Vulnerability Assessment

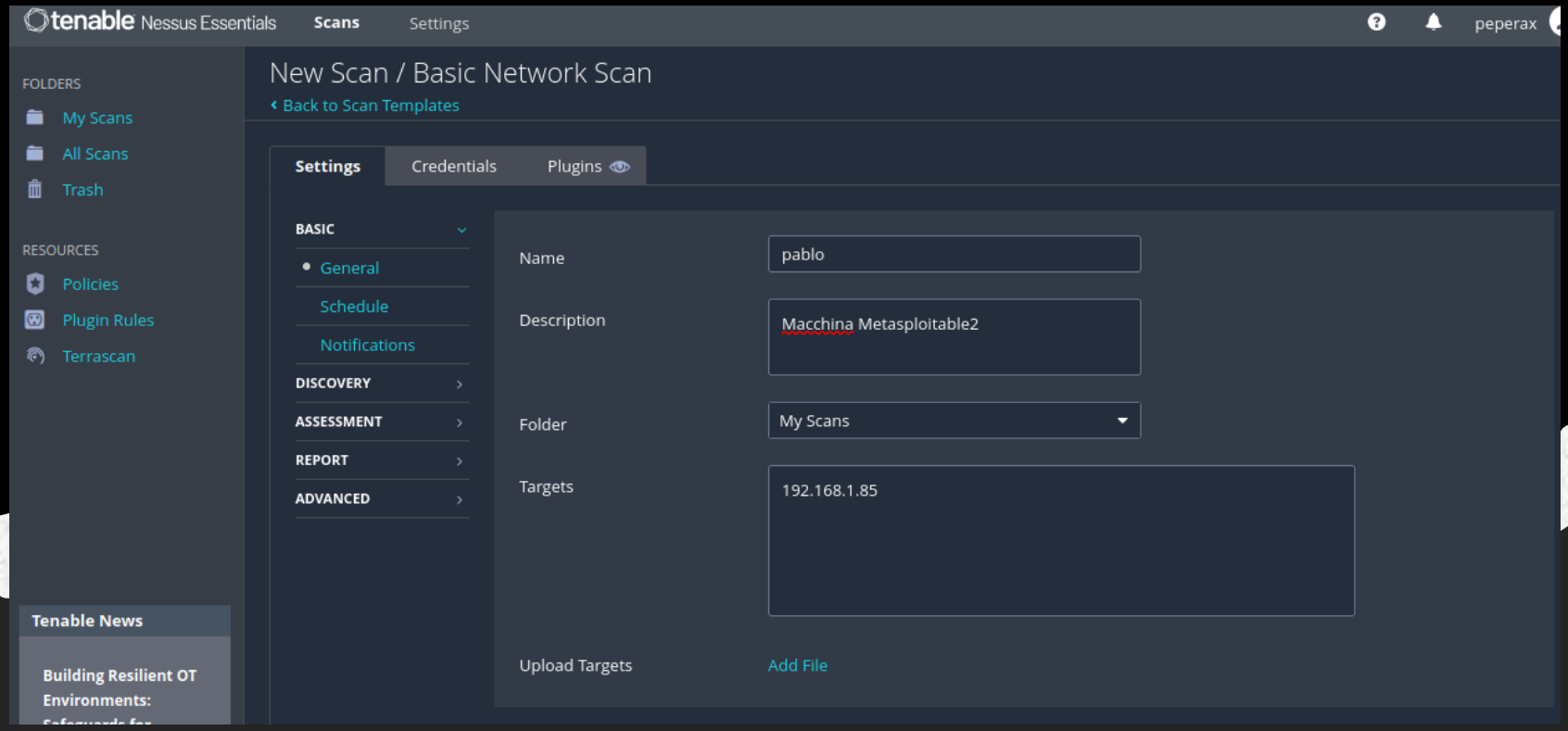
Pablo Andres Balbuena Rios

Esercizio 4
Settimana 5

Lìesercizio è di effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo). A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web. Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Effettuare un Vulnerability Assessment



