Autor: Erick Menezes
Data: 30/11/2025
Versão: 1.0
Repositório: https://www.github.com/erickmnz/recon-simulado

Sumário Executivo

Foi realizada uma avaliação de segurança em um serviço web simulado hospedado em ambiente de laboratório. Durante o exercício foram identificadas múltiplas exposições e más configurações que permitem descoberta de arquivos sensíveis, acesso a FTP público, enumeração de serviços via Nmap, acesso SSH e extração de segredos armazenados em banco de dados. Foram encontradas evidências em `robots.txt`, diretórios de backup e arquivos de configuração que indicam risco de divulgação de dados e credenciais. Recomenda-se correções imediatas em autenticação, controle de acesso e isolamento de serviços.

Objetivo

Avaliar a superfície de ataque do serviço web simulado para identificar exposições, dados sensíveis e vetores de escalonamento de privilégio.

Escopo

Ambiente web simulado contendo serviços web, FTP, SSH e banco de dados em hosts internos identificados na varredura.

Metodologia

- **Ferramentas:** `nmap`, `nikto`, `gobuster`, clientes FTP/SSH, consultas SQL manuais
- **Atividades:** varredura de portas, enumeração de diretórios, leitura de `robots.txt`, conexão FTP, tentativa de SSH, inspeção de arquivos de configuração e extração de segredos do banco de dados
- **Horários relevantes:** varredura iniciada às **20:00**; conexão FTP às **20:17**; acesso SSH às **20:32**

Achados Detalhados

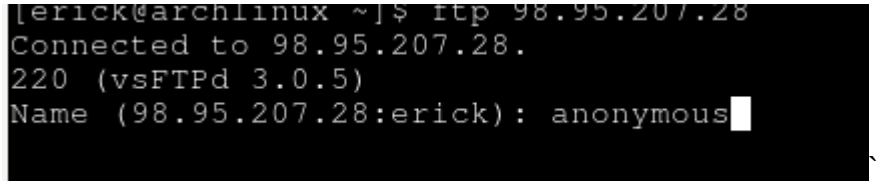
robots.txt e descoberta inicial

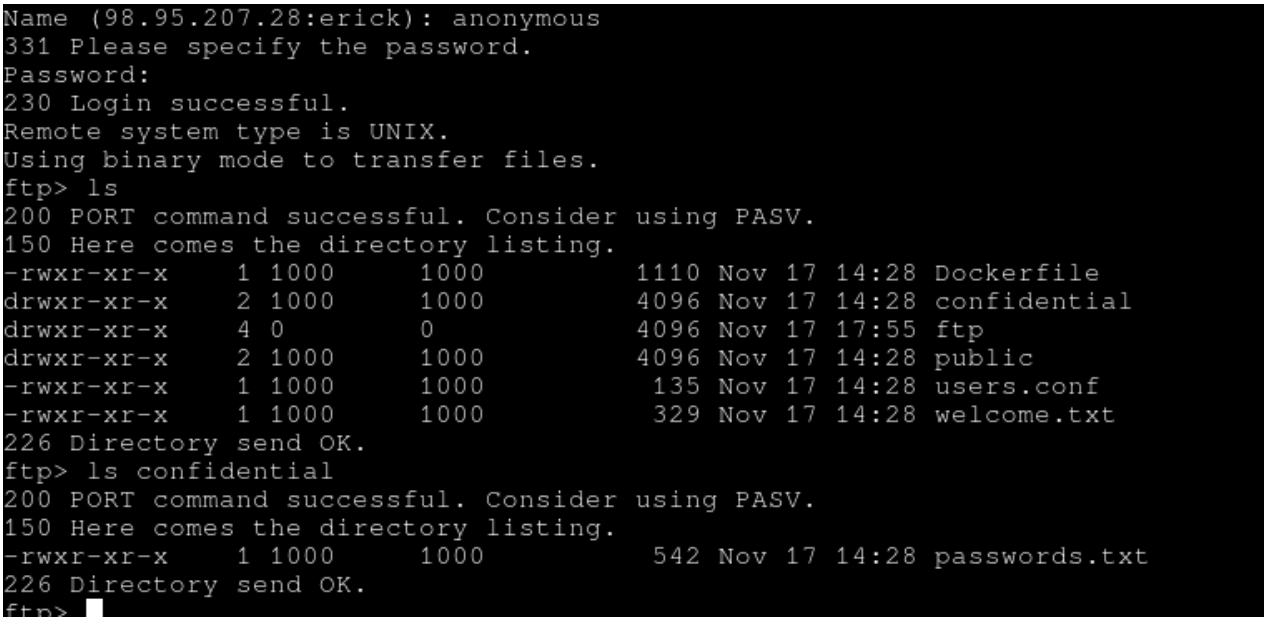
- **Conteúdo relevante encontrado em `robots.txt`:**
  - `Disallow: /admin/`
  - `Disallow: /backup/`
  - `Disallow: /.git/`

