RESULTADO DO DESAFIO

O desafio de segurança do EnSI premiou os participantes pela ordem de recebimento das respostas. Ao todo foram recebidas quatro respostas corretas, sendo o primeiro colocado **Caio Vargas Rocha** (UFBA), o segundo **Gilson de Souza Camelo** (Área1), o terceiro **Carlos Marx Novais Assunção** (UFBA) e o quarto **Pedro Henrique Carvalho Sampaio** (UFBA). A seguir são apresentadas as soluções enviadas por cada participante.

1.) Caio Vargas Rocha

Level 0:

Precisamos encontrar a porta que o serviço ssh está escutando no servidor, para isso executamos o seguinte comando nmap que escaneia todas as portas na range 1-65353:

```
$ nmap -T4 -A -Pn -p 1-65535 200.128.6.66
...
Discovered open port 8017/tcp on 200.128.6.66
...
```

Encontramos a porta 8017 aberta.

```
$ ssh leve0@200.128.6.66 -p 8017
```

nos loga na máqunina com o usuário level0.

O arquivo README indica que existe um binário no sistema com setuid que nos permitirá avançar ao próximo nível.
Fazendo uma busca por arquivos cujo dono é o usuário do próximo nível (level1)

```
level0@ensi2015:~$ find
/{usr,bin,var,lib,home,bin,etc,opt,root,sbin,srv} -user level1 -type f
-exec ls -la {} \; 2>/dev/null
-rwsr-x--- 1 level1 level0 7016 Sep 26 12:09 /usr/bin/lololo
```

Encontramos o arquivo /usr/bin/lololo com a flag setuid ligada. Este binário se comporta como uma shell (que roda como usuário level1 por conta do setuid).

```
level0@ensi2015:~$ /usr/bin/lololol
```

Executando esse binário, entramos em uma shell com o usuário level1 (como o comando whoami mostra):

```
level0@ensi2015:~$ /usr/bin/lololo
$ whoami
level1
$ groups
level0
```

Observando o conteúdo da home de level1, notamos que não podemos ler o conteúdo de README pois somente o usuário root e membros do grupo level1 possuem permissão de leitura para o arquivo.

```
level1@ensi2015:~$ ls -la /home/level1
```

```
total 20
dr-xr-x--- 3 level1 level1 4096 Sep 26 16:49 .
drwxr-xr-x 9 root   root   4096 Sep 27 16:32 ..
dr-xr-x--- 2 level1 level1 4096 Sep 26 15:32 ...
-rw-r----- 1 root   level1  763 Sep 26 16:26 .bash_history
-rw-r----- 1 root   level1  266 Sep 26 16:49 README
```

Entretando o diretório /home/level1/... possui um arquivo com permissão de leitura para o usuário level1:

```
$ ls -la /home/level1/...
total 12
-r--r----- 1 level1 level1   14 Sep 26 11:58 -
dr-xr-x--- 2 level1 level1 4096 Sep 26 15:32 .
dr-xr-x--- 3 level1 level1 4096 Sep 26 16:49 ..

$ cat /home/level1/.../-
aeAmVyf09E9F2
```

nos revela a senha do próximo nível.

Level 1:

O arquivo README indica que existe um arquivo de senhas no servidor e que existe alguma pista sobre a senha no histórico. O history, nos mostra uma entrada "camshaft" que não corresponde a nenhum programa ou comando no Linux.

Fazendo uma busca por arquivos no grupo level1 descobrimos o arquivo /var/lib/dpkg/info/data

```
level1@ensi2015:~$ find
/{usr,bin,var,lib,home,bin,etc,opt,root,sbin,srv} -group level1 -type f
-exec ls -la {} \; 2>/dev/null
-rw-r----- 1 root level1 4184396 Sep 26 15:50 /var/lib/dpkg/info/data
-rw-r----- 1 root level1 763 Sep 26 16:26 /home/level1/.bash_history
-rw-r----- 1 root level1 266 Sep 26 16:49 /home/level1/README
-r--r----- 1 level1 level1 14 Sep 26 11:58 /home/level1/.../-
```

O grep abaixo nos revela uma string alfanumérica que é a senha para o próximo nível.

```
level1@ensi2015:~$ grep 'camshafts' /var/lib/dpkg/info/data
camshafts       e9K8A0TcYiMfXzsjnC1drznf7MLjeGbA
```

Level 2:

Este nível indica no README que a senha para o próximo nível só aparece uma vez no arquivo /home/level2/data.txt.

Utilizando as ferramentas sort e uniq, obtemos a string que só ocorre uma vez no arquivo:

```
level2@ensi2015:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

Level 3:

Este nível é resolvido facilmente decodificando a string contida no arquivo /home/level3/.pass que está códificada em ROT13.

```
level3@ensi2015:~$ cat .pass
    N FRAUN QB YRIRY4 RU WWSEGXVVEDUG
```

O seguinte script em Python decodifica a mensagem e nos revela a senha:

```
    import string
    rot13 =
string.maketrans("ABCDEFGHIJKLMabcdefghijklmNOPQRSTUVWXYZnopqrstuvwxyz",
"NOPQRSTUVWXYZnopqrstuvwxyzABCDEFGHIJKLMabcdefghijklm")
    print string.translate("N FRAUN QB YRIRY4 RU WWSEGXVVEDUG", rot13)
```

```
$ python2.7 rot13
A SENHA DO LEVEL4 EH JJFRTKIIRQHT
```

Level 4:

```
level4@ensi2015:~$ cat README
Parabéns!
```

2.) Gilson de Souza Camelo

Level0

Para achar a porta aberta no servidor utilizei a ferramenta NMAP.
Após algumas tentativas obtive sucesso com o comando:
nmap -Pn -sV 200.128.6.66 -p 0-65535 /* Os parâmetros foram para não usar ping, mostrar a versão dos serviços e scan em todas as portas */
Demorou um pouco mais retornou a porta 8017 aberta com o serviço ssh na escuta.
ssh -p 8017 level0@200.128.6.66 password: level0

Level1

Ao ler o arquivo README a dica era sobre SUID habilitado.
Usei o comando:
find / -perm -4000 -print /* Retornou uma lista com os arquivos com SUID habilitado */
/usr/bin/lololo /* Me chamou atenção por causa do nome */
após executar o comando “lololo” percebi que estava com uid=1002(level1)
acessei o pasta /home/level1
Mas ao tentar ler o arquivo README não obtive sucesso. Olhando com mais calma
Usando o comando “ls –la” percebi que “...” na verdade era um diretório.
Ao acessar o diretório “...” percebi um arquivo “ - “ mais ao tentar ler não tive sucesso.
Conseguir ler o conteúdo do arquivo “ - “ voltando um diretório e executando
“cat ..../-“
A senha para o level1 foi revelada “aeAmVyf09E9F2”

Level2

Com a dica usei o comando: find / -group level1 para listar todos os arquivos que fazia parte do grupo level1.
Notei o arquivo /var/lib/dpkg/info/data diferente dos outros ao ler o conteúdo se tratava do arquivo da dica.
A segunda dica era sobre o passado poderia me ensinar muita coisa
olhando o arquivo /home/level1/.bash_history notei algo diferente executado
“camshafts”
Ao ler novamente o arquivo data filtrando pelo camshafts usando o comando:
cat data | grep camshafts
Tive como retorno a senha do level 2. “e9K8A0TcYiMfXzsjnC1drznf7MLjeGbA”

Level3

A dica dizia q a senha estava no arquivo data.txt e era a única que não se repetia.
Usando o comando “sort” para ordenar a lista de senhas e filtrando com “uniq”
consegui a senha.
sort data.txt | uniq –u
Senha level 3 “UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR”Level4
A dica diz q a senha usa uma cifra de substituição.
Primeiro passo achar o arquivo com a cifra.

Com o bom e velho comando “ls –la” encontrei o arquivo “.pass”
O arquivo me retornou a cifra “N FRAUN QB YRIRY4 RU WWSEGXVVEDUG"
Pesquisando no site sugerido http://www.cryptool-online.org/ percebi que a cifra usada é a cifra de César.
No próprio site possui uma ferramenta pra decrypt da cifra.
Ao decifrar tive como retorno. “a SeNha dO leVel4 eh jjfRTkiiRQhT”
O detalhe q a senha é toda Capital Letter.
Senha level 4 “JJFRTKIIRQHT”

3.) Carlos Marx Novais Assunção

Level 0

Utilizando o comando `nmap -vv -Pn -p- 200.128.6.66` descobri a porta `8017` aberta. Com o comando `nmap -sV -p 8017 200.128.6.66` confirmei que nessa porta estava rodando um servidor SSH.

Com as credenciais `level0:level0` consegui acesso a servidor.

Level 1

O comando `find / -perm +6000 -type f -exec ls -ld {} \;` me retornou todos os binários com SUID. Dentre eles `/usr/bin/lololo` que me deu acesso aos arquivos do usuário `level1`. Com isso eu pude encontrar e ler o arquivo `/home/level1/.../-`, que continha uma sequencia de caracteres. Saí do servidor e loguei novamente com o usuário `leve1` e testei como senha a string que encontrei. Funcionou!

Level 2

Com `find / -group level1 -type f -exec ls -ld {} \;` encontrei o arquivo `/var/lib/dpkg/info/data` com uma lista de senhas e palavras aleatorias (ou talvez não...).

Não sou muito bom com charadas, então ignorei a dica "seu passado pode te ensinar muita coisa", copiei o arquivo, exclui as palavras aleatórias e utilizei como wordlist para efetuar um bruteforce com `hydra 200.128.6.66 ssh -l level2 -P wordlist -s 8017 -vV`. Em 19min foi encontrada a senha.

Level 3

Só foi necessário procurar uma senha única com a ajuda do `sort data.txt`.

Level 4

Com poucos minutos de pesquisa descobri que o texto em `.pass` estava cifrado com ROT-13, uma cifra de substituição simples. A frase dizia "A SENHA DO LEVEL4 EH JJFRTKIIRQHT".

DONE!

4.) Pedro Henrique Carvalho Sampaio

Level0

O servidor estava dropando pings, então fiz um portscan com nmap sem verificar se o host estava live.
#nmap -Pn -p1-65365 -T5 200.128.6.66
porta 8017 aberta

achei o arquivo com suid usando:
$find / -perm 4000
um binario chamado 'lololo' me deu um shell com uid do usuário level1.
dentro do diretorio /home/level1/.../ tinha uma arquivo chamado "-" que eu li com $cat ./-

Level1

procurei pelo arquivo com senhas usando:
find / -gid 1002
achei o arquivo /usr/lib/dpkg/data
no histórico tinha o termo camshafts digitado pelo usuário.
procurei dentro do arquivo data pelo termo e voilá!

Level2

A senha foi descoberta usando:
$sort data.txt | uniq -u

Level3

havia um arquivo oculto chamado .pass no diretorio home.
Dentro dele havia a seguinte frase:
N FRAUN QB YRIRY4 RU WWSEGXVVEDUG

Decifrei pelo site dado no README com cifra de cezar na rotaçao 39.
a SeNha dO leVel4 eh jjfRTkiiRQhT

Ao conectar a senha não deu certo, então percebi que a frase descriptografa estava com maiúsculos e minúsculos alternados.
Tentei tudo minúsculo, e consegui com tudo maiúsculo.

Level4

no README tinha parabéns.

Yeah \O/