



UNIVERSITÀ
DEGLI STUDI DI BARI
ALDO MORO



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

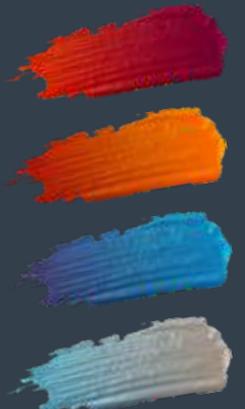
Relatori

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
- ...



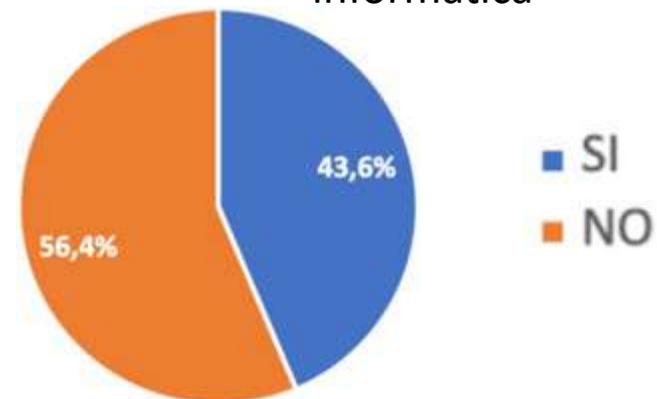
SICUREZZA E FORMAZIONE

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

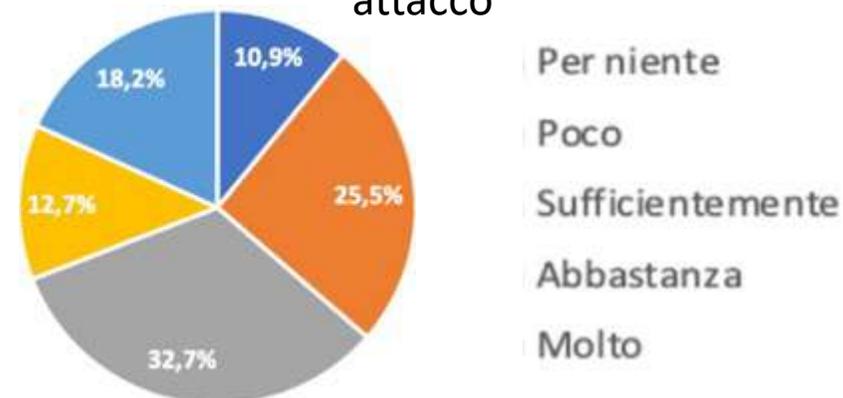
Lo studio condotto **sullo stato della cybersecurity nel Sud Italia**, rileva che il 56,4% di aziende/enti intervistate non offre corsi specifici sulla cybersecurity.

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.

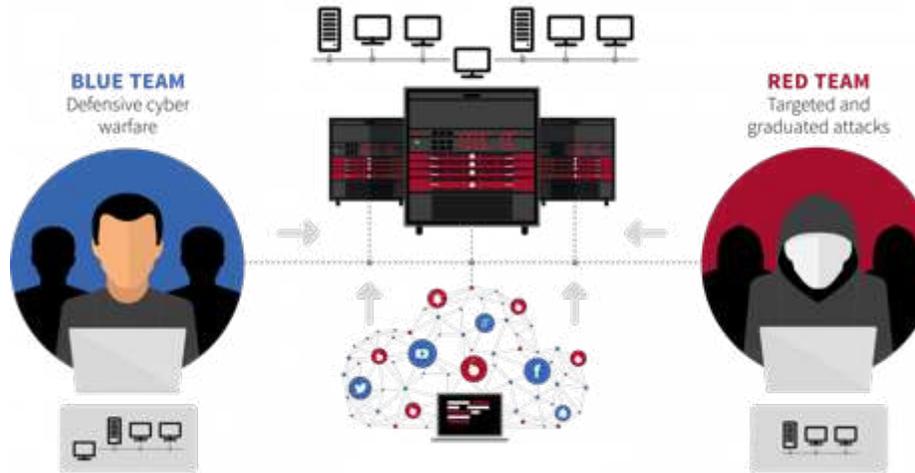
Ripartizione del campione intervistato rispetto all'attività formativa svolta sulla sicurezza informatica