metasploit®

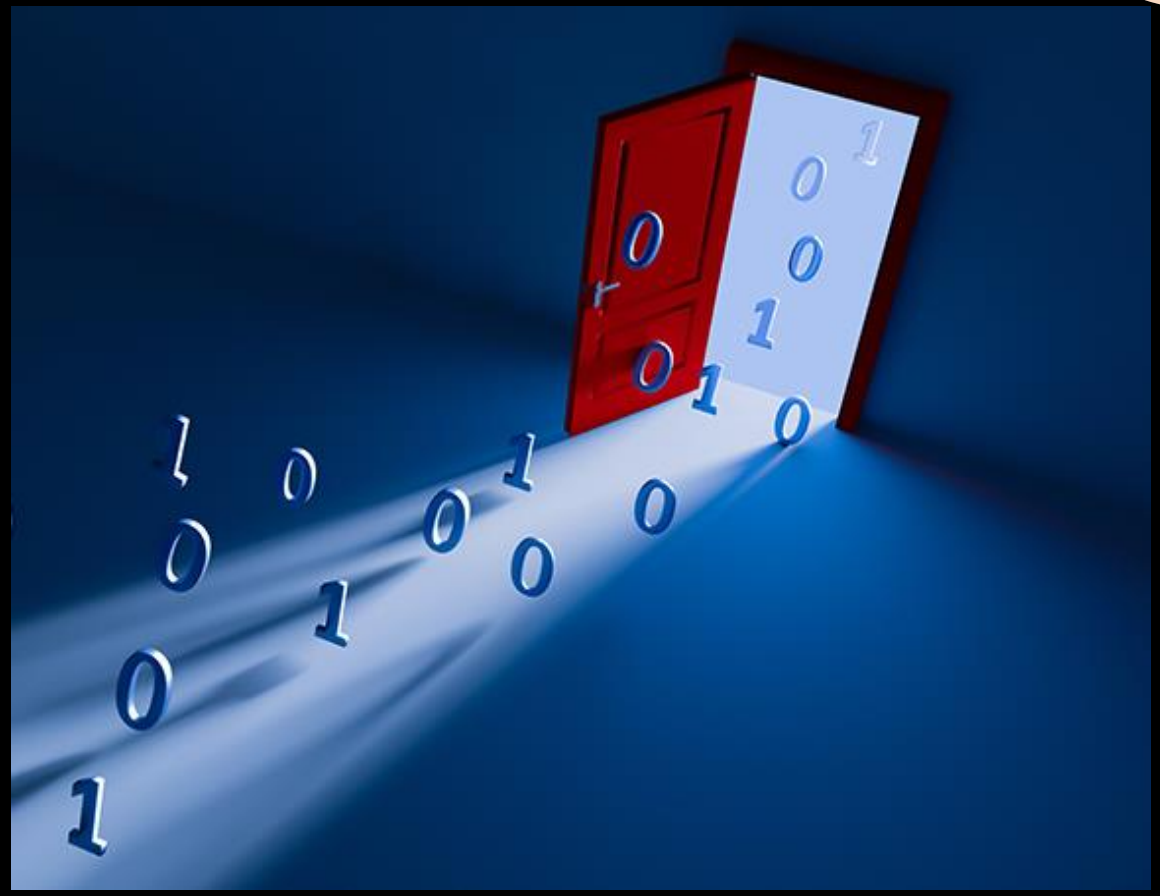
Report Macchina Metasploitable2

Report

Protocollo: UnrealIRCd Backdoor Detection

CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection

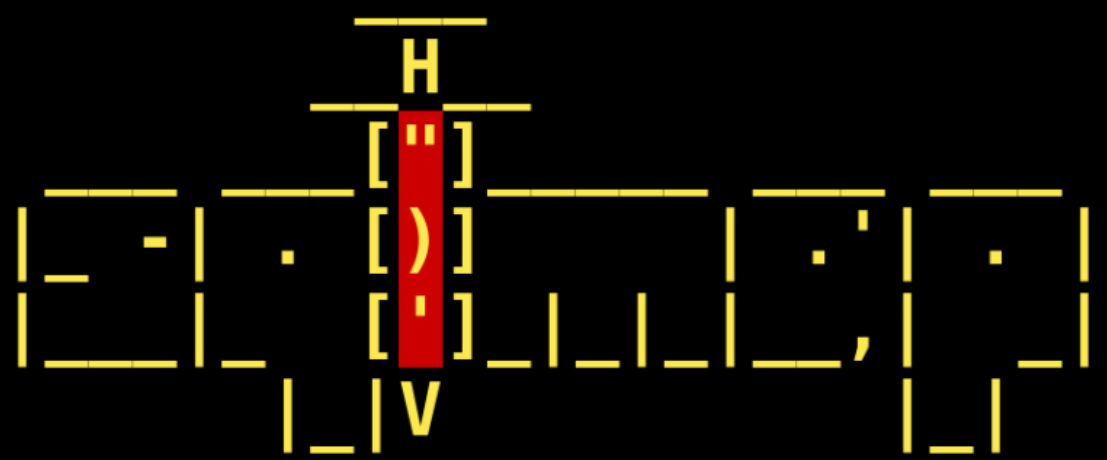
Questo protocollo è stato utilizzato come backdoor, per poter entrare dentro la macchina.



```
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
```

Protocollo: Apache Tomcat AJP Connector Request Injection

Il protocollo consente ad una persona di leggere o caricare file nel server.



CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)

Protocollo: HTTP TRACE / TRACK Methods Allowed

Questo protocollo indica che il sito è stato richiesto con l'intestazione del dominio, ma la risposta HTTP contiene informazioni sul nome del server. Questo consente agli utenti malintenzionati di vedere il nome host originale e il nome dell'istanza AEM.