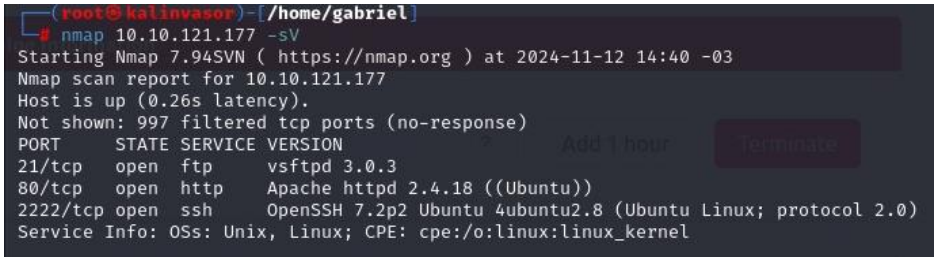
GABRIEL JULIANI SEGATTO
GRUPO DE SEGURANÇA OFENSIVA - OFFSEC

WRITE-UP DO CTF - 12/11/2024

A maneira com que eu vou tentar estruturar esse documento é em tópicos tentando separar bem os conteúdos e os passos que eu acabei seguindo pra completar o desafio. Idealmente eu não vou explicar como iniciar o CTF (conexão com VPN, etc), mas já vou iniciar na resolução em si.

1. Enumeração Inicial

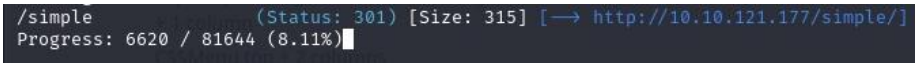
Normalmente, a primeira coisa a se fazer é a enumeração inicial, ou seja, estando conectado na rede que a gente quer atacar, utilizar o nmap pra identificar dispositivos e serviços nela. Eu usei o comando **"nmap [IP alvo] -sV"** pra isso e obtive a seguinte saída:



Com isso, eu consigo identificar que tem um servidor http rodando na porta 80 e um serviço ssh na 2222. Decidi seguir pelo http para procurar por vulnerabilidades pois me pareceu mais promissor.

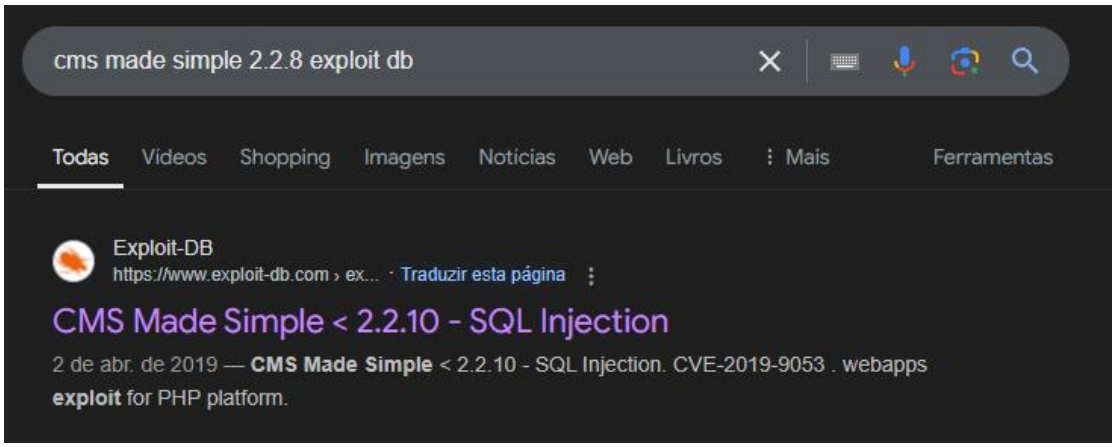
Porém, antes de seguir, com essas informações adquiridas já é possível responder as duas primeiras questões do CTF. São 2 serviços rodando abaixo da porta 1000 (21/ftp e 80/http) e o serviço rodando na porta mais alta é justamente o ssh na porta 2222.

