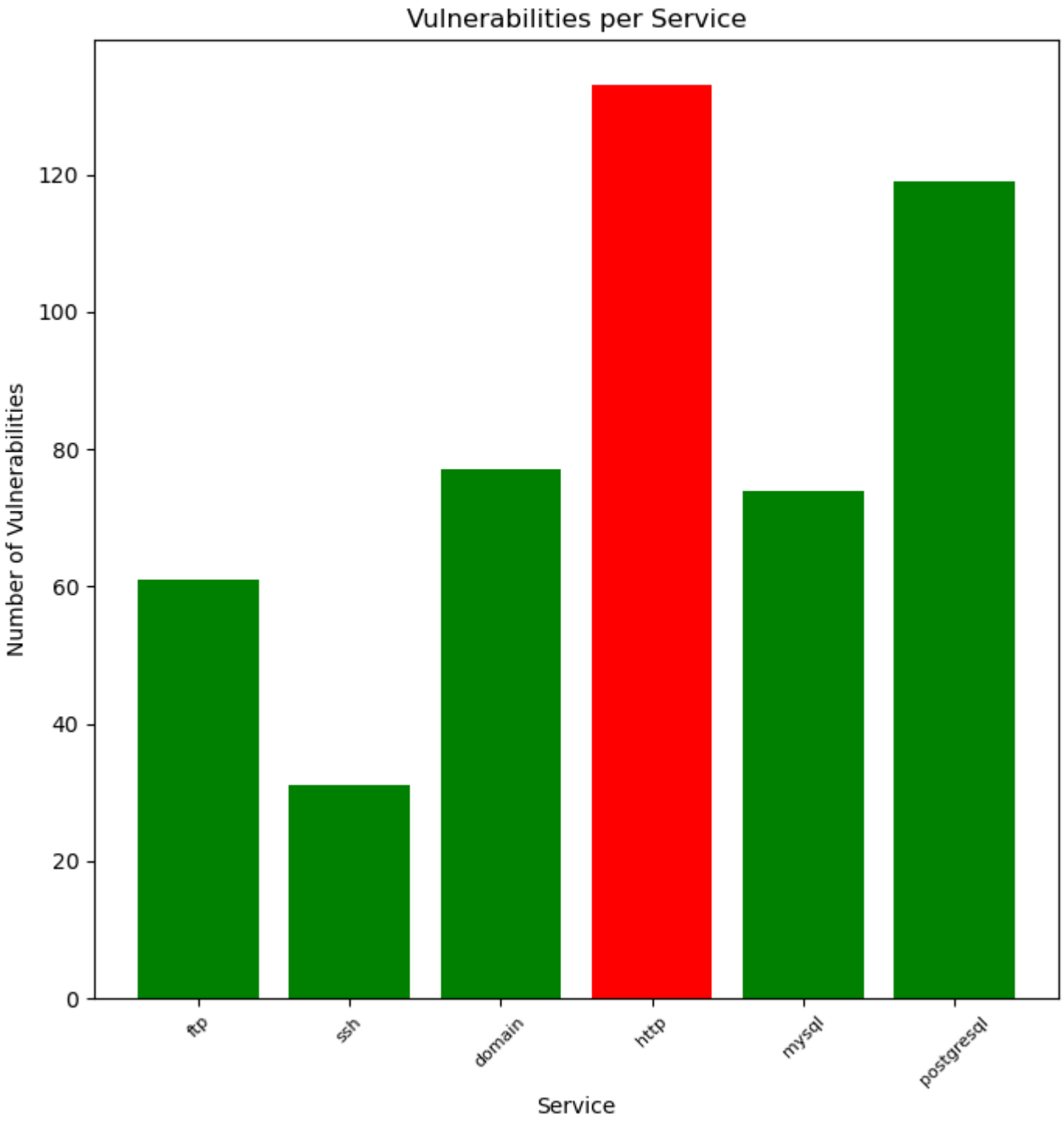
Rapport du : 16/05/2024

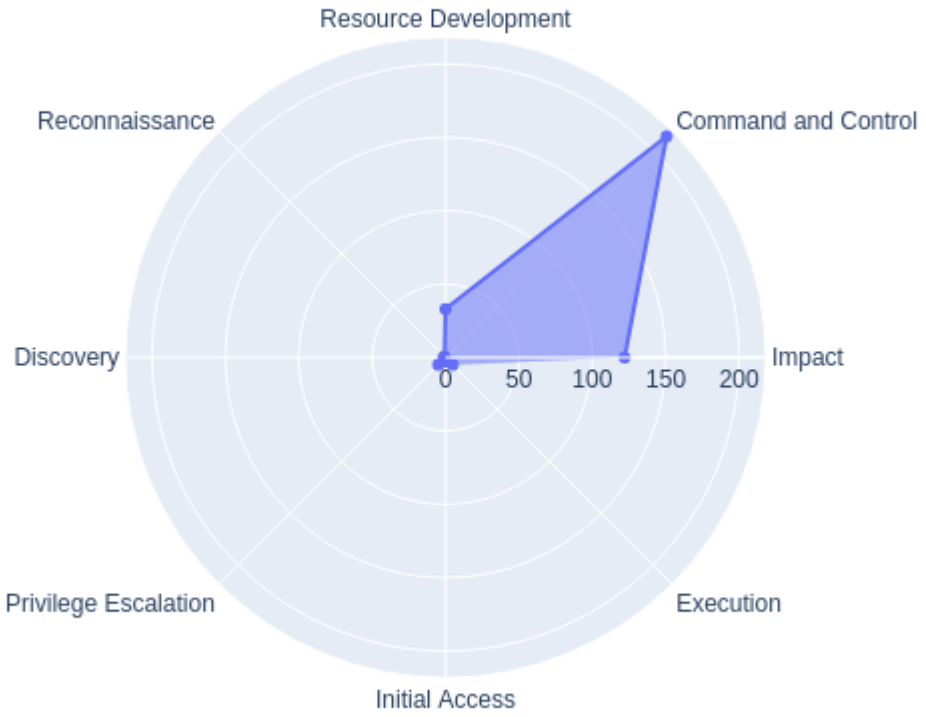
Nom de Session : clabonne3

REPORT VANGUARD TOOLBOX

Une analyse complète d
sécurité informatique


Vulnerabilities per Service
Number of Vulnerabilities
0
20
40
60
80
100
120
ftp
ssh
domain
http
mysql
postgresql
Service

MITRE&ATTACK



HOST VULNERABILITY REPORT

Scan de vulnérabilité réalisé sur la target : 192.168.0.28

Name	Information
Total de vulnérabilités trouvées	495
Total d'exploit disponible	167
Nombre total de ports ouverts	8

Détails des vulnérabilités par port :

Port Number	Number of Vulnerability	Service
21/tcp	3	ftp
22/tcp	31	ssh
53/tcp	77	domain
80/tcp	127	http
2121/tcp	58	ftp
3306/tcp	74	mysql

5432/tcp	119	postgresql
8180/tcp	6	http

Scan Nikto Effectué :

Target ip	Target Port	App Outdated
192.168.0.28	80	True

Rapport Nikto :

Nombre de Directory	Nombre de dossier sensibles	Nombre de fichier intéressant	Nombre de fichier de credential
4	4	1	1

Une recherche d'email à été lancé sur la cible avec 1 résultat(s)

Email Scrapper

Email msfdev[at]metasploit.com

Exploit SSH lancé

Target	Port	Technique	Resultat
192.168.0.28	22	BruteForce	True

Les identifiants trouvé par bruteforce sont : username = **msfadmin** et password = **msfadmin**

Le password existe dans des bases de données leaked

Le password est considéré comme faible

Résultat de la Post-Exploitation

Fichiers sensibles sur le système cible

Total de fichiers sensibles	Total de fichiers de clés	Autres fichier sensibles
21	8	13

Il y a un total de **594** applications découvert sur le systeme cible

Il y a un total de **36** utilisateurs découvert sur le systeme cible