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



SICUREZZA E FORMAZIONE



Monitoring
Monitor progress of testing and assessment enterprise-wide

Qualifications

Ensure all employees have the required qualifications

Training

Manage training activities across the organization



Courses

Integrate 3rd party courses or design your own

Administration

Manage and collect test scores and other records

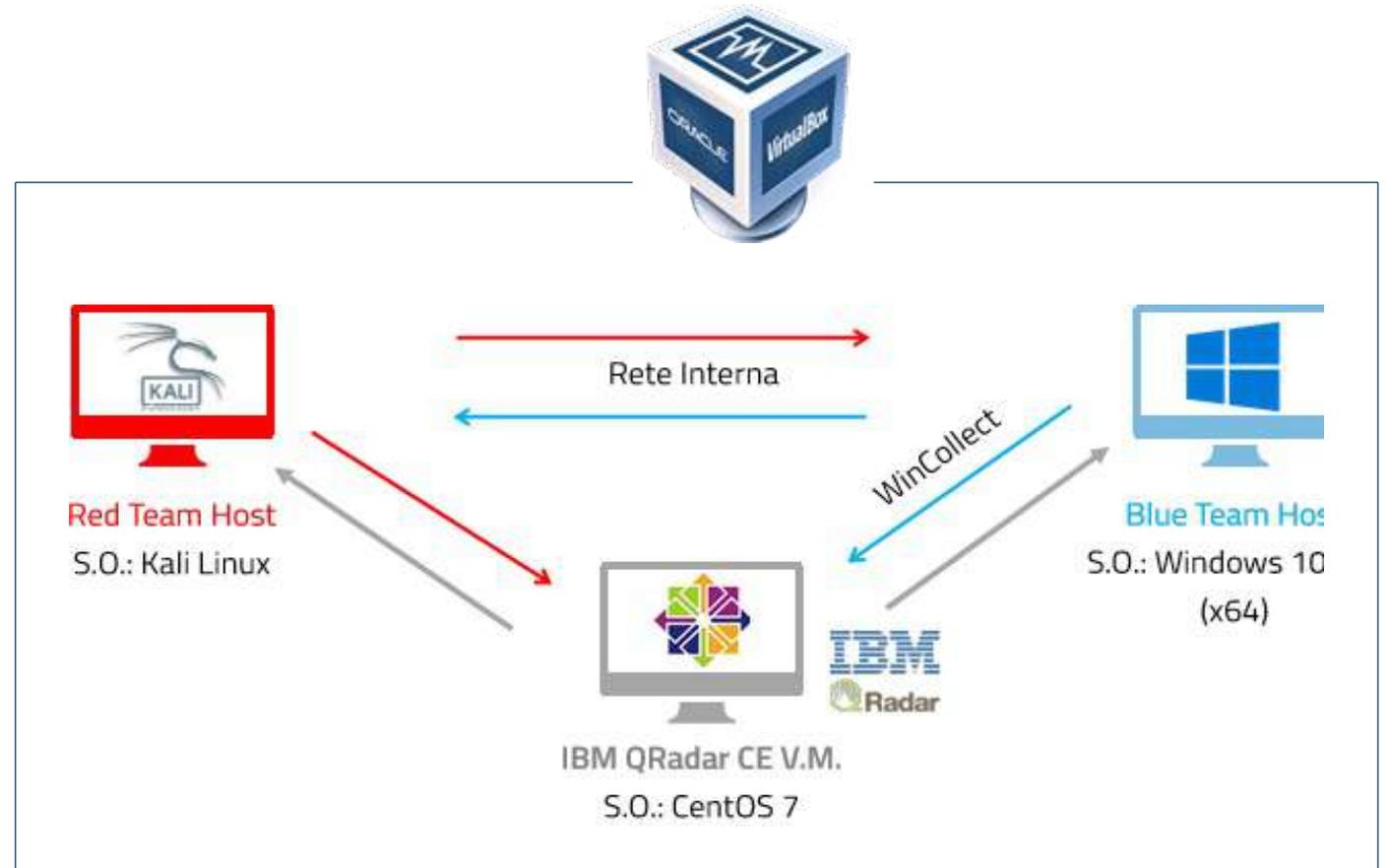


THE HACK-SPACE CYBER RANGE

Ambiente virtuale creato con il software Oracle VM VirtualBox

3 Host

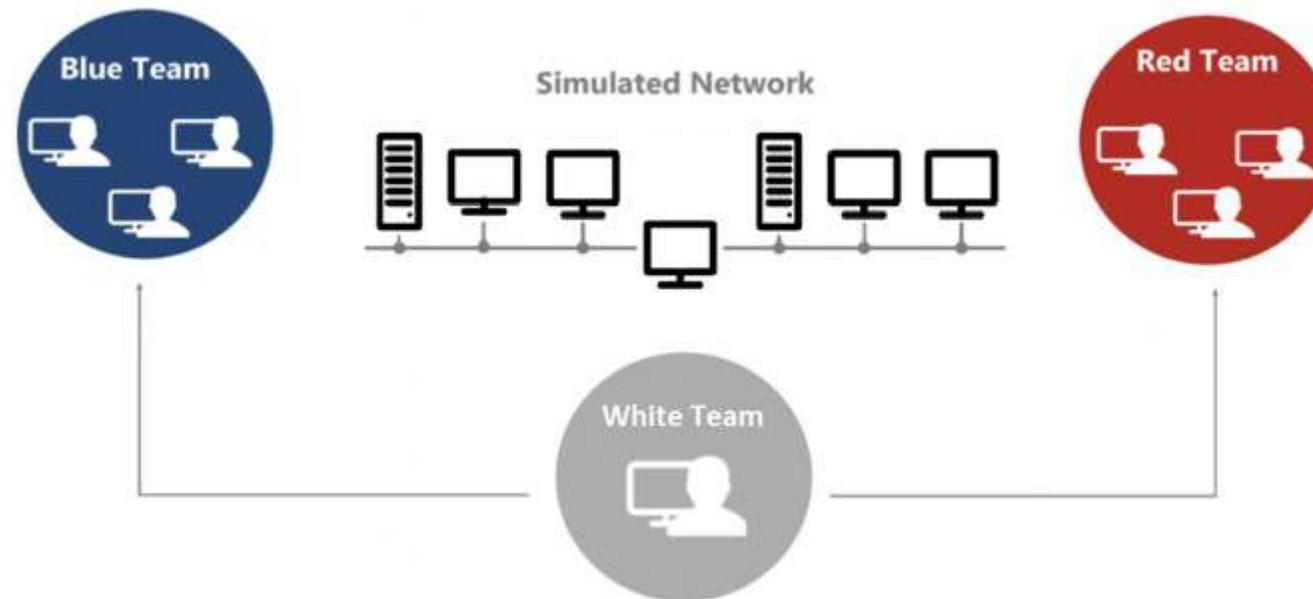
- Red Team Host
- Blue Team Host
- IBM Qradar CE V.M.



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: orchestra 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



UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO The Hack-Space Cyber Range

Home Dashboard Eventi i miei corsi Nel corso

Nascondi blocchi Schermi

I miei corsi > The Hack-Space Cyber Range

Annunci

Configurazione ambiente

- Configurazione ambiente

Cyber Kill Chain

- Cyber Kill Chain

Valutazione Red Team vs Blue Team

- Esercitazione Red Team
- Esercitazione Blue Team

Navigazione

Amministrazione



MATERIALE DIDATTICO CYBER KILL CHAIN

 UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

 SERLAB
Software Engineering Research

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

CYBER KILL CHAIN ESECUZIONE DI UN ATTACCO INFORMatico

PROCEDI →

Francesco Moramarco
Informatica e Tecnologie per la Produzione del Software
A.A. 2019/2020

THE HACK-SPACE CYBER RANGE

CYBER KILL CHAIN

- La **Cyber Kill Chain** è un modello costituito da sette fasi che identifica cosa i malintenzionati devono fare per realizzare un attacco informatico.
- Si tratta di un framework sviluppato da **Lockheed Martin**, facente parte del modello di *Intelligence Driven Defense* per l'identificazione e prevenzione di attività di cyber intrusione.
- Dunque, aiuta a comprendere in anticipo le possibili azioni di un malintenzionato, in modo da cogliere i segnali di un attacco e utilizzare gli strumenti di sicurezza necessari per la difesa dei perimetri aziendali.

