

HackerFrogs Afterschool Network Hacking – Session 5

Class:
Network Hacking

Workshop Number:
AS-NET-05

Document Version:
1.75

Special Requirements:
Registered account
at tryhackme.com



Welcome to HackerFrogs Afterschool!

This is the fifth session
for network hacking!

Let's go over the concepts
we covered in the previous
session!

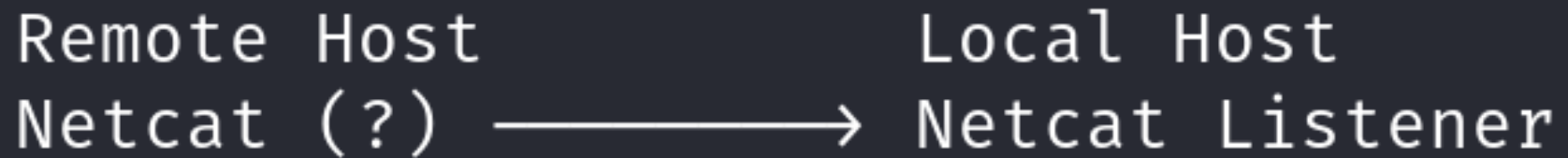


What is Remote Shell Access?

A remote shell is command-line interface (CLI) access to a remote server. This allows OS commands to be run through the remote shell



Reverse Shells

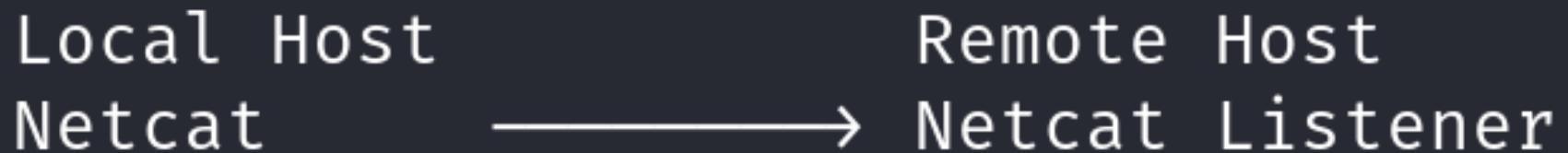


A diagram illustrating a reverse shell connection. It shows two columns. The left column is labeled 'Remote Host' and contains the text 'Netcat (?)'. The right column is labeled 'Local Host' and contains the text 'Netcat Listener'. A horizontal arrow points from 'Netcat (?)' to 'Netcat Listener'.

```
graph LR; A[Remote Host  
Netcat (?)] --> B[Local Host  
Netcat Listener]
```

Reverse shell access is where a listening port is created on the local host and the connection is established by the remote host connecting to that port

Bind Shells



```
graph LR; A[Local Host  
Netcat] --> B[Remote Host  
Netcat Listener]
```

The diagram illustrates a connection between a local host and a remote host. On the left, under the heading "Local Host", is the text "Netcat". On the right, under the heading "Remote Host", is the text "Netcat Listener". A horizontal arrow points from "Netcat" to "Netcat Listener", indicating a connection or data flow from the local host to the remote host.

And bind shells access is created when the remote host opens a networking port which is then connected to by the local host

This Session's Topics

- What is Password Cracking?
 - CrackStation Website
- Cracking Password Protected Zip Files
 - Cracking Linux Password Hashes
- Cracking SSH Private Key Passphrases

What is Password Cracking?



Password cracking is the act of determining the plaintext of a password hash by hashing a string and comparing it to the password hash

What is Password Cracking?

Hashed Password (MD5)

24f2536aeb9ecebbacfb4ccc0745c1ff

Plaintext Password

hackerfrogs

So if the plaintext password is hackerfrogs, we use MD5 hashing with that plaintext, and if the resulting hash and the hashed password is the same, then we've cracked the password

Accessing TryHackMe

Let's access this TryHackMe room to learn about cracking passwords access:

<https://tryhackme.com/room/crackthehash>

CrackStation Website



CrackStation is a good website to use if you're dealing with insecure hashing methods, such as MD5 and SHA1

Identifying Hash Types

```
-$ hash-identifier 24f2536aeb9ecebbacfb4ccc0745c1ff
```

Possible Hashs:

[+] MD5

[+] Domain Cached Credentials

A couple of different ways to identify the type of hash being used, including the CLI program, **hash-identifier**, and the **hashes.com** website

Cracking Zip File Password Hashes

```
└─$ unzip zip_crack.zip  
Archive:  zip_crack.zip  
[zip_crack.zip] zip_flag.txt password:
```

Zip files are a common file type that can be password protected, and we can extract the hash, then crack the password using a tool like John the Ripper

Cracking Linux Password Hashes

```
[root@localhost ~]# cat /etc/shadow  
root:$6$432i34ZEGoZkWcZw$VfY69D4.3pPNrW.RpJKmY8cnDc  
0H5Vwi0C2yPv0rhLhxoHCEgRuxznzN.:18604:0:99999:7:::
```

Linux password hashes can be captured and cracked, and this technique is used in network CTF exercises

Cracking SSH Private Key Hashes

```
——BEGIN OPENSSH PRIVATE KEY——  
b3B1bnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGY  
R/3d0KNBMoYrcfAAAAEAAAAAAEAAAEXAAAAB3NzaC1yc2E  
/oDep7wmVjIILRA46qWK2DRk7PIy6fBr8qQaAnHsXYZHu  
QjdA+4D06qxRGUyL5SZRnt+qeGN5z1dgBF69Gd1UjGIJ8
```

Another common file that can be cracked are the
passphrases for SSH private keys, which allow
users to login

Summary



Let's review the network hacking concepts we learned in this workshop:

What is Password Cracking?



Password cracking is the act of determining the plaintext of a password hash by hashing a string and comparing it to the password hash

Identifying Hash Types

```
-$ hash-identifier 24f2536aeb9ecebbacfb4ccc0745c1ff
```

```
Possible Hashs:
```

```
[+] MD5
```

```
[+] Domain Cached Credentials
```

A couple of different ways to identify the type of hash being used, including the CLI program, **hash-identifier**, and the **hashes.com** website

Cracking Zip File Password Hashes

```
└─$ unzip zip_crack.zip  
Archive:  zip_crack.zip  
[zip_crack.zip] zip_flag.txt password:
```

Zip files are a common file type that can be password protected, and we can extract the hash, then crack the password using a tool like John the Ripper

Cracking SSH Private Key Hashes

```
——BEGIN OPENSSH PRIVATE KEY——  
b3B1bnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGY  
R/3d0KNBMoYrcfAAAAEAAAAAAEAAAEXAAAAB3NzaC1yc2E  
/oDep7wmVjIILRA46qWK2DRk7PIy6fBr8qQaAnHsXYZHu  
QjdA+4D06qxRGUyL5SZRnt+qeGN5z1dgBF69Gd1UjGIJ8
```

Another common file that can be cracked are the
passphrases for SSH private keys, which allow
users to login

What's Next?

In the next HackerFrogs Afterschool Network Hacking workshop, we'll be learning how to do online password brute forcing attacks!

