SIMULATION

Relatori

Prof. Michele SCALERA

Dott.ssa Vita Santa BARLETTA

Laureando

Francesco MORAMARCO

SICUREZZA E FORMAZIONE

Il rapporto CLUSIT pubblicato nel primo trimestre del 2020 rileva che Malware e Phishing/Ingegneria sociale sono stati gli attacchi informatici maggiormente utilizzati nel 2019.

Si tratta di attacchi in cui il fattore umano è di fondamentale importanza.

TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Malware	127	106	229	446	585	730	24.8%	↑
Unknown	199	232	338	277	408	317	-22.3%	↓
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	-28.8%	↓
Phishing / Social Engineering	4	6	76	102	160	291	81.9%	↑
Multiple Techniques / APT	60	104	59	63	98	65	-33.7%	↓
Account Cracking	86	91	46	52	56	86	53.6%	↑
DDoS	81	101	115	38	38	23	-39.5%	↓
0-day	8	3	13	12	20	30	50.0%	↑
Phone Hacking	3	1	3	3	9	1	-88.9%	↓
SQL Injection	110	184	35	7	1	1	0.0%	-
TOTALE	873	1012	1050	1127	1552	1670		

Rapporto CLUSIT 2020 sulla distribuzione delle tecniche di attacco

SICUREZZA E FORMAZIONE

Phishing: **ingannare la vittima**

Ingegneria sociale: **Manipolare la vittima**

Per indurlo ad agire secondo i propri fini, il malintenzionato può far leva su

- **Panico** e **Urgenza**
- **Mancanza** di **conoscenza** tecnica
- spacciarsi per qualcuno al di sopra della sua posizione professionale
- …

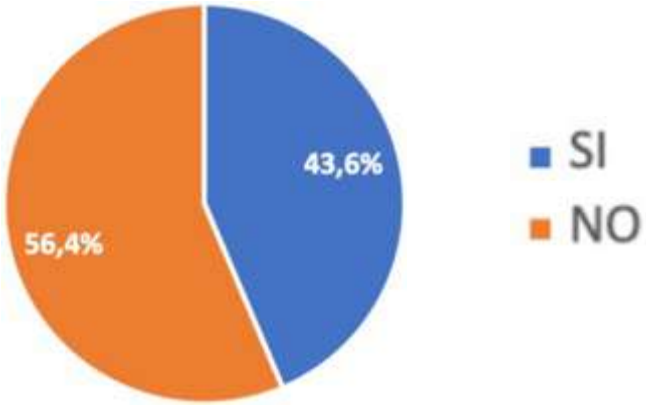
SICUREZZA E FORMAZIONE

Occorre **aumentare la consapevolezza** sulla sicurezza informatica nel pubblico e le **competenze** di cyber security tra i professionisti della sicurezza. Tuttavia…

Lo studio condotto **sullo stato della cybersecurity nel Sud Italia**, rileva che il 56,4% di aziende/enti intervistate non offre corsi specifici sulla cybersecurity.

Tra i dipendenti, il 32,7% e il 36,4% si ritengono rispettivamente poco o per niente consapevoli circa i rischi conseguenti ad un attacco informatico.

Ripartizione del campione intervistato rispetto all'attività formativa svolta sulla sicurezza informatica



Ripartizione del campione intervistato per grado di consapevolezza sui rischi conseguenti un attacco

SICUREZZA E FORMAZIONE

Formazione teorica

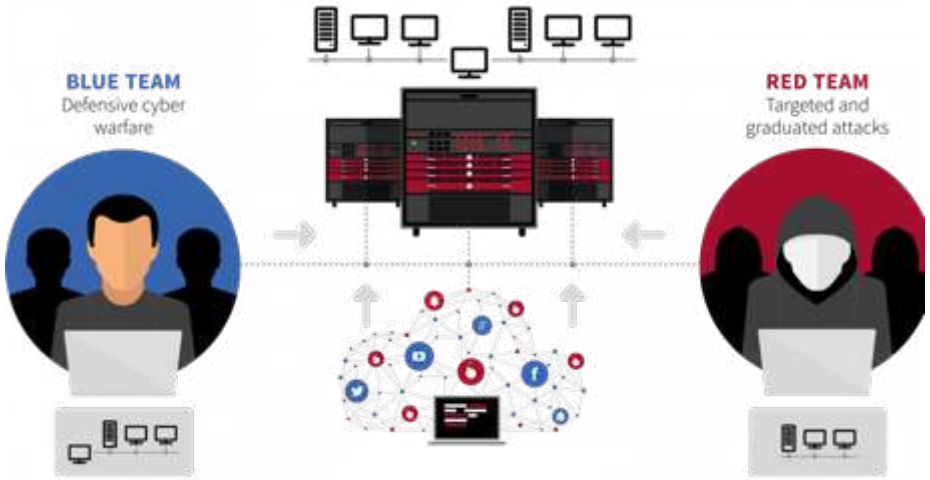
Corsi formativi fruibili in modalità e-learning (SCORM)