- `Disallow: /config/`
- **Flag descoberta:** `FLAG{r0b0ts_txt_l34k4g3}`
- **Observação:** `robots.txt` revela caminhos sensíveis e aponta para arquivo de backup em `/backup/database_backup_2024.sql`.

Serviço FTP

- **Comportamento:** FTP acessível por acesso anônimo; listagem de diretórios disponível
- **Arquivos e diretórios listados:** `Dockerfile`; `confidential/`; `ftp/`; `public/`; `users.conf`; `welcome.txt`
- **Permissões e metadados:** arquivos com permissões `-rwxr-xr-x` e diretórios com proprietário UID 1000 e root em alguns itens
- **Flags e strings encontradas em arquivos de configuração:**
  - `# FLAG{c0nf1g_f1l3_r34d}`
  - `FLAG{p4ssw0rd_f1l3_d1sc0v3ry}`
  - `FLAG{ftp_4n0nym0us_4cc3ss}`
- **Avaliação:** FTP totalmente exposto presença de diretórios `confidential` e `backup` representa risco de vazamento.





```
ftp> ls confidential
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 1000     1000          542 Nov 17 14:28 passwords.txt
226 Directory send OK.
ftp> ls public
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 1000     1000          208 Nov 17 14:28 readme.txt
226 Directory send OK.
ftp> ls ftp
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 17 17:55 confidential
drwxr-xr-x    2 0        0            4096 Nov 17 17:55 public
-rwxr-xr-x    1 0        0             329 Nov 17 17:55 welcome.txt
226 Directory send OK.
ftp>
```

- **Arquivos achados no servidor ftp:**

  users.conf

vsftpd user configuration
FLAG{c0nf1g_f1l3_r34d}

anonymous:password123
ftpadmin:ftp@dm1n123
techcorp:TechCorp2024!
guest:guest123

  welcome

==========

TechCorp Solutions - FTP Server

==========

Bem-vindo ao servidor FTP corporativo!

Este servidor é usado para compartilhamento
interno de arquivos da empresa.

ATENÇÃO: Apenas para uso autorizado!

==========

FLAG{ftp_4n0nym0us_4cc3ss}

  readme

TechCorp FTP - Public Directory

Esta é uma área pública para compartilhamento de arquivos.

