Cyber Security - Planning

Andrea Esposito, Alessandro Annese, Graziano Montanaro

2 dicembre 2019

Indice

1 Il gruppo

Dettagli da inviare a: vita.barletta@uniba.it

Tabella 1: Gli studenti componenti del gruppo per il caso di studio di Sicurezza Informatica. In grassetto è riportato il referente del gruppo.

Nome e Cognome	Matricola	E-Mail
Andrea Esposito	**677021**	**a.esposito39@studenti.uniba.it**
Graziano Montanaro	677909	g.montanaro16@studenti.uniba.it
Alessandro Annese	676964	a.annese23@studenti.uniba.it

2 Lo scenario

Si vuole effettuare un furto di materiale sensibili (file) da un laptop Windows (a cui si ha accesso fisico). Si sa per certo che vi sono periodicamente delle riunioni aziendali (durante cui il laptop è utilizzato), di cui si vuole ottenere una registrazione audio.

3 La killchain

La seguente possibile killchain è stata costruita seguendo la matrice MITRE ATT&CK. L'elenco puntato contiene link alla descrizione delle *entry* sul sito MITRE ATT&CK.

Red Team		Blue Team
Utilizzo di `nmap` per individuare l'OS e le porte target. Uso di Social Engineering per definire le mail	**Reconnaisance**	
Utilizzo di un file PDF infetto	**Weaponization**	Utilizzo di un Antivirus
Invio di una mail con allegati malevoli	**Delivery**	Verifica della correttezza e della certificazione del mittente
Creazione di un servizio e attivazione del microfono	**Exploit**	Non avviare il file come amministratoreq
Creazione di un servizio	**Installation**	Verifica dei servizi attii

Red Team		Blue Team
Scoperta delle directory e attivazione del microfono	**Command & Control**	Non avere cartelle o file sensibili non protetti
Invio dei file in rete	**Action**	Eliminare la connettività di rete, uso di un firewall a livello di router

1. Initial Access
   - Replication Through Removable Media
2. Execution
   - Command Line Interface
   - Powershell
3. Persistence
   - File System Permissions Weakness
   - Hidden Files and Directories
4. Privilege Escalation
   - File System Permissions Weakness
   - New Service
5. Defense Evasion
   - Binary Padding
6. Credential Access
   - Input Capture
7. Discovery
   - File and Directory Discovery
8. Lateral Movement
   - Replication Through Removable Media
9. Collection
   - Audio Capture
   - Data from Local System
   - Screen Capture
   - Video Capture
10. Command and Control
    - Communication Through Removable Media
11. Exfiltration
    - Exfiltration Over Alternative Protocol
    - Exfiltration Over Physical Medium
12. Impact
    - Data Destruction
    - Data Encrypted for Impact