Formazione pratica

Cyber Range

Gestione & Valutazione

Learning Management System

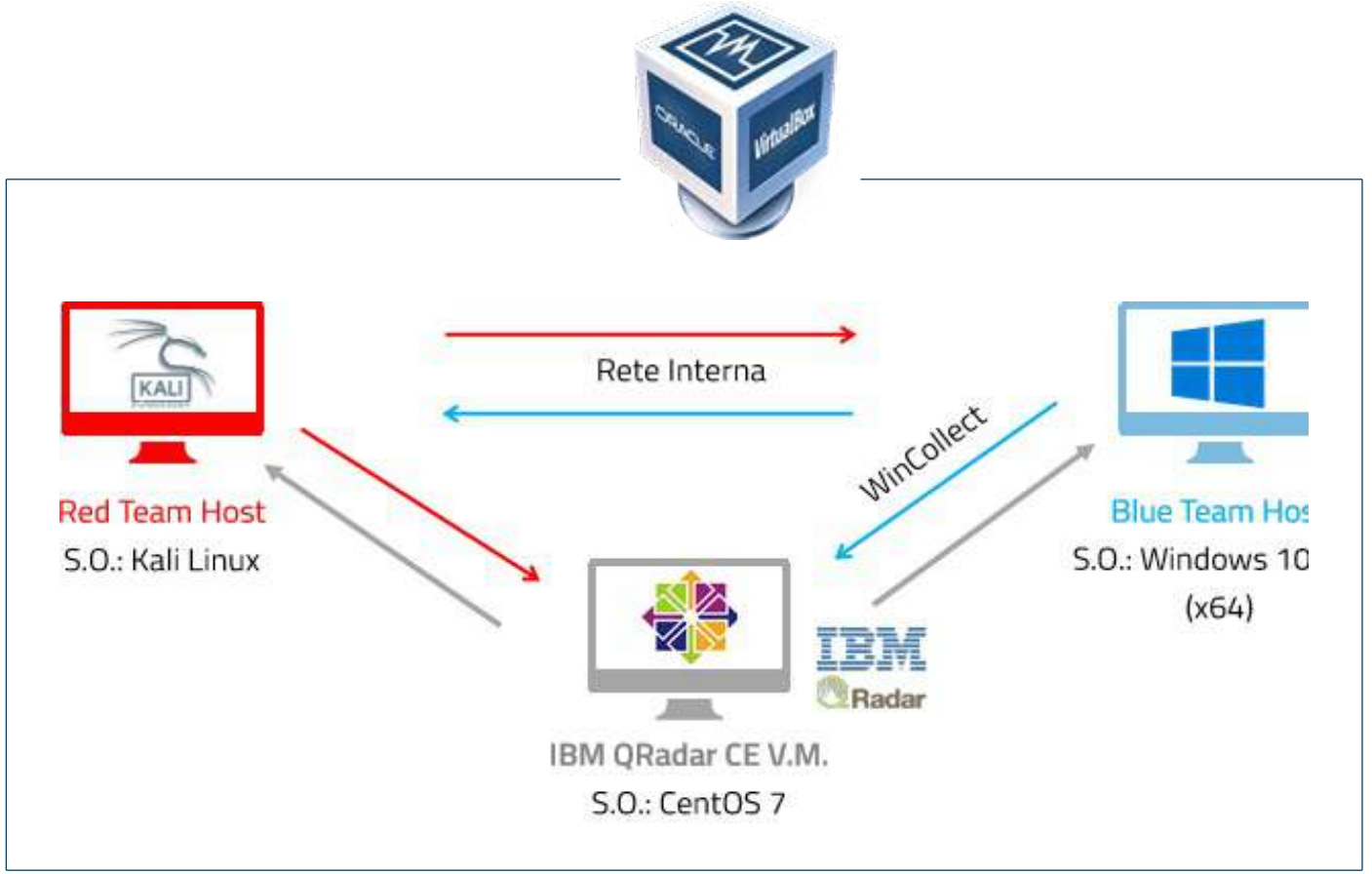


THE HACK-SPACE CYBER RANGE

Ambiente virtuale creato con il software Oracle VM VirtualBox

3 Host

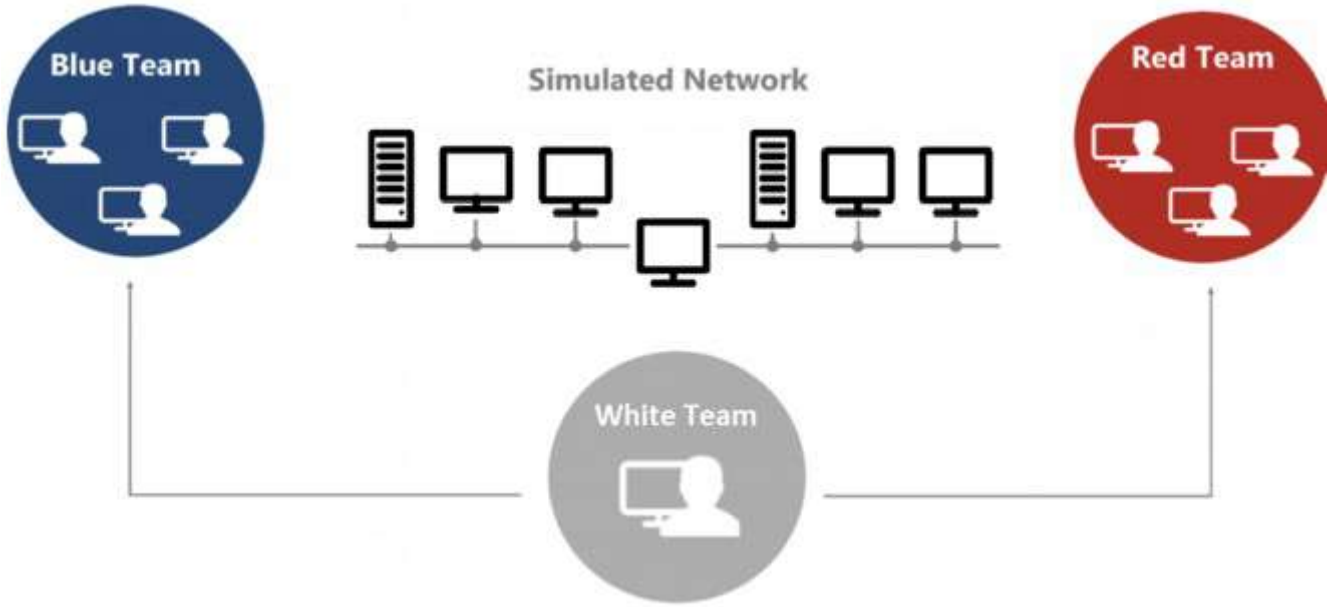
- Red Team Host
- Blue Team Host
- IBM Qradar CE V.M.



RED TEAM VS BLUE TEAM

Si tratta di una esercitazione dove il Cyber Range offre il campo di battaglia in cui si contrappongono Red Team e Blue Team.

- Red Team: compromette la sicurezza dello scenario simulato
- Blue Team: difende lo scenario simulato
- White Team: orchestrata l'intero processo formativo



LEARNING MANAGEMENT SYSTEM

- Fruizione di corsi formativi in modalità e-learning
- Unità didattiche e test di valutazione personalizzati distribuiti tramite pacchetti SCORM

MATERIALE DIDATTICO CYBER KILL CHAIN

MATERIALE DIDATTICO CYBER KILL CHAIN

THE HACK-SPACE CYBER RANGE

2. WEAPONIZATION

TATTICA	
ID	NOME
T1347	Build Capabilities
TECNICHE	
T1350	Discover new exploits and monitor exploit-provider forums
T1346	Obtain/re-use payloads

THE HACK-SPACE CYBER RANGE

2. WEAPONIZATION

La creazione dell'exploit avviene attraverso l'utilizzo del Metasploit Framework, preinstallato all'interno del sistema operativo Kali Linux.