Arquivos confidenciais devem ser colocados em /confidential/

Para mais informações, contate o administrador.

  passwords

> # TechCorp Solutions - Password Archive
> # Data: 2024-01-15
> # CONFIDENCIAL - NÃO COMPARTILHAR
>
> SSH Server Credentials:
>
> - User: techcorp
> - Password: TechCorp2024!
>
> FTP Admin:
>
> - User: ftpadmin
> - Password: ftp@dm1n123
>
> Database Backup User:
>
> - User: backup_user
> - Password: B4ckup_S3cr3t_2024
>
> WiFi Office:
>
> - SSID: TechCorp_Corporate
> - Password: TechC0rp_W1F1_2024
>
> VPN Access:
>
> - Username: vpn_user
> - Password: VPN_P4ssw0rd!
>
> FLAG{p4ssw0rd_f1l3_d1sc0v3ry}
>
> # NOTA: Estas senhas devem ser trocadas mensalmente!
> # Última atualização: 15/01/2024

Acesso SSH e Banco de Dados

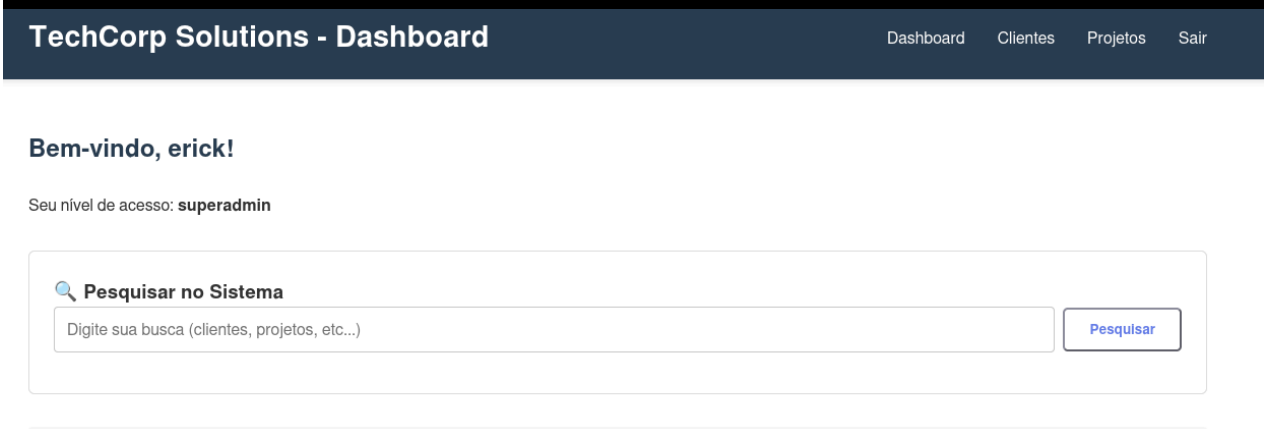
- **Acesso SSH obtido:** sessão interativa permitiu navegação no sistema e acesso a arquivos locais, acesso ao banco de dados e inserção de usuário superadmin no painel do site.
- **Evidências de exploração de banco de dados:** extração de tabela contendo segredos
- **Escalada de privilégios:** consegui escalar privilégios apenas com a senha vazada do techcorp.
- **Flags adicionais encontradas no sistema:**

- `FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n}`
- `FLAG{v13w_d1sc0v3ry_4dv4nc3d}`
- `FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}`