THE HACK-SPACE CYBER RANGE

CYBER KILL CHAIN - FASI

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions On Objectives



With "stealthy" malware, attackers accomplish their original goal.

THE HACK-SPACE CYBER RANGE

1. RECONNAISSANCE

I malintenzionati sono nella **fase di pianificazione** della loro operazione. Conducono ricerche per capire **quali target** consentiranno loro di raggiungere l'obiettivo.

- Ricerca di indirizzi e-mail;
- Identificazione dei dipendenti di una organizzazione sui social media;
- Individuazione di server connessi a internet.



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 attaccante 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



STRUMENTI UTILIZZATI – RED TEAM



Metasploit Framework

Raccolta di moduli exploit e payload per eseguire un attacco



NMAP

Nmap

Port scanner
Individuazione punti deboli



STRUMENTI UTILIZZATI – BLUE TEAM



IBM Qradar

Security Information and Event
Management



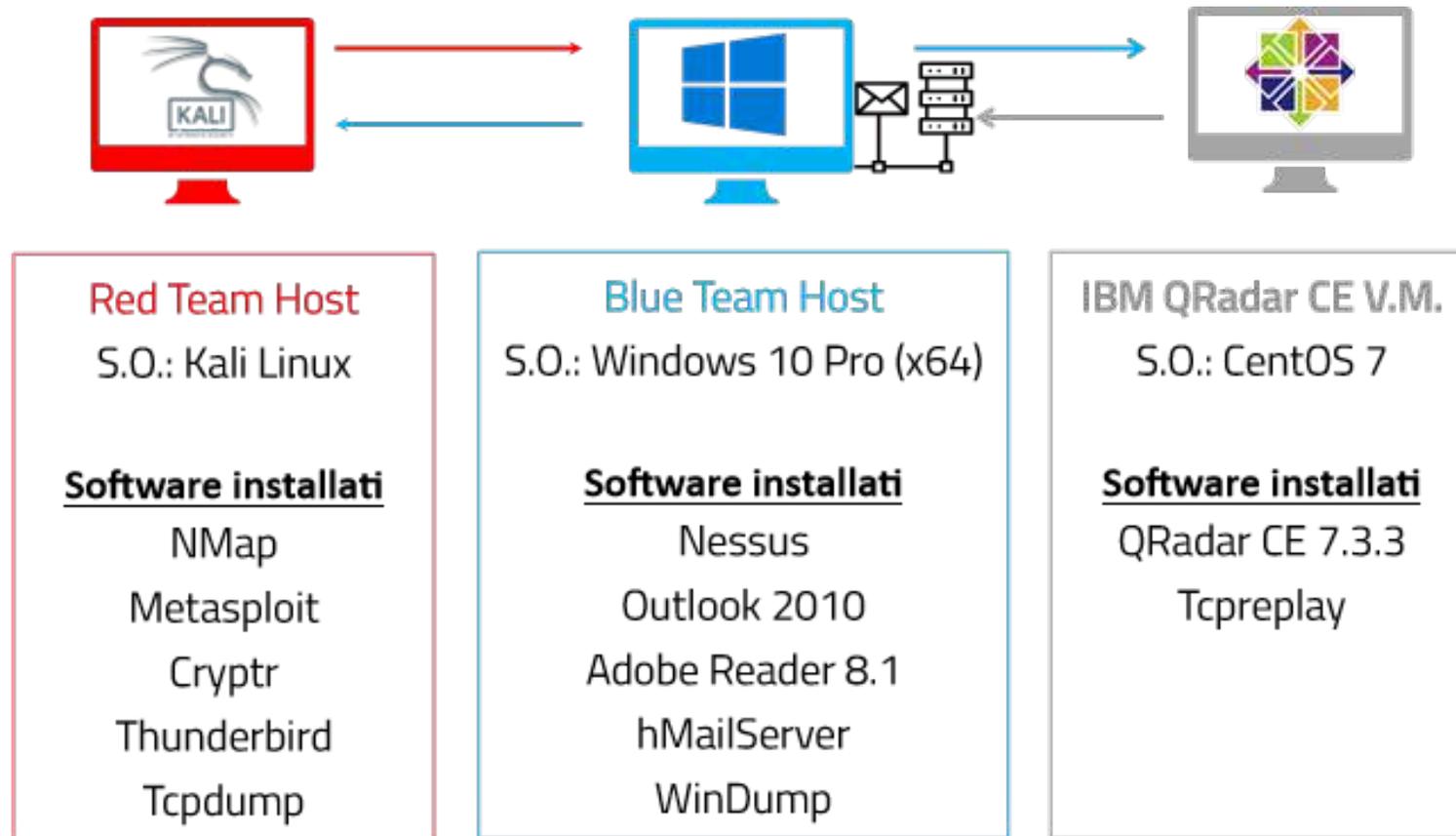
Nessus Essentials

Vulnerability scanner



CONFIGURAZIONE CYBER RANGE

14





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

17



- 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

18



- 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

19



- 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

20



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



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



INSTALLATION

21



- 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



THE HACK-SPACE CYBER RANGE

AVVIO ESERCITAZIONE DI RED TEAMING

PROCEDI →

Ricorda che una volta avviata l'esercitazione, non potrai più tornare indietro. Buona lavoro!

THE HACK-SPACE CYBER RANGE

1. RECONNAISSANCE

1. Qual è l'indirizzo IP della macchina vittima?
 
2. Qual è il sistema operativo della macchina vittima?
 

THE HACK-SPACE CYBER RANGE

2. WEAPONIZATION

1. Quale exploit consente di generare un file pdf da utilizzare per un attacco di Ingegneria Sociale ?
 
2. Quale payload consente di stabilire una Reverse TCP Connection?
 
3. Quale comando mostra le opzioni configurabili di exploit e payload?
 
4. Inserisci il valore corretto da assegnare al parametro LHOST
 

THE HACK-SPACE CYBER RANGE

3. DELIVERY

