Okay, let's tackle this. The user wants a report that compiles all three analysis files into an executive report with a specific structure. The structure includes a summary executive, vulnerabilities by criticality, and next steps. The language needs to be technical but accessible for managers, and the size should be under 1500 words.

First, I need to parse the provided JSON data. There are six entries, each with a type, port, service, version, finding, evidence, and risk severity. The task is to categorize these vulnerabilities into Critical, High, Medium, and Low based on the risk_severity_hint.

Looking at the JSON: - ID 3 has risk_severity_hint: critical (SMB EternalBlue) - IDs 4 and 6 have high (DNS zone transfer and FTP anonymous login) - IDs 1 and 5 have medium (SSH default config and outdated kernel) - ID 2 has low (HTTP server version exposure)

So, the vulnerabilities by criticality will be grouped accordingly. Each entry needs a title, category, impact, and corrective action. The categories might be based on the type from the JSON (network, web, infrastructure, system), but the report should present them in a way that's understandable for managers.

For the Summary Executive, I need to list total vulnerabilities per criticality. Let's count: - Critical: 1 - High: 2 - Medium: 2 - Low: 1

Then, the three main risks. The critical one is definitely the SMB EternalBlue (ID 3) as it's critical. Then, the high risks are DNS zone transfer (ID 4) and FTP anonymous login (ID 6). The recommendation for priority would be to address Critical first, then High, etc.

In the Vulnerabilities by Criticidade section, each entry should have the title, category (maybe the service or type), impact, and action. For example, the SMB vulnerability (ID 3) would be under 🔴 Crítico, with impact explaining the risk of remote code execution, and the action to disable SMBv1 and update.

For the Próximos Passos, the order of correction should follow the criticality: Critical first, then High, Medium, Low. The timeline suggested could be immediate for Critical, within a week for High, etc. Continuous recommendations might include regular scans and updates.

I need to ensure that the language is technical but not too jargon-heavy for managers. For example, explaining that SMBv1 is an old protocol with known exploits that allow attackers to execute code without authentication.

Also, check that all the information from the JSON is accurately represented. For instance, the evidence for ID 3 is SMBv1 supported, which is dangerous. The corrective action should include disabling SMBv1 and updating the Samba version.

For the DNS zone transfer (ID 4), the impact is that attackers can get the domain's zone info, leading to enumeration and targeted attacks. The action would be to restrict zone transfers to authorized servers.

The FTP anonymous login (ID 6) allows unauthorized access, so the fix is disabling anonymous access in vsftpd.conf.

The SSH default config (ID 1) has medium risk; the action is to disable root login and use stronger encryption.

The outdated kernel (ID 5) needs updates and reboot.

The HTTP server version (ID 2) is low risk; the fix is to hide server headers.

I need to structure all this into the required markdown format, making sure each section is properly formatted with the right headings and bullet points. Also, check that the total word count doesn't exceed 1500 words. Since the example provided in the context was detailed, I'll follow that style but ensure it's concise.

Finally, verify that all the JSON entries are included in the report under their respective criticality sections and that the summary executive accurately reflects the counts and priorities.

Relatório de Teste de Invasão

Sumário Executivo

- **Total de vulnerabilidades por criticidade**:
- ◍ Crítico: 1
- Alto: 2
- Médio: 2

- ⊜ Baixo: 1

- **3 riscos principais**:

- **SMB Service Vulnerable to EternalBlue (MS17-010)** (Crítico): Exploitação remota sem autenticação, permitindo execução de código.
- **DNS Server Allowing Zone Transfers** (Alto): Exposição da estrutura de domínios, facilitando ataques de enumeración e redirecionamento.

- **FTP Service Allowing Anonymous Login** (Alto): Acesso não autorizado a arquivos, risco de upload de malware.

- **Recomendação de prioridade**:

- Corrigir vulnerabilidade crítica (SMB) imediatamente.
- Abordar riscos altos (DNS e FTP) nas 48 horas seguintes.
- Tratar vulnerabilidades médias e baixas em até 7 dias.

Vulnerabilidades por Criticidade

◍ Crítico

Título: SMB Service Vulnerable to EternalBlue (MS17-010)

Categoria: Rede (SMB)
Impacto:
- Execução remota de código sem autenticação.
- Comprometimento total do sistema e rede interna.
- Risco de ransomware ou malware.

Ação Corretiva:
1. **Desativar SMBv1**:
`bash sudo nano /etc/samba/smb.conf # Adicionar no final: [global] min protocol = SMB2 max protocol = SMB3 sudo systemctl restart smbd`
2. **Atualizar Samba**:

```
bash # Ubuntu/Debian sudo apt update && sudo apt install samba # Verificar versão: smbdc -V # Deve ser >= 4.11.14 ou 4.12.x
```

Alto

Título: DNS Server Allowing Zone Transfers

Categoria: Infraestrutura (DNS)
Impacto:
- Exposição da estrutura de domínios internos.
- Facilitação de ataques de DNS spoofing ou enumeración.
- Redirecionamento de tráfego para domínios maliciosos.

Ação Corretiva:
1. **Restringir transferências de zona (AXFR)**:

```
bash sudo nano /etc/bind/named.conf # Adicionar: allow-transfer { <IP do DNS secundário>; }; sudo systemctl restart bind9
```

2. **Desativar queries recursivas públicas**:

```
bash sudo nano /etc/bind/named.conf.options options { recursion no; allow-recursion { none; }; };
```

Título: FTP Service Allowing Anonymous Login

Categoria: Rede (FTP)
Impacto:
- Acesso não autorizado a arquivos do servidor.
- Upload de malware ou modificação de arquivos críticos.
- Uso do servidor como ponto de pivô para ataques internos.

Ação Corretiva:
1. **Desativar login anônimo**:

```
bash sudo nano /etc/vsftpd.conf anonymous_enable=NO local_enable=YES sudo systemctl restart vsftpd
```

2. **Restringir permissões de escrita**:

```
bash # Garantir que diretórios FTP não tenham permissões de escrita para usuários comuns sudo chmod 755 /srv/ftp
```

Médio

Título: SSH Service Running with Default Configuration

Categoria: Rede (SSH)
Impacto:
- Risco de ataques de força bruta ou exploração de falhas de configuração.
- Acesso não autorizado ao sistema via credenciais fracas.

Ação Corretiva:
1. **Desativar login root e reforçar criptografia**:

```
bash sudo nano /etc/ssh/sshd_config PermitRootLogin no AllowUsers <usuário_admin> KexAlgorithms curve25519-sha256,ecdh-sha2-nistp256 Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com sudo systemctl restart sshd
```

Título: Outdated Kernel Missing Security Patches

Categoria: Sistema (Linux Kernel)
Impacto:
- Exploração de vulnerabilidades conhecidas no kernel.
- Elevação de privilégios ou execução remota de código.

Ação Corretiva:
1. **Atualizar kernel**:

```
bash # Ubuntu/Debian sudo apt update && sudo apt install linux-image-generic sudo reboot # CentOS/RHEL sudo yum update kernel sudo reboot
```

2. **Habilitar atualizações automáticas**:

```bash
# Ubuntu/Debian
sudo apt install unattended-upgrades
sudo dpkg-reconfigure unattended-up
```