Exploit scelto:
exploit/windows/fileformat/adobe_pdf_embedded_exe
Payload scelto:
windows/x64/meterpreter/reverse_tcp

Questo exploit consente di sfruttare una vulnerabilità del programma Adobe Reader nelle versione 8.x e 9.x per l'esecuzione del payload che, una volta eseguito, avvierà una reverse TCP connection tra attacante e vittima. Il codice malevolo sarà nascosto all'interno di un file pdf, generato in automatico dal modulo exploit scelto.

THE HACK-SPACE CYBER RANGE

2. WEAPONIZATION

Video dimostrativo

THE HACK-SPACE CYBER RANGE

2. WEAPONIZATION

Tabella dei comandi utilizzati in video

COMANDO	FUNZIONE
msfconsole	Avvia il Metasploit Framework
exploit	esegue il modulo exploit
use <exploit>	Imposta il modulo exploit da utilizzare
set <payload>	Imposta il payload da utilizzare Assegna un valore ai parametri da configurare
info	Mostra una descrizione relativa all'exploit selezionato
Show options	Visualizza i parametri configurabili, sia per exploit che payload

METODOLOGIE DI ESECUZIONE

- CYBER KILL CHAIN
  1. Reconnaissance
  2. Weaponization
  3. Delivery
  4. Exploitation
  5. Installation
  6. Command & Control
  7. Actions On Objectives
- MITRE ATT&CK
  - Tattiche
  - Tecniche, Sotto-Tecniche
  - Mitigazioni
- CIS CONTROLS
  - Best practices

MITRE ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

CIS Controls®

STRUMENTI UTILIZZATI – RED TEAM

Metasploit Framework

Raccolta di moduli exploit e payload per eseguire un attacco

Nmap

Port scanner

Individuazione punti deboli

STRUMENTI UTILIZZATI – BLUE TEAM

IBM Qradar

Security Information and Event Management

Nessus Essentials

Vulnerability scanner

CONFIGURAZIONE CYBER RANGE

Red Team Host

S.O.: Kali Linux

Software installati

NMap
Metasploit
Cryptr
Thunderbird
Tcpdump

Blue Team Host

S.O.: Windows 10 Pro (x64)

Software installati

Nessus
Outlook 2010
Adobe Reader 8.1
hMailServer
WinDump

IBM QRadar CE V.M.

S.O.: CentOS 7

Software installati

QRadar CE 7.3.3
Tcpreplay

SPERIMENTAZIONE

SCENARIO

Spear Phishing Attachment: attacco mirato a una persona in particolare o a un impiegato specifico di un'azienda basato sull'utilizzo di allegati malevoli, generalmente inviati tramite e-mail.

Il messaggio, di solito, cerca di fornire una ragione plausibile per cui il file dovrebbe essere aperto e con quali modalità, per aggirare le protezioni del sistema. Ad esempio, l'e-mail potrebbe contenere le istruzioni su come decriptare un allegato.

RECONNAISSANCE

- People Information Gathering
- Social Engineering
- Technical Information Gathering - Scansione della rete con il tool Nmap

- Rispettare le Policy di Sicurezza aziendale
- Limitare la diffusione di informazioni confidenziali
- Formazione e sensibilizzazione del personale sulla sicurezza

WEAPONIZATION

- Creazione dell'allegato pdf malevolo, tramite il Metasploit Framework

- Scansione delle vulnerabilità tramite il software Nessus Essentials
- Aggiornare S.O. e software di terze parti
- Tenersi aggiornati sulle ultime vulnerabilità scoperte

DELIVERY

- Creazione di un indirizzo email verosimile attraverso cui fingersi il direttore del reparto
- Invio dell'email di Spear Phishing
- In attesa di esecuzione del payload

- Analisi dei flussi di comunicazione tramite il tool WinDump e il SIEM QRadar
- Dotarsi di Antivirus/Antimalware aggiornati

EXPLOITATION

- Esecuzione del payload da parte della vittima
- Acceso remoto alla vittima (Reverse TCP Connection)

- Analisi evento Process Create
- Analisi evento Unusual Process Launched a Command Shell
- Analisi evento Network connection detected

INSTALLATION

- Privilege Escalation: bypass del Controllo Account Utente
- Accesso permanente: modifica al registro di sistema

- Analisi eventi Process Create, Unusual Process Launched a Command Shell, Network Connection Detected
- Analisi registro di sistema