Invia una mail di Phishing, con il documento PDF generato allegato, all'indirizzo esempio@azienda.it.
Utilizza il client email configurato sulla macchina.
Scrivi qui il contenuto della mail.

VALUTAZIONE RED TEAM

THE HACK-SPACE CYBER RANGE

4. EXPLOITATION

1. Quale modulo di Metasploit occorre utilizzare per mettersi in ascolto della vittima ?
type your text here 
2. Quale payload è necessario impostare ?
type your text here 
3. Cosa viene mostrato nella shell una volta stabilita la connessione con la vittima ?
type your text here 

THE HACK-SPACE CYBER RANGE

5. INSTALLATION

1. Quale modulo exploit permette di bypassare l'UAC di Windows? Visualizzane le informazioni con il comando *info*
type your text here 
2. Dopo aver impostato il payload, digita il comando show options. Escludendo i parametri LHOST e LPORT, quali altri parametri sono da configurare?
type your text here 
3. Selezionata la nuova sessione, esegui i comandi *getsystem* e *getuid* di Meterpreter. Cosa restituisce quest'ultimo ?
type your text here 

THE HACK-SPACE CYBER RANGE

5. INSTALLATION

4. Con quale modulo di Metasploit si realizza l'accesso permanente tramite modifica alle chiavi di registro ?
type your text here 
5. Dove verrà inserita la nuova chiave di registro se il parametro STARTUP è impostato su SYSTEM ?
type your text here 
6. Quale parametro è possibile modificare per assegnare un nome specifico alla nuova chiave di registro ?
type your text here 

THE HACK-SPACE CYBER RANGE

6. COMMAND & CONTROL

1. Inserisci la porta di comunicazione utilizzata dall'host vittima (inserire solo le prime 2 cifre seguite da xxx)
type your text here 
2. Naviga nel file system della vittima. Qual è il nome del documento word presente nella cartella *Documenti* ?
type your text here 

VALUTAZIONE RED TEAM

THE HACK-SPACE CYBER RANGE

7. ACTIONS ON OBJECTIVES

1. Quale comando di Meterpreter permette di prelevare dati dalla vittima ?
 [Verifica](#)
2. Utilizza il tool Cryptr per crittografare il file "credenziali personali.docx" prelevato dalla vittima. Qual è l'estensione del file ottenuto ? Rispondi in questo modo: *.estensione*
 [Verifica](#)

THE HACK-SPACE CYBER RANGE

ESERCITAZIONE COMPLETATA

RISULTATO

Your Score: 62.5%

Passing Score: 80%

You did not pass.

