Vulnerabilità e Difesa dei Sistemi Internet

A.K.A. ETHICAL HACKING

FRANCESCO MANCINI - francesco.mancini@uniroma2.it

PASQUALE CAPORASO - pasquale.caporaso@uniroma2.it

SARA DA CANAL - sara.da.canal@uniroma2.it

PIERCIRO CALIANDRO – pierciro.caliandro@uniroma2.it

Vulnerabilità e Difesa dei Sistemi Internet

LINUX INTRODUCTION – PRATICE

Exercise 1

Q: Write a short script that given a website extracts the url from it

wget www.uniroma2.it -O uniroma2.html

cat uniroma2.html | grep "href=" | cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1 | grep -v "<a" | sort -u

cat uniroma2.html | grep -Eo '"(http:|https:|)//[^/"]+' | cut -d "/" -f 3 | sort -u

Exercise 1

#!/bin/bash

if [**$#** -lt 1]

then

    echo "Usage: $0 <website url>"

    exit 1

fi

curl -k -s **$1** | grep -Eo '"(http:|https:|)//[^/"]+' | cut -d "/" -f 3 | sort -u

Exercise 2

Q2: Research bash loops and write a short script to perform a ping sweep of your target IP range of your network

ping 127.0.0.1

ping -c 1 127.0.0.1

ping -c 1 -w 1 1.2.3.4

man ping (search code)

Exercise 2

```bash
#!/bin/bash

trap 'echo Process Interrupted; exit' INT # catch ctrl-c

for i in $(seq 1 255);do
        ip=10.11.1.$i
        ping -w 3 -c 1 $ip > /dev/null;
        if [ $? -eq 0 ]
        then
                echo "- $ip is UP";
        else
                echo "- $ip is DOWN";
        fi
done
```

Exercise 2

```python
#!/usr/bin/env python

import sh

print "Scanning..."

for i in range(201,255):
  address = "160.80.80." + str(i)
  try:
      sh.ping(address, "-c 1", "-w 3", _out="/dev/null")
      print "ping to", address, "OK"
  except sh.ErrorReturnCode_1:
      print "no response from", address
```

Exercises

- Try hack me:
  - Link fundamentals: https://tryhackme.com/module/linux-fundamentals

- Hack the box:

  - Linux fundamentals: https://academy.hackthebox.com/module/details/18

Exercises - more

- Hack the box:

  - Bash fundamentals: https://academy.hackthebox.com/module/details/21

Conclusion

THAT ALL FOLKS!

Thank you for your attention 😄 !