

Hack The Box Meetup Onsite @ Sphères RAUM86 Zurich



HACKTHEBOX

Agenda



18.00 Uhr	Türöffnung
18.15 Uhr	Begrüßung und Setup
18.45 – 21.30 Uhr	Workshop Praxisteil
21.30 – 22.00 Uhr	Abschluss und Abschied

Admin

- Wi-Fi
- Food / drinks (input)
- Toilets (output)
- Pictures ok/nok?

Hosts



Antoine Neuenschwander
Tech Lead Bug Bounty Swisscom

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

Unauthorised 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)

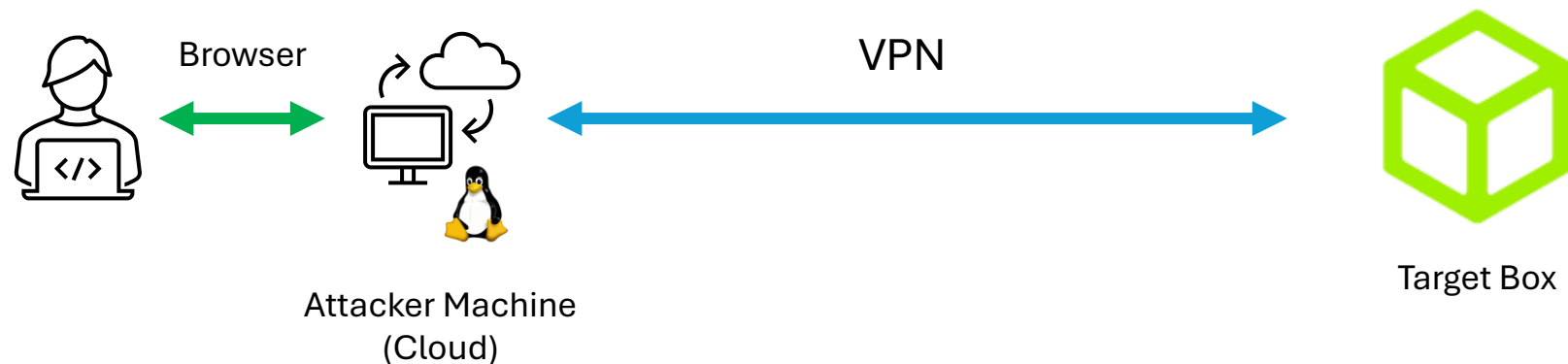
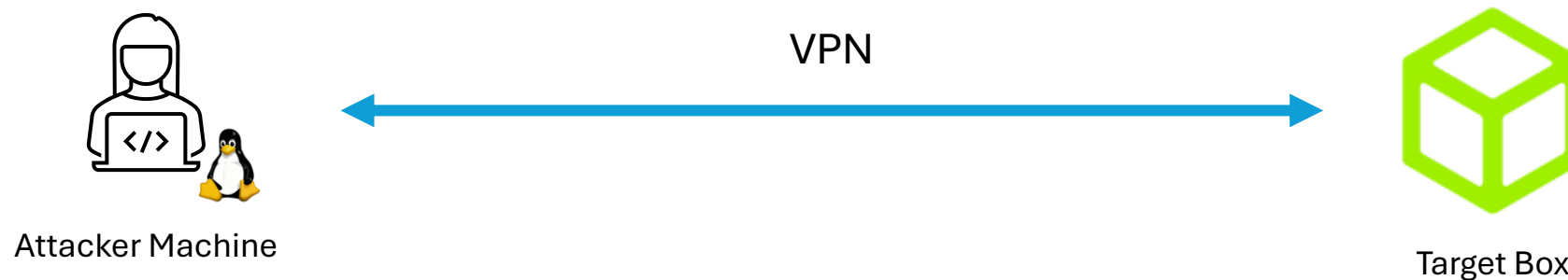