- **Observação:** presença de `api_secret` e caminhos de backup indicam risco de comprometimento de dados em produção se reutilizados.

```
+----+------------+-----------------------------+------------+---------------------+
| id | username   | password                    | role       | created_at          |
+----+------------+-----------------------------+------------+---------------------+
|  1 | admin      | admin123                    | admin      | 2025-11-17 14:30:36 |
|  2 | user       | password123                 | user       | 2025-11-17 14:30:36 |
|  3 | manager    | manager2024                 | manager    | 2025-11-17 14:30:36 |
|  4 | guest      | guest                       | guest      | 2025-11-17 14:30:36 |
|  5 | superadmin | Sup3r@dm1n!2024#Secure      | superadmin | 2025-11-17 19:38:25 |
|  6 | gilson     | g1ls0n123                   | user       | 2025-11-17 22:52:03 |
|  7 | cl4ud1o    | https://fakeupdate.net/wnc/ | superadmin | 2025-11-17 22:55:10 |
|  8 | al1nn3     | estiveaqui,yes              | superadmin | 2025-11-18 14:17:09 |
+----+------------+-----------------------------+------------+---------------------+
8 rows in set (0.00 sec)
mysql> insert into users(username,password,role) value('erick','bomdiagrupodozap','superadmin');
Query OK, 1 row affected (0.01 sec)

mysql> select * from users;
+----+------------+-----------------------------+------------+---------------------+
| id | username   | password                    | role       | created_at          |
+----+------------+-----------------------------+------------+---------------------+
|  1 | admin      | admin123                    | admin      | 2025-11-17 14:30:36 |
|  2 | user       | password123                 | user       | 2025-11-17 14:30:36 |
|  3 | manager    | manager2024                 | manager    | 2025-11-17 14:30:36 |
|  4 | guest      | guest                       | guest      | 2025-11-17 14:30:36 |
|  5 | superadmin | Sup3r@dm1n!2024#Secure      | superadmin | 2025-11-17 19:38:25 |
|  6 | gilson     | g1ls0n123                   | user       | 2025-11-17 22:52:03 |
|  7 | cl4ud1o    | https://fakeupdate.net/wnc/ | superadmin | 2025-11-17 22:55:10 |
|  8 | al1nn3     | estiveaqui,yes              | superadmin | 2025-11-18 14:17:09 |
|  9 | erick      | bomdiagrupodozap            | superadmin | 2025-11-19 10:16:03 |
+----+------------+-----------------------------+------------+---------------------+
9 rows in set (0.00 sec)
```




```
mysql> select * from sensitive_info;
+----------+----------+-------+------------------------------+
| username | password | role  | hidden_flag                  |
+----------+----------+-------+------------------------------+
| admin    | admin123 | admin | FLAG{v13w_d1sc0v3ry_4dv4nc3d} |
+----------+----------+-------+------------------------------+
1 row in set (0.00 sec)

mysql> select * from secret_data;
+----+---------------+-----------------------------------------------+---------------------+
| id | secret_key    | secret_value                                  | created_at          |
+----+---------------+-----------------------------------------------+---------------------+
|  1 | database_flag | FLAG{sql_1nj3ct10n_m4st3r}                    | 2025-11-17 14:30:36 |
|  2 | admin_token   | FLAG{h1dd3n_d4t4_1n_d4t4b4s3}                 | 2025-11-17 14:30:36 |
|  3 | api_secret    | sk_prod_A7x9mP2qR5tY8wZ3vC6nB4jK1lM0hG        | 2025-11-17 14:30:36 |
|  4 | backup_path   | /var/backups/techcorp/backup_20240115.tar.gz  | 2025-11-17 14:30:36 |
+----+---------------+-----------------------------------------------+---------------------+
```

- **Arquivos relevantes encontrados no servidor ssh:**

> home_ssh_content
> techcorp@024a36a8e6ca:~$ cat *
> TechCorp Solutions - Internal Notes
> ==========
>
> Senhas importantes:
>
> - Root MySQL: r00t_P4ssw0rd_2024
> - Admin Panel: admin / admin123
>
> Backup Location: /var/backups/techcorp/

> API Keys:
>
> - Production: tc_sk_prod_9Kx7mN2pQ4rT8wY
> - Development: tc_sk_dev_1Aa2Bb3Cc4Dd5Ee
>
> FLAG{ssh_h0m3_d1r3ct0ry_3xpl0r4t10n}
>
> Notas:
>
> - Fazer backup toda segunda-feira
> - Verificar logs de segurança semanalmente
> - Atualizar certificados SSL em março
>   TODO List - TechCorp IT Department
>   ==========
>
> [X] Configurar novo servidor web
> [X] Instalar certificado SSL
> [ ] Trocar senha do banco de dados (ainda é T3chC0rp_S3cr3t_2024!)
> [ ] Configurar firewall
> [ ] Revisar acessos FTP
> [ ] Atualizar documentação
> [ ] Fazer backup dos logs
>
> Reunião na sexta às 14h para discutir migração para cloud.