COMMAND & CONTROL

- Non-standard Port: controllo della vittima tramite comunicazione TCP utilizzando una porta non comune

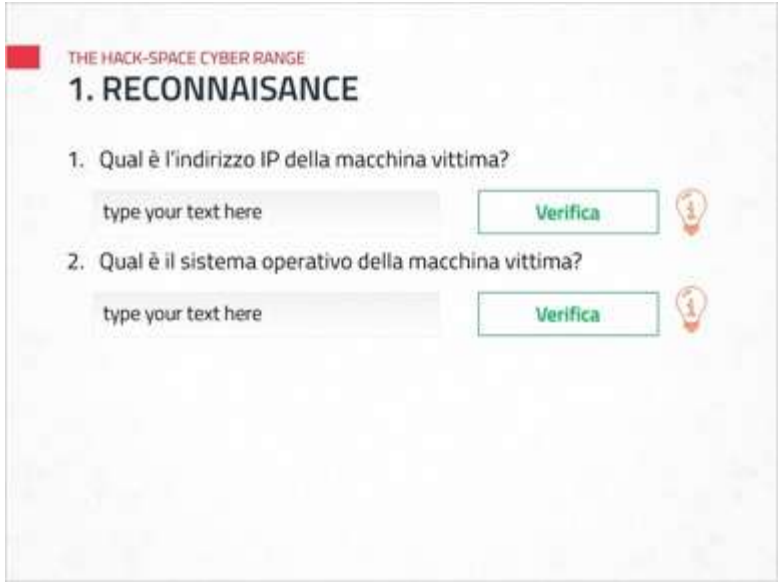
- Analisi dei flussi
- Individuazione di una comunicazione sospetta
- Definizione Regola «Comunicazione sospetta avviata»

ACTIONS ON OBJECTIVES

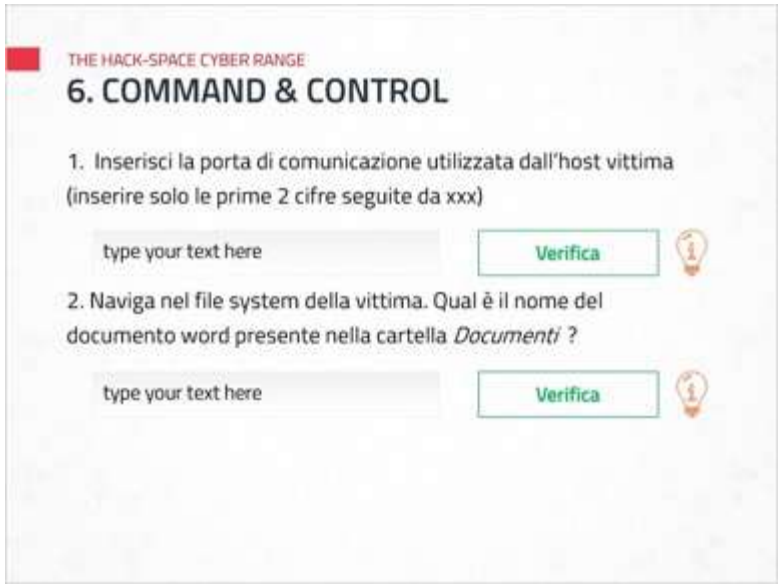
- Estrazione dati critici
- Cifratura dati critici
- Lessons-learned

