Penetration Testing Narrative

Giorgio Colella (0522501752)
A.A. 2024/2025

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Contents

1 Target Scoping

- **Obiettivo**: Definire i confini del test modellando una rete aziendale fittizia in CyberBattleSim e individuando gli asset critici (host, servizi e vulnerabilità simulate).
- **Strumenti**: Modulo dei requisiti e esempi di CyberBattleSim.
- **Output**: diagramma di rete con 15 nodi e vulnerabilità definite ed approccio Black Box.

2 Information Gathering

- **Obiettivo**: Raccolta di dati dalla rete per cercare di capire la sua infrastruttura, azione compiuta dall'agente.
- **Strumenti**: codice sorgente di CyberBattleSim e Reinforcement Learning, azione LeakedNodeId dell'agente.
- **Output**: Topologia di rete con host e collegamenti.

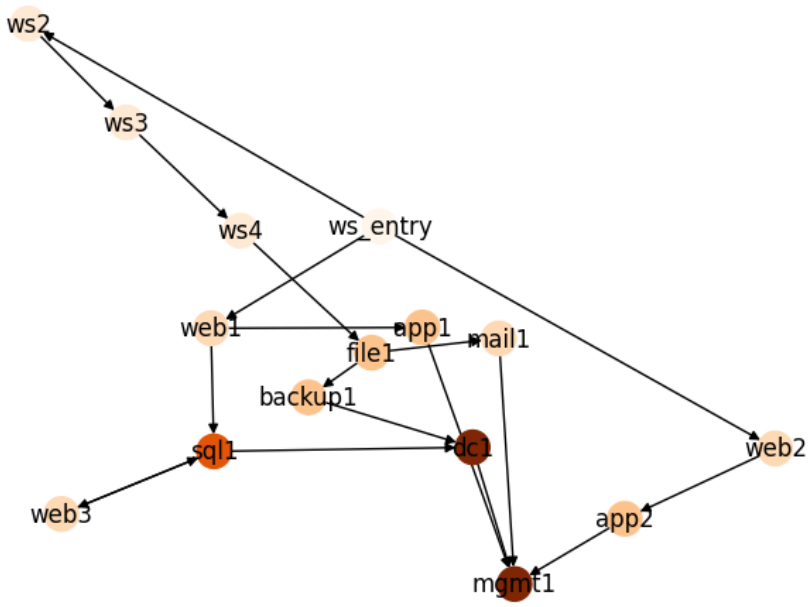

Figure 1: Topologia della rete

3 Target Discovery

- **Obiettivo**: Identificare gli host attivi e raggiungibili tramite scanning.
- **Strumenti**: codice sorgente di CyberBattleSim e Reinforcement Learning.
- **Output**: Lista degli 11 host attivi con subnet corrispondenti e prime informazioni di routing.

- **Note**: Log di DiscoverRemoteSystems per ciascuna subnet, confermando l'individuazione di web1, file1, app1, app2, backup1, sql1, mail1, dc1, mgmt1, web3, ws_entry.

4 Enumerating Target

- **Obiettivo**: Scoprire servizi e versioni sui nodi identificati.
- **Strumenti**: codice sorgente di CyberBattleSim e Reinforcement Learning.
- **Output**: Tabella dei servizi (HTTP, SMB, SSH, SQL, RDP, SMTP e GIT) e delle vulnerabilità associate (come SMBWeakShare, WebAdminCreds, SQLi e cosi via).

5 Vulnerability Mapping

- **Obiettivo**: Individuare ciascuna vulnerabilità nota ed associarla ad i diversi host attivi.
- **Strumenti**: codice sorgente di CyberBattleSim e Reinforcement Learning.
- **Output**: Tabella dei servizi (HTTP, SMB, SSH, SQL, RDP, SMTP e GIT) e delle vulnerabilità associate (come SMBWeakShare, WebAdminCreds, SQLi e cosi via). Individuazione di 25 vulnerabilità con gravità da Low a Critical.

Nodo	**OS**	**Servizi aperti**	**Vulnerabilità**
ws_entry	Linux		WeakAdmin
web1	Linux	HTTP, GIT	WebExploit, WebAdminCreds, GitHistory, GitSMBCreds
file1	Windows	SMB	SMBWeakShare, SMBCreds
app2	Linux	SSH	App2APIExploit, App2FileCreds, App2PrivEsc
app1	Linux	SSH	App1PrivEsc, App1DBCreds
backup1	Windows	SMB	BackupExploit, BackupSQLCreds
sql1	Windows	SQL	SQLi, SQLiCreds, SQLiDataBreach
mail1	Linux	SMTP	MailLeak, MailLeakCreds
dc1	Windows	RDP	RDPBrute, RDPBruteCreds, WeakAdmin
mgmt1	Linux	SSH	MgmtExploit, MgmtCreds
web3	Windows	HTTP	Web3SSRF, Web3BackupCreds

6 Target Exploitation

- **Obiettivo**: Verificare l'effettivo sfruttamento di ciascuna vulnerabilità e l'impatto sul sistema.
- **Strumenti**: Azioni ExploitRemoteService, LeakedCredentials, SystemEscalation e cosi via dell'agente RL.
- **Output**: Conferma di compromissione di 11/15 host, con esfiltrazione credenziali, escalation a root/ADMIN e takeover del Domain Controller (dc1) tramite RDPBrute e WebAdminCreds. Log di exploit riusciti (es. "Backup server SMB root password leaked", "Privilege escalation on app1").

7 Post-Exploitation

- **Obiettivo**: Valutare possibili movimenti laterali, privilege escalation e persistenza dopo l'exploit iniziale.
- **Strumenti**: Azioni LateralMove, PrivilegeEscalation, AdminEscalation e SystemEscalation dell'agente RL.
- **Output**: Movimenti laterali ed elevazione dei privilegi.
- **Note: non è possibile ottenere persistenza tramite backdoor e si rende quindi necessaria l'attesa dell'aggiunta di questa funzione all'interno di CyberBattleSim.**

8 Reporting

- **Obiettivo**: Produrre il documento tecnico finale, completo di tabelle, grafici e raccomandazioni.
- **Strumenti**: LaTeX per stesura, screenshot di Kali, e matplotlib per diagrammi di topologia e grafi.
- **Output**: Report in PDF con: Executive Summary, Engagement Highlights, Vulnerability Report, Findings Summary, Remediation Recommendations e cosi via.

9 Appendice

Nel Reporting sarà presenta anche la sperimentazione ed il confronto di **CyberBattleSim** con **CybORG**, **NetworkAttackSimulation** e **Infection Monkey**.