Serviços e Hosts identificados via Nmap

- **Resumo da varredura Nmap:** 6 hosts ativos identificados na rede de laboratório
- **Hosts relevantes:**

Host	IP	Observação
Gateway local	172.20.0.1	Host up
Database container	172.20.0.2	Serviço de banco de dados identificado
phpMyAdmin container	172.20.0.3	Interface de administração web do BD
Web application	172.20.0.10	Serviço web principal
FTP container	172.20.0.20	Serviço FTP acessível
Host adicional	172.20.0.30	Container/host visível

- **Nmap:** varredura rápida de 256 IPs retornou 6 hosts up; latências muito baixas indicam ambiente local de containers.

Riscos Identificados

- **Exposição de backups e arquivos sensíveis** via `robots.txt` e diretórios públicos.
- **FTP com conteúdo confidencial** acessível sem controles adequados.
- **Segredos em banco de dados** (tokens, chaves de API, caminhos de backup) armazenados sem criptografia.
- **Acesso SSH obtido** permite movimentação e extração de dados.
- **Possível vulnerabilidade XSS refletida** indicada por cookie codificado com flag.
- **Presença de arquivos de configuração e `.git` potencialmente acessíveis** aumenta risco de leak de código e credenciais.

Recomendações Imediatas

- **Remover ou restringir** `robots.txt` para não expor caminhos sensíveis; mover backups para local inacessível via web.
- **Isolar e proteger FTP:** desabilitar acesso anônimo, aplicar autenticação forte, restringir por IP e criptografar informações importantes, como senhas.
- **Rotacionar segredos:** invalidar e rotacionar `api_secret`, `admin_token` e quaisquer credenciais encontradas.
- **Remover arquivos sensíveis do repositório público** e proteger `.git` e `/config`.
- **Hardening no SSH:** desabilitar autenticação por senha, usar chaves, restringir usuários e registrar sessões.
- **Criptografar segredos em banco de dados** e aplicar controle de acesso baseado em privilégios mínimos.
- **Rever logs e auditoria** para identificar possíveis acessos não autorizados.

Plano de Ação Prioritário (80/20)

Ação	Impacto	Facilidade	Prioridade
Rotacionar segredos expostos	Alto	Média	Alta
Restringir acesso a backups e `/config`	Alto	Alta	Alta
Desabilitar FTP público / aplicar autenticação	Alto	Média	Alta
Remover dados sensíveis de repositórios públicos	Alto	Média	Alta
Harden SSH e revisar contas	Alto	Média	Alta

