Informe de Reconocimiento Pasivo

Academia: Hacker Mentor

Fecha: 30/03/2024

Alumno: Heber Daniel Pérez Iñiguez

Resumen:

Durante el proceso de reconocimiento pasivo, se llevó a cabo un análisis a la base de datos de filtraciones "**Breach Compilations"** para identificar la exposición del email y credenciales del administrador de la sucursal alemana de Toyota **"Rainer Luecke"** y de un hacker del cual solo conocemos parcialmente su correo "**hacker-root___@live.cn**". Posteriormente se realiza el reconocimiento de un servidor VPN de **Tesla** en Japón con la herramienta **dnsdumpster** para obtener el nombre del dominio y la dirección IP.

Se emplearon estas herramientas para recopilar información de manera discreta y cuidadosa para garantizar la privacidad y seguridad de los sistemas involucrados. A continuación, se presentan los hallazgos principales obtenidos durante este proceso.

Descripción del Proceso:

El proceso de exploración pasiva se basó en la consulta de bases de datos de filtraciones de datos conocidas, así como en el uso de herramientas de escaneo y recopilación de información. Se evitó cualquier acción que pudiera comprometer la seguridad de los sistemas del cliente o violar la privacidad de terceros.

Hallazgos:

1. Correos Electrónicos y Contraseñas Comprometidas:
    - Se identificaron los 2 correos electrónicos con sus respectivas credenciales asociados a filtraciones de datos.
        - ➔ **rainer.luecke@toyota.de**:**Luecke99**
        - ➔ **hacker-rootkit@live.cn: shjzcy@#**

Comando: grep -R “rainer” > rainer.txt

```
┌──(hmstudent㉿kali)-[~/Desktop/breach-parse/BreachCompilation]
└─$ grep -R  "rainer" > rainer.txt
grep: data/r/o/s: binary file matches
grep: data/r/o/b: binary file matches
grep: data/r/o/n: binary file matches
grep: data/r/k: binary file matches
grep: data/r/a: binary file matches
grep: data/r/i: binary file matches
grep: data/r/e: binary file matches
grep: rainer.txt: input file is also the output
```

Comando: cat rainer.txt | grep “toyota.de”

```
┌──(hmstudent㉿kali)-[~/Desktop/breach-parse/BreachCompilation]
└─$ cat rainer.txt | grep "toyota.de"
data/r/a:rainer.luecke@toyota.de:Luecke99
```

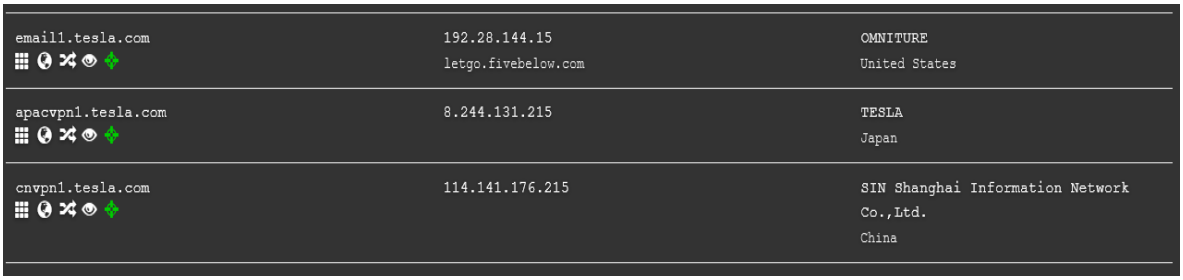
Comandos para hacker-root

```
┌──(hmstudent㉿kali)-[~/Desktop/breach-parse/BreachCompilation]
└─$ grep -R  "hacker-root" > hacker-root.txt
grep: hacker-root.txt: input file is also the output

┌──(hmstudent㉿kali)-[~/Desktop/breach-parse/BreachCompilation]
└─$ grep -R  "hacker-root"
hacker-root.txt:data/h/a:hacker-rootkit@live.cn:shjzcy@#
```

2. Reconocimiento Servidor VPN:
    - Se identifica el nombre del Host y la dirección IP del servidor VPN de Tesla en Japón.

➔ **Host: apacvpn1.tesla.com IP: 8.244.131.215 Tesla Japón**



Conclusión:

Durante el reconocimiento pasivo realizado el 30 marzo del 2024, se analizó una base de datos de filtraciones para identificar la exposición del correo y las credenciales del administrador de la sucursal alemana de Toyota, Rainer Luecke, así como de un hacker identificado por su correo parcial "hacker-root___@live.cn".

Utilizando técnicas no intrusivas, se identificaron las credenciales asociadas a los correos electrónicos expuestos y se obtuvieron detalles del servidor VPN de Tesla. Estos hallazgos proporcionan información valiosa para mejorar la seguridad y proteger la integridad de los sistemas involucrados.