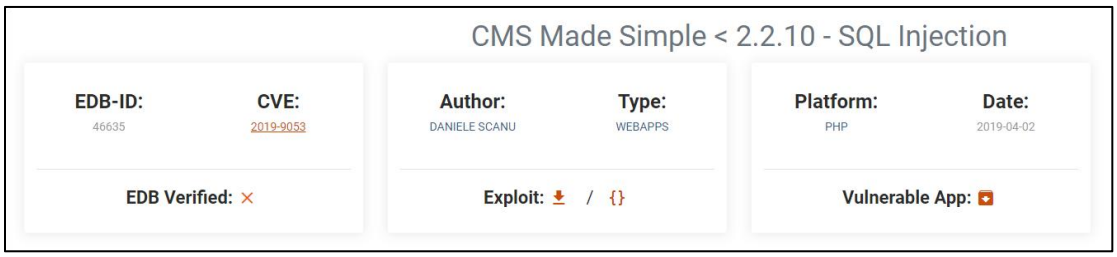
Feito isso, decidi utilizar o gobuster, umas das ferramentas de enumeração que a gente estudou, pra procurar por diretórios ocultos no ip que estamos atacando. Após algumas tentativas com diferentes listas de palavras, utilizei o comando **"gobuster -u http://[IP alvo] -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt"**, que me retornou um diretório **"/simple"** possível de ser acessado pelo browser através de **"[IP alvo]/simple"** e resultando em uma página web.



2. Exploit-DB

Bem embaixo dessa página existe uma informação de que o site tem suporte do CMS Made Simple version 2.2.8. Usaremos ess informação pra pesquisar no google e descobrir vulnerabilidades conhecidas desse software com essa versão.





Com essas informações a gente consegue responder as duas perguntas seguintes do CTC. A **CVE-2019-9053** (vulnerabilidade) que pode ser explorada é um SQLInjection (**sqli** na resposta).

3. Explorando a vulnerabilidade encontrada

Após isso, é só baixar o exploit dessa página do Exploit-DB que, nesse caso, é um script em python2. Então temos que (eu fiz indo no diretório de Downloads) rodar o comando **"python2 46635.py -u http://[IP alvo]/simple --crack -w /usr/share/wordlist/fasttrack.txt"** sendo a flag **--crack** necessária pra nos retornar a senha real, senão a gente só teria o hash (pode ser que ela não retorne certo de primeira, então teria que rodar de novo". No entanto, no momento de executar esse script pode ser que vc tenha erros no pythons como "No module named termcolor" ou algo assim, e isso é por que o exploit é um pouco antigo e a gente precisa baixar

esse módulo no pc. Acredito que seguindo esses comandos seja possível de instalar o pip do python 2.

```
sudo apt update
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
sudo python2 get-pip.py
```

Após esses comandos, é preciso rodar o **"pip2 install termcolor"**. Se, depois de seguir esses passos e tentar executar o exploit novamente aparecer um erro de **"invalid command 'egg_info' "** é um bom sinal kkkk. Nesse caso é só executar **"pip2 install --upgrade setuptools"** que vai atualizar o pacote necessário pra, enfim, executar o exploit corretamente.

Tendo executado o exploit do python, é esperado que se tenha uma saída parecida com isso:

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

A informação da senha (**secret)**, além de importante para os passos seguintes da invasão, serve de resposta para mais um campo do CTF.

4. Conectando à máquina remota e escalando privilégios

Lembrando que na primeira etapa, quando eu fiz e enumeração, tivemos a informação de um serviço SSH rodando na porta 2222 do servidor e é ela que vamos explorar agora, pois temos o nome e a senha do usuário dessa máquina.

Utilizando a função **"ssh -p 2222 mitch@[IP alvo]"** e, em seguida entrando com a senha, obtemos acesso remoto à máquina que estamos atacando. Nesse ponto, é sempre interessante rodar um **"sudo -l"** pois isso pode expor alguma vulnerabilidade da máquina, e é o caso aqui. Fazendo isso, recebemos **"INSERT HERE"** que indica que talvez o root possa ser acessado através de alguma fragilidade no Vim, que é o que eu fiz. Com essa informação é só pesquisar por "vim" no GTFOBins e ir para a sessão de **sudo**, onde tem a linha **"sudo vim -c ':!/bin/sh' "** que fará a escalada de priviégio necessária.

Com os privilégios de root o ataque já foi bem sucedido e agora dá pra explorar o sistema como achar melhor, mas vou descrever como recuperei as últimas informações pedidas no desafio. A flag de usuário pode ser obtida utilizando

“cat user.txt” (sei disso pois eu utilizei o **ls** antes). Em seguida, com **“cd .. && ls”** descobrimos o nome de todos os usuários da máquina, para mais uma resposta. A questão seguinte é relacionada ao método que já foi usado pra escalar privilégios, o **vim**. Por fim, para a flag de root podemos realizar **“cd ../root && cat root.txt”**, finalizando o desafio.