Conclusão

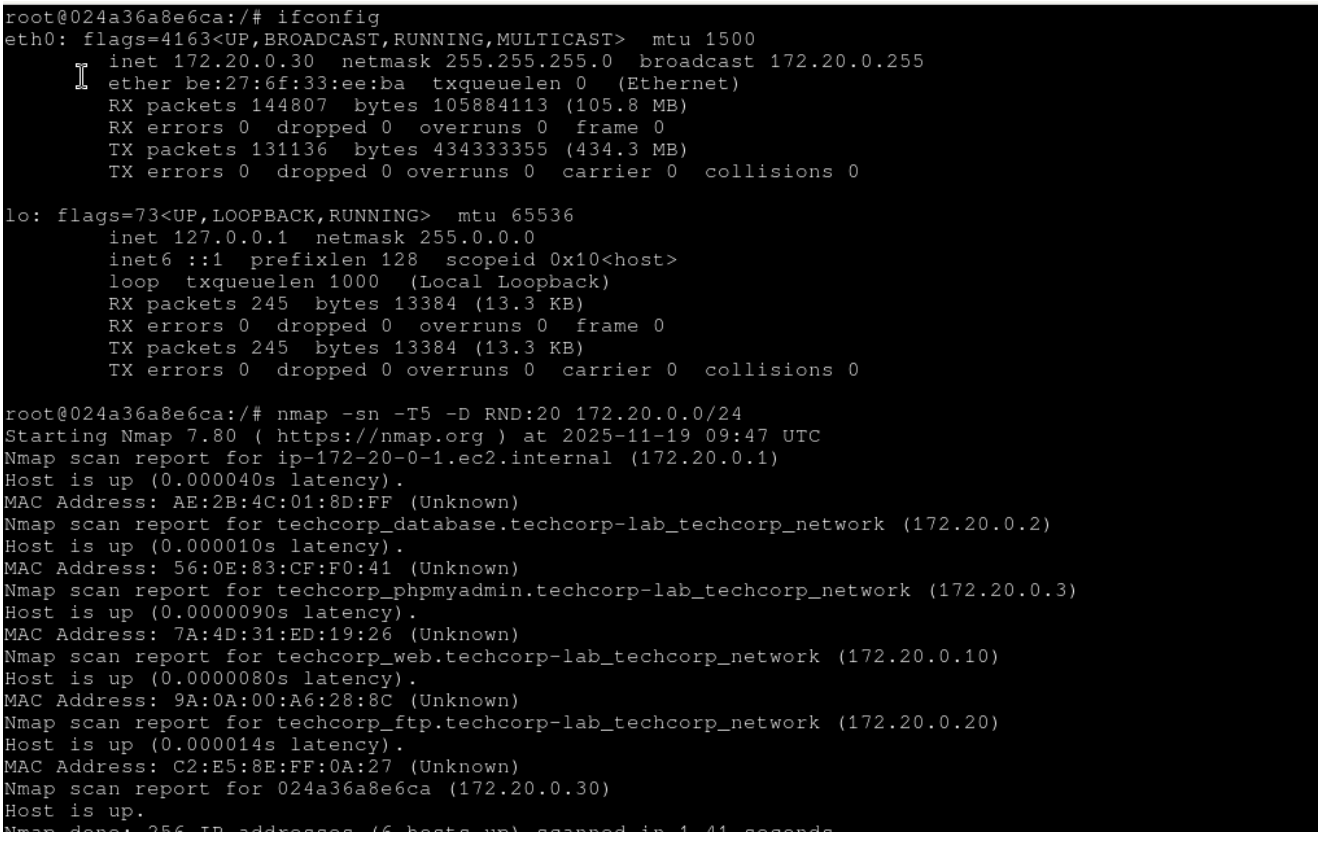
O serviço web simulado apresenta exposições críticas e práticas inseguras de armazenamento de segredos que permitem descoberta e extração de dados sensíveis. A combinação de arquivos de backup acessíveis, FTP público e segredos em banco de dados facilita comprometimento em ambiente real. Recomenda-se executar as correções listadas com prioridade alta, realizar nova varredura após mitigação e implementar monitoramento contínuo.

Redes e Hosts Identificados

Rede Estimada	Subnet	Finalidade Suposta
lab_net	172.20.0.0/24	Ambiente de containers e serviços simulados

Hosts por função

IP	Função estimada	Evidência
172.20.0.1	Gateway/container host	Nome `ec2.internal` detectado
172.20.0.2	Database	Nome `techcorp_database` detectado; Banco de dados acessível
172.20.0.3	phpMyAdmin	Nome `techcorp_phpmyadmin` detectado; Acessível através do browser
172.20.0.10	Web app	Nome `techcorp_web` detectado
172.20.0.20	FTP	Nome `techcorp_ftp` detectado; FTP acessível
172.20.0.30	Host adicional	Servidor SSH que loguei



Observações Finais de Risco

- **Alta prioridade:** rotacionar segredos, proteger backups, criptografar senhas e banco de dados.

- **Média prioridade:** revisar exposição de diretórios e arquivos estáticos.