**1.0 Relatório – Resumo**

Este documento mostra o resumo e passo a passo de como a máquina BASIC2 foi infiltrada a partir de um teste de penetração interno. Este tipo de teste é um ataque simulado contra máquinas conectadas internamente.

O foco do teste é de realizar ataques similares aos de um cenário real, na tentativa de infiltração na máquina BASIC2. O objetivo é de avaliar a rede, identificar sistemas e explorar vulnerabilidades, e assim reportar os resultados.

Em resumo, as maiores vulnerabilidades encontradas foram dados pessoais que estavam expostos a partir da página web do servidor e senhas de fácil acesso. Além disso, chaves de autenticação de usuários estavam vulneráveis para qualquer pessoa que acesse a máquina. A partir disso, foi possível conseguir acesso de administrador a vários sistemas.

**1.1 Relatório – Recomendações**

É recomendável que as senhas dos usuários sejam alteradas, seguindo um padrão de ao menos uma letra maiúscula, um número e um carácter especial. O ideal é alguma frase para ajudar na memorização e que não tenha relação com algo pessoal (como o nome de algum familiar, datas de nascimento, etc.). Outra recomendação é dar direitos de ler as chaves de autenticação apenas para o usuário que a utiliza.

**2.0 Relatório – Metodologias**

Foi utilizado um método muito comum para testar a segurança da máquina na qual foi atacada. Abaixo estará listado o passo a passo de como foi possível identificar e explorar as vulnerabilidades apresentadas.

**2.1 Relatório – Coleta de Informações**

Esta fase do teste de penetração foca em identificar possíveis vulnerabilidades que possam ser exploradas por um atacante. O IP específico da máquina é:

10.10.214.55

**2.2 Relatório – Enumeração de Serviços**

Nesta parte o foco é coletar informações sobre quais serviços estão disponíveis e que podem potencialmente serem vetores de ataque, para conseguir informações críticas que podem levar o atacante a invadir o sistema. Será listado apenas os serviços utilizados para realizar a intrusão.

|  |  |  |
| --- | --- | --- |
| IP do servidor | Portas | Serviço |
| 10.10.214.55 | TCP 22, 80, 445 | OpenSSH, Apache, Samba |

**2.3 Relatório – Penetração**

Esta etapa foca em ganhar acesso aos diferentes sistemas observados na enumeração. O acesso foi concedido a partir da quebra da senha do usuário pelo serviço de OpenSSH e pela enumeração dos usuários cadastrados no serviço de Samba.

**Vulnerabilidade utilizada**: OpenSSH – Quebra de senha

**Sistema Vulnerável**: 10.10.214.55

**Explicação**: O usuário jay, que foi descoberto a partir da enumeração do serviço Samba, utiliza uma senha fraca que foi quebrada facilmente pela ferramenta hydra utilizando uma lista.

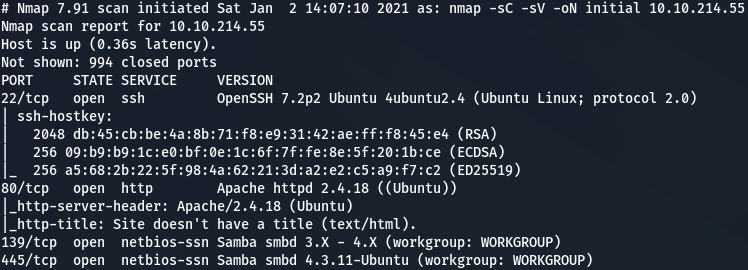
**Escalação de Privilégio**: Acesso a um usuário local do servidor.

**Mitigação**: Utilização de uma senha forte

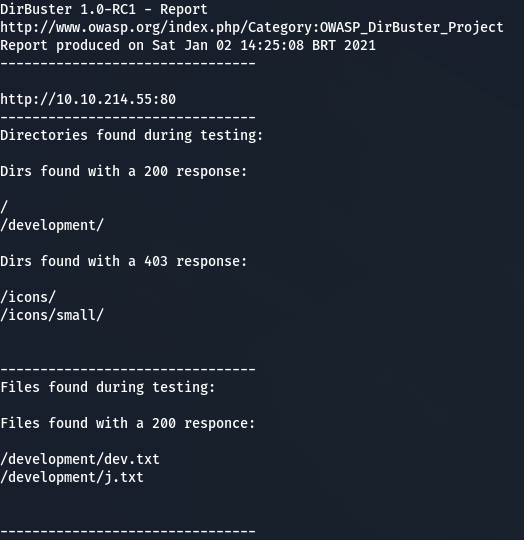
**Severidade**: Crítica

**Coleta de Informações**:

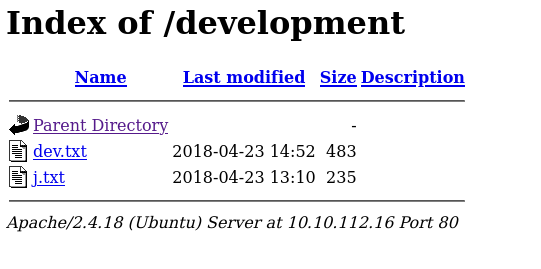
**Scan do Nmap das portas**:



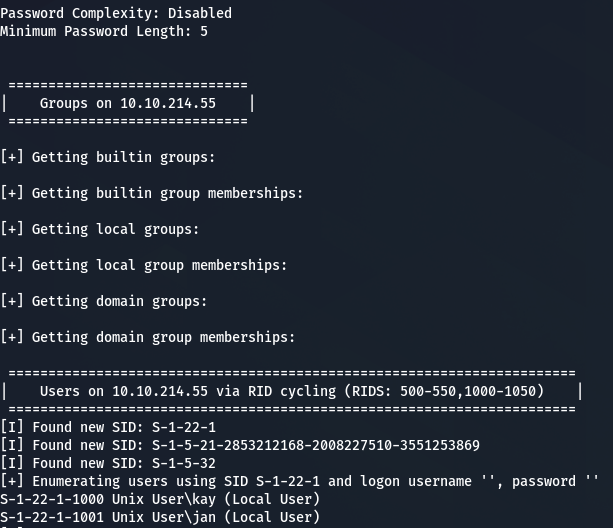
**Scan do DirBuster para a porta 80**:



Com isso, foram encontrados arquivos pessoais acessíveis pelo browser a partir do diretório /development:

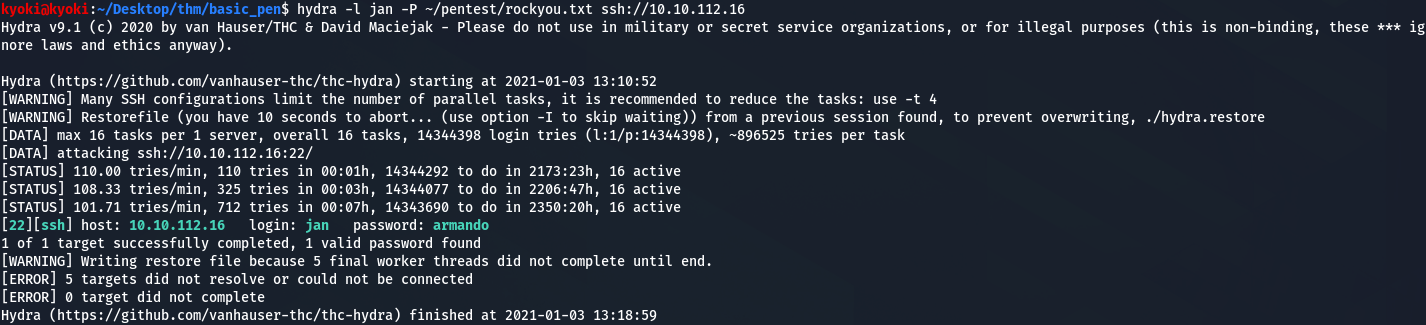


**Scan do enum4linux para o protocolo 445**:



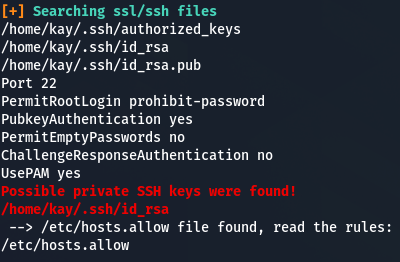
Com essa enumeração, é possível ver dois usuários locais, kay e jan.

Tendo o conhecimento a partir das mensagens trocadas pelos usuários, nas quais foram acessadas a partir do diretório /development, foi optado por quebrar a senha do usuário jan.

 **Utilizando a ferramenta hydra, foi descoberto que a senha é armando:**

Tendo acesso ao usuário, foi possível transferir a ferramenta linpeas para o usuário jan e utilizar a ferramenta para achar alguma forma de escalar o privilégio.

**A partir do linpeas, foi visto que existem chaves privadas de SSH no diretório do usuário kay:**



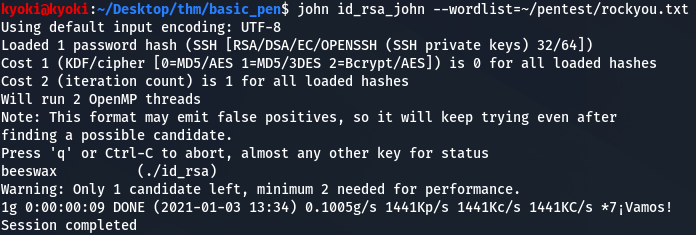
O arquivo com a chave foi copiado e ela necessita de um código para ser acessado por SSH.

Com isso, foi utilizado ssh2john.py para transformar a chave RSA em código legível para ser utilizado pela ferramenta John The Ripper.

Comando utilizado:

Python3 ~/pentest/ssh2john.py ./id\_rsa | tee id\_rsa\_john

**A partir disto, foi utilizado John para quebrar a senha da chave:**



Tendo acesso ao usuário kay, foi possível ter acesso privilegiado a todo o sistema.

**3.4 Relatório – Limpeza**

A última parte é a de certificar que todos os traços do teste sejam removidos. A ferramenta linpeas foi retirada do sistema e os logs foram passados para o computador do atacante. Não foram deixados traços e arquivos no sistema no qual o teste foi realizado.