[Rivedi](#) [Stampa](#) [Riprova](#)

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SERLAB
Software Engineering Research

GRAZIE PER LA PARTECIPAZIONE

ESERCITAZIONE TERMINATA

Se lo desideri, puoi ripetere il corso cliccando il pulsante sottostante.

[RIPETI](#) →

Francesco Moramarco
Informatica e Tecnologie per la Produzione del Software
A.A. 2019/2020

VALUTAZIONE BLUE TEAM



THE HACK-SPACE CYBER RANGE

AVVIO ESERCITAZIONE DI BLUE TEAMING

PROCEDI! →

Ricorda che una volta avviata l'esercitazione non potrai più tornare indietro. Buon lavoro!

THE HACK-SPACE CYBER RANGE

1. RECONNAISSANCE

1. Quale software sulla macchina vittima è in una versione particolarmente datata ?
2. Qual è il sistema operativo della macchina vittima?
3. Eseguire una scansione delle vulnerabilità

THE HACK-SPACE CYBER RANGE

2. WEAPONIZATION

1. Quale sito è buona norma consultare per essere aggiornati sulle ultime vulnerabilità scoperte ?
 
2. All'apertura del documento ricevuto, una schermata di dialogo richiede di premere il pulsante *apri* per visualizzare il messaggio criptato. Quale vulnerabilità di Adobe Reader è stata sfruttata ? Indicarne il CVE-ID
 

THE HACK-SPACE CYBER RANGE

3. DELIVERY

Utilizzando il tool WinDump, analizzare il flusso di rete relativo allo scambio e-mail.

1. Qual è il contenuto del messaggio ?
 
2. Quale parola dell'oggetto influenza il comportamento della vittima ?
 
3. Qual è il nome dell'allegato (compresa la sua estensione) ?
 

VALUTAZIONE BLUE TEAM

THE HACK-SPACE CYBER RANGE

4. EXPLOITATION

Analizzare gli eventi rilevati dal SIEM IBM QRadar.

1. Qual è il nome del processo avviato da Adobe Reader ?
type your text here 
2. Qual è il messaggio contenuto nella finestra di dialogo menzionato nella fase di Weaponization ?
type your text here 
3. Sotto quale nome si nasconde il payload ?
type your text here 

THE HACK-SPACE CYBER RANGE

5. INSTALLATION

Analizzare gli eventi rilevati dal SIEM IBM QRadar.

1. Quale processo di Windows è stato sfruttato per ottenere i permessi di amministratore ?
type your text here 
2. Quale processo, sfruttando la vulnerabilità della domanda precedente, viene avviato per modificare il registro di sistema ?
type your text here 
3. Quale nuova chiave di registro viene creata ?
type your text here 

THE HACK-SPACE CYBER RANGE

5. INSTALLATION

4. Sotto quale nome viene eseguito il payload questa volta ?
type your text here 
5. Analizzare il registro di sistema del computer vittima. Quale chiave di registro è stata modificata per la persistenza ?
type your text here 
6. Analizzare le connessioni instaurate dal computer vittima. Quale risulta sospetta ? Riportare il valore *indirizzo esterno*
type your text here 

THE HACK-SPACE CYBER RANGE

6. COMMAND & CONTROL

1. Inserisci la porta di comunicazione utilizzata dall'host vittima (inserire solo le prime 2 cifre seguite da xxx)
type your text here 
2. Inserisci la porta di comunicazione utilizzata dall'attaccante
type your text here 

VALUTAZIONE BLUE TEAM

THE HACK-SPACE CYBER RANGE

7. ACTIONS ON OBJECTIVES

1. Quale mitigazione propone il MITRE ATT&CK contro il Data Encrypted for Impact ?

THE HACK-SPACE CYBER RANGE

ESERCITAZIONE COMPLETATA

RISULTATO		
Your Score:	62.5%	
Passing Score:	80%	
You did not pass.		
Rivedi	Stampa	Riprova

UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

SERLAB
Software Engineering Research

GRAZIE PER LA PARTECIPAZIONE

ESERCITAZIONE TERMINATA

Se lo desideri, puoi ripetere il corso cliccando il pulsante sottostante.

Francesco Moramarco
Informatica e Tecnologie per la Produzione del Software
A.A. 2019/2020

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!