HACKTHEBOX

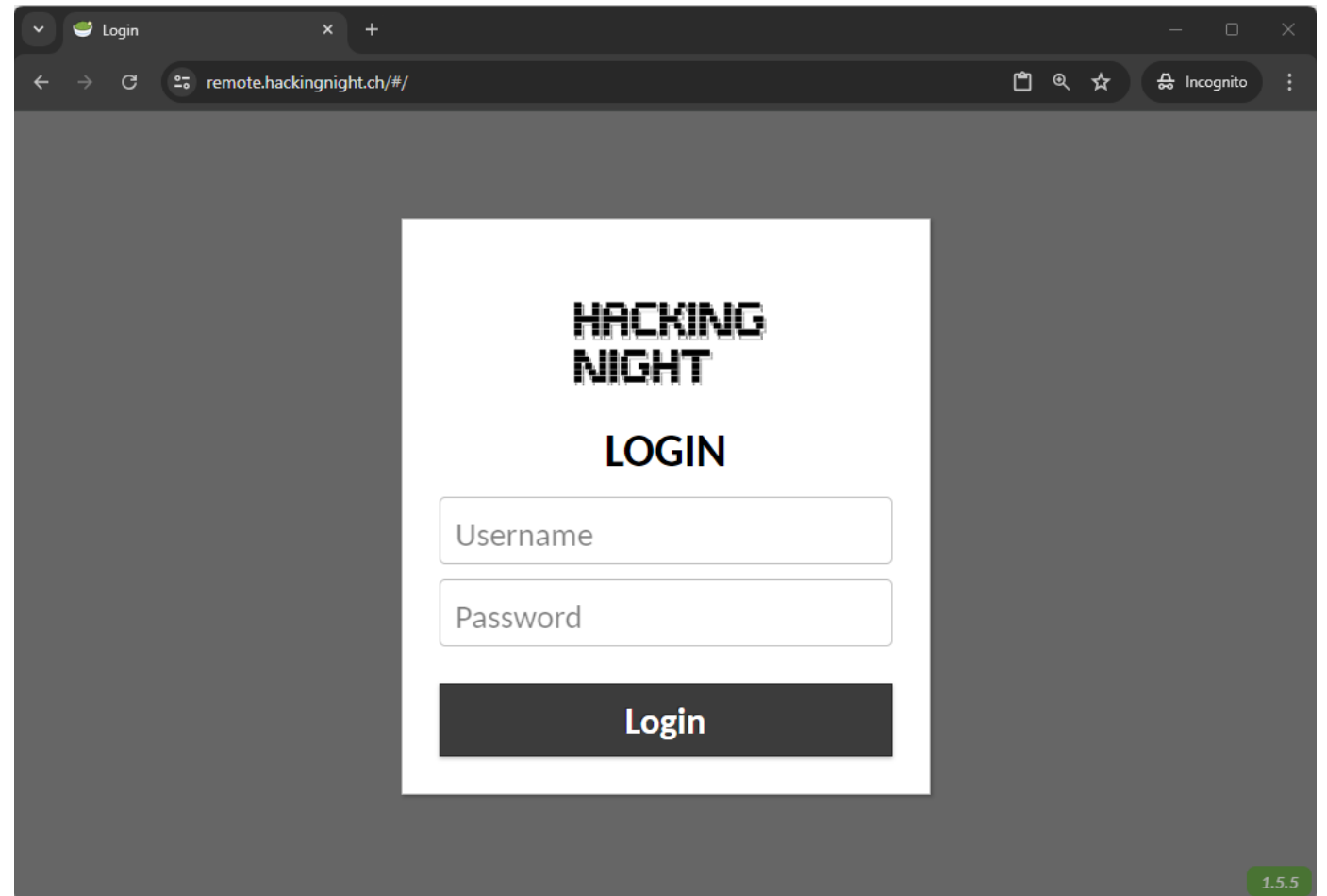
419 virtual machines (boxes)