- Backup dei dati
- Lessons-learned

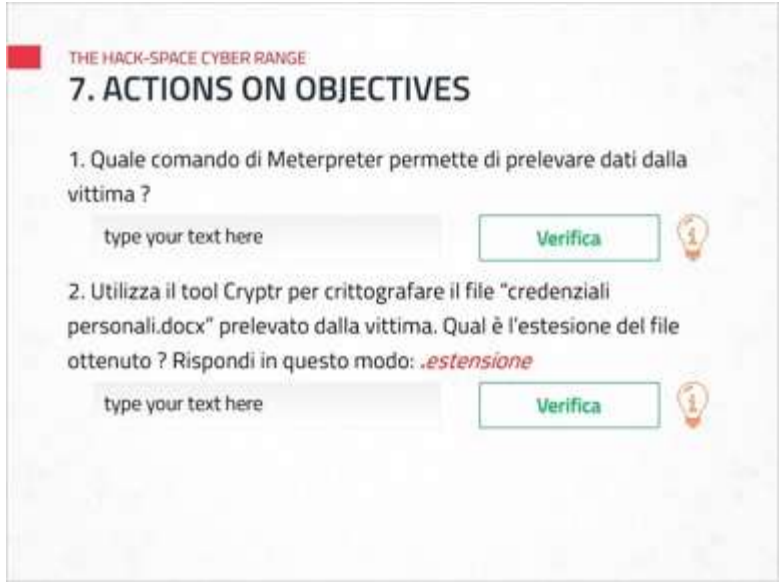
VALUTAZIONE RED TEAM



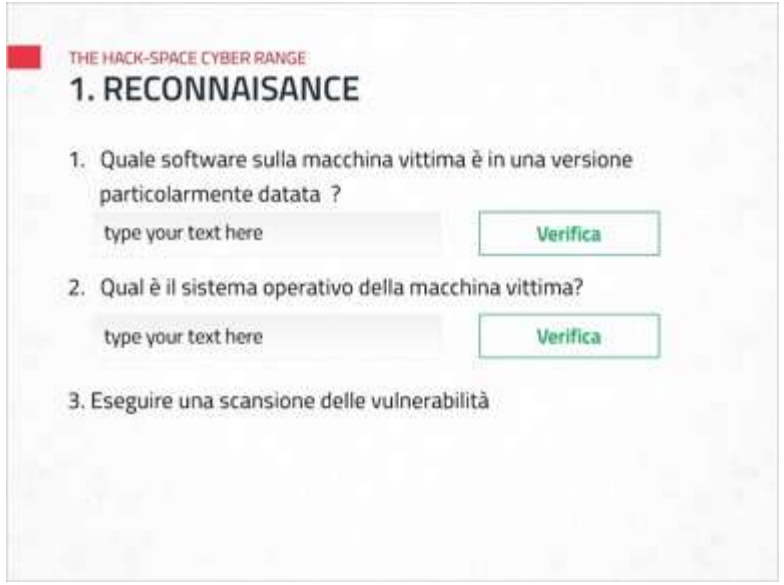
VALUTAZIONE RED TEAM

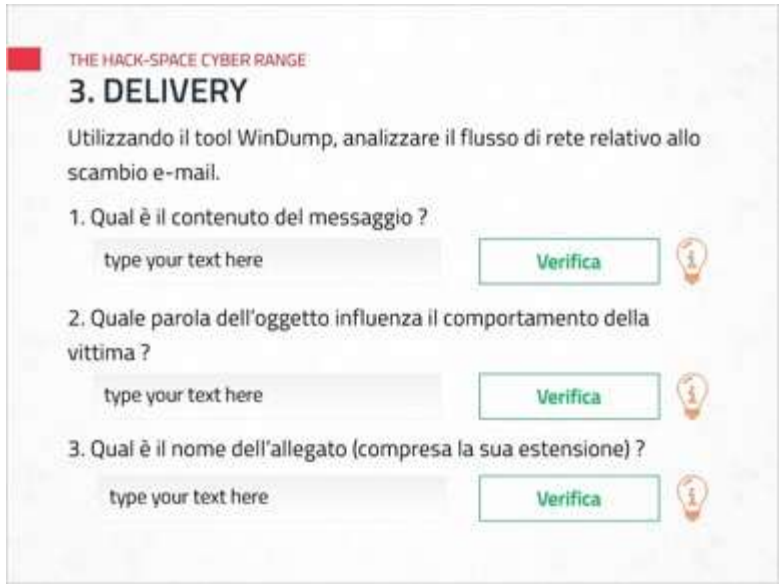


VALUTAZIONE RED TEAM



VALUTAZIONE BLUE TEAM





VALUTAZIONE BLUE TEAM

VALUTAZIONE BLUE TEAM

CONCLUSIONI

- Cyber Range fondamentali per tutte le organizzazioni interessate alla formazione avanzata del proprio personale
- Simulazione di scenari d'attacco efficace alla comprensione di **tattiche**, **tecniche** e **procedure** utilizzate dai malintenzionati per attuare in futuro una corretta attività di *incident response*
- Utilizzo di LMS per la gestione del processo formativo e della valutazione del personale

SVILUPPI FUTURI

- Esecuzione di altre tipologie di esercitazioni
- Progettazione di scenari sempre più variegati, complessi e vicini alla realtà
- Ampliamento dell'infrastruttura virtuale

GRAZIE PER L'ATTENZIONE

Ad Maiora!