Hacking Setup



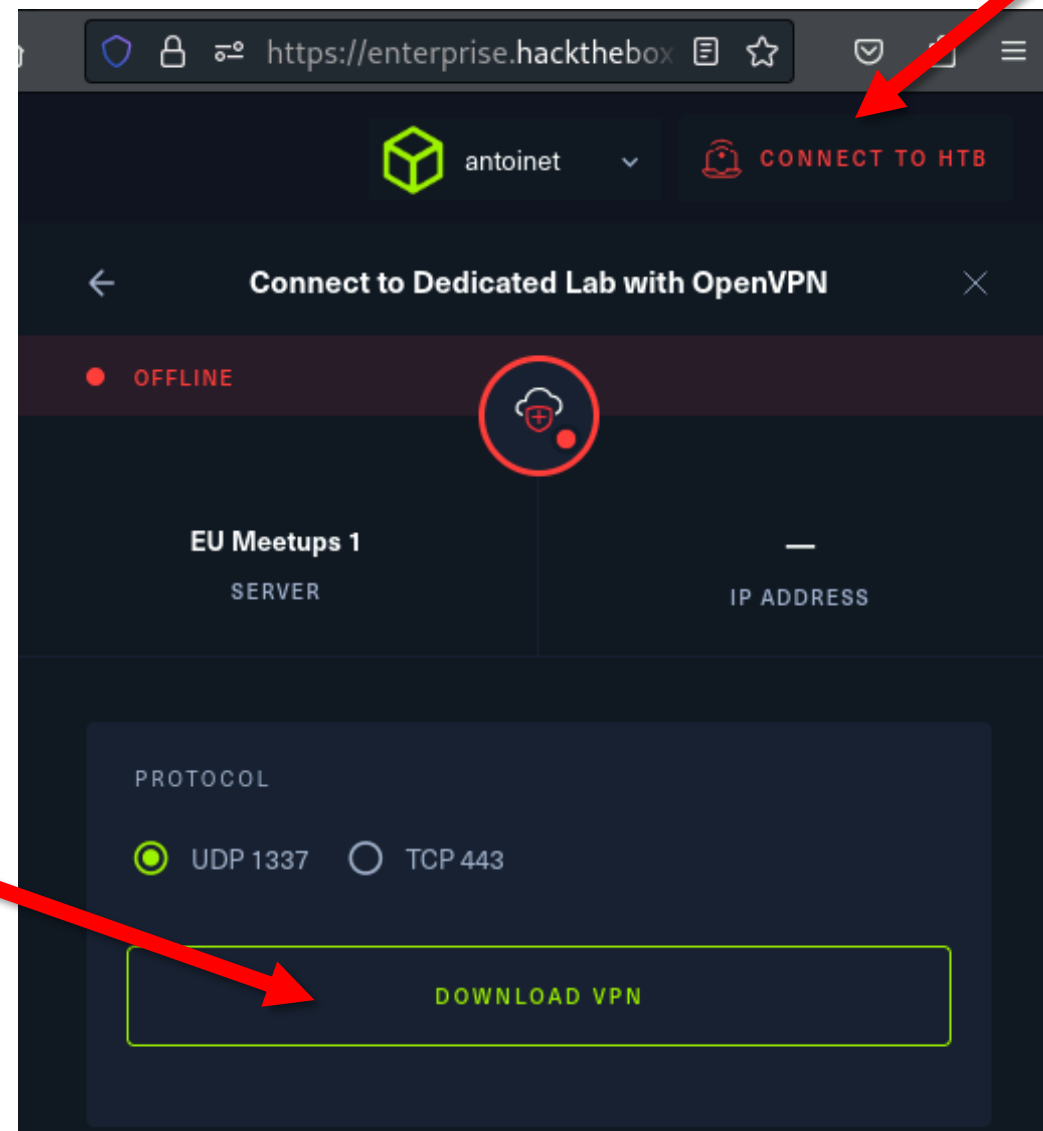
Connection to Attacker Machine

1. Visit remote.hackingnight.ch
2. Login with username **kali-X**
3. Password **hackingnight-X**



Configure VPN

Download VPN profile



Tips for the Browser-Based VM

- @-Symbol:
 - Alt-Gr = Ctrl-Alt
 - Ctrl-Alt 2
- Copy-Paste from the Host:
 - Press Ctrl-Alt-Shift
 - Paste or copy selection in the text field



Responder

- Very easy difficulty Windows box
- File inclusion vulnerability
- NetNTLMv2 challenge interception
- Hash cracking
- Windows Remoting

Exploitation Steps

1. Network Scanning & Service Enumeration
2. Web Application Security
3. NetNTLMv2 Challenge Interception
4. Remote Access

#1 Network Scanning & Service Enumeration

Application

Provides **network services** to applications

HTTP, FTP, SMTP, SSH, etc.

Transport

Ensures **reliable data transfer** between devices

TCP Port
1337

Internet

Routing of data packets within and between networks

IP Address
203.0.113.45

Network Access

Physical Transmission of Data

- Ethernet (LAN cable)
- Wi-Fi

MAC Address
48:2C:6A:1E:59:3F




TCP Ports

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

Service	No	Description
HTTP	80	Web traffic
HTTPS	443	Secure web traffic
FTP	20/21	File transfer
SSH	22	Secure shell access
SMTP	25	Email sending



Service Enumeration using nmap

nmap = the network mapper

`nmap <IP address>`

example:

`nmap 10.11.12.240`

#2 Web Application Security

LFI/RFI Vulnerability

- Local File Inclusion
- Remote File Inclusion



A screenshot of a web browser's address bar. The address bar has a search icon on the left and a URL in the center. The URL is `https://www.mycloud.ch/show?file=IMG1721308024.jpg`. The file path `IMG1721308024.jpg` is highlighted with a red rectangular box, illustrating a Remote File Inclusion (RFI) vulnerability where a remote file is being included into the application.

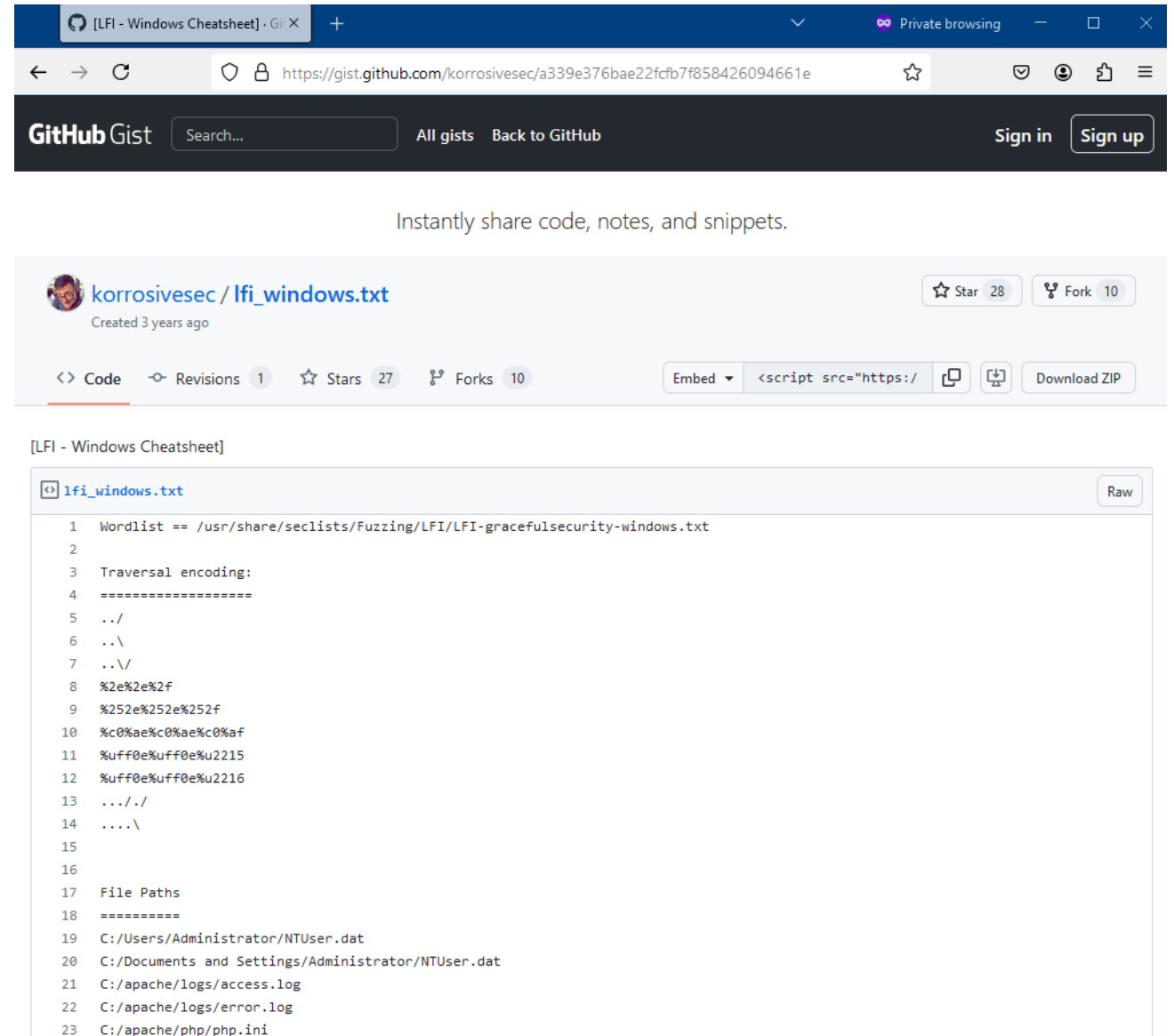
`https://www.mycloud.ch/show?file=IMG1721308024.jpg`

Local File Inclusion (LFI)

Check for world-readable files

- Linux:
/etc/passwd
- Windows:
C:/WINDOWS/System32/drivers/etc/hosts

Tip: try also relative paths ../../..



The screenshot shows a web browser displaying a GitHub Gist page. The URL is <https://gist.github.com/korrosivesec/a339e376bae22fcfb7f858426094661e>. The page title is "[LFI - Windows Cheatsheet] · Gist X". The user is "korrosivesec" and the file is "lfi_windows.txt", created 3 years ago. The file content is as follows:

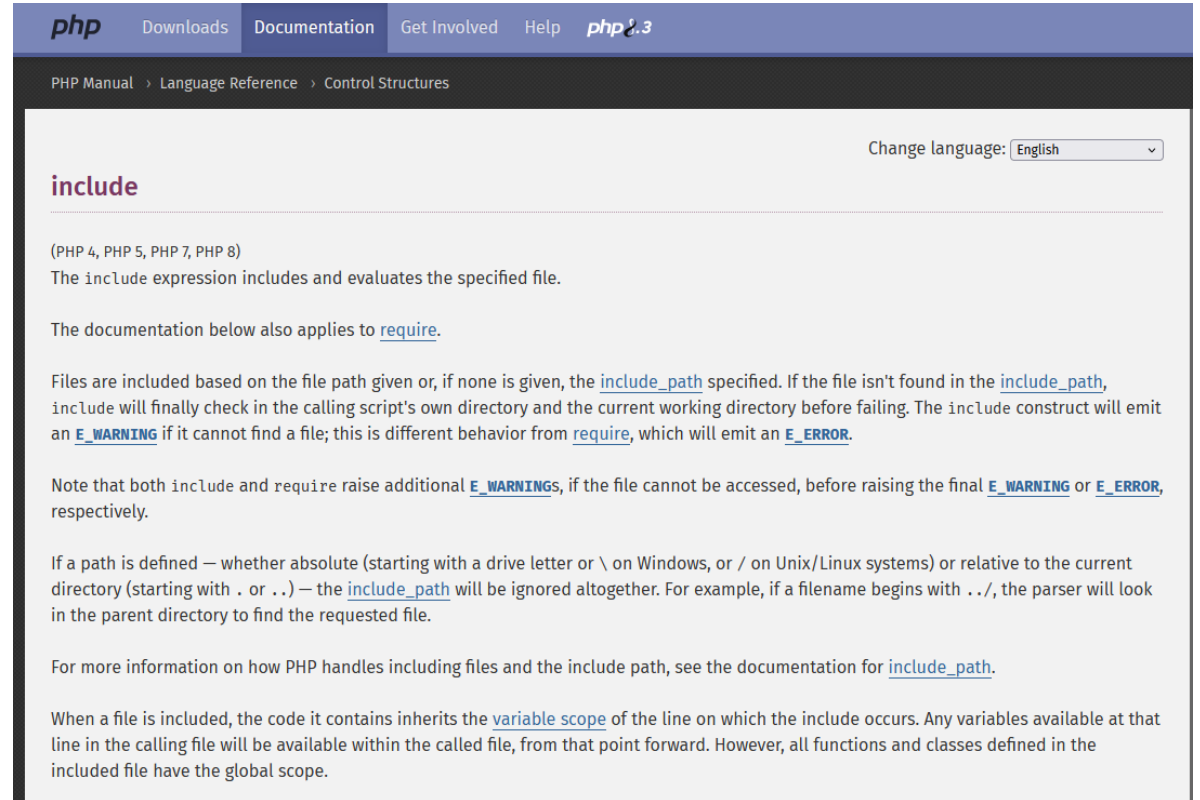
```
1 Wordlist == /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-windows.txt
2
3 Traversal encoding:
4 =====
5 ../
6 ..\
7 ../
8 %2e%2e%2f
9 %252e%252e%252f
10 %c0%ae%c0%ae%c0%af
11 %uff0e%uff0e%u2215
12 %uff0e%uff0e%u2216
13 ..././
14 ....\
15
16 File Paths
17 =====
18 C:/Users/Administrator/NTUser.dat
19 C:/Documents and Settings/Administrator/NTUser.dat
20 C:/apache/logs/access.log
21 C:/apache/logs/error.log
22 C:/apache/php/php.ini
```

<https://gist.github.com/korrosivesec/a339e376bae22fcfb7f858426094661e>

Remote File Inclusion (RFI)

Specify URI scheme for network access

- http://
- ftp://
- \\ (Windows UNC path)



The screenshot shows the PHP 8.3 documentation page for the `include` function. The page has a dark blue header with navigation links: [php](#), [Downloads](#), [Documentation](#), [Get Involved](#), [Help](#), and [php 8.3](#). Below the header, a breadcrumb trail reads: [PHP Manual](#) > [Language Reference](#) > [Control Structures](#). On the right, there is a language selector: "Change language: English".

include

(PHP 4, PHP 5, PHP 7, PHP 8)

The `include` expression includes and evaluates the specified file.

The documentation below also applies to [require](#).

Files are included based on the file path given or, if none is given, the [include_path](#) specified. If the file isn't found in the [include_path](#), `include` will finally check in the calling script's own directory and the current working directory before failing. The `include` construct will emit an [E_WARNING](#) if it cannot find a file; this is different behavior from [require](#), which will emit an [E_ERROR](#).

Note that both `include` and `require` raise additional [E_WARNINGS](#), if the file cannot be accessed, before raising the final [E_WARNING](#) or [E_ERROR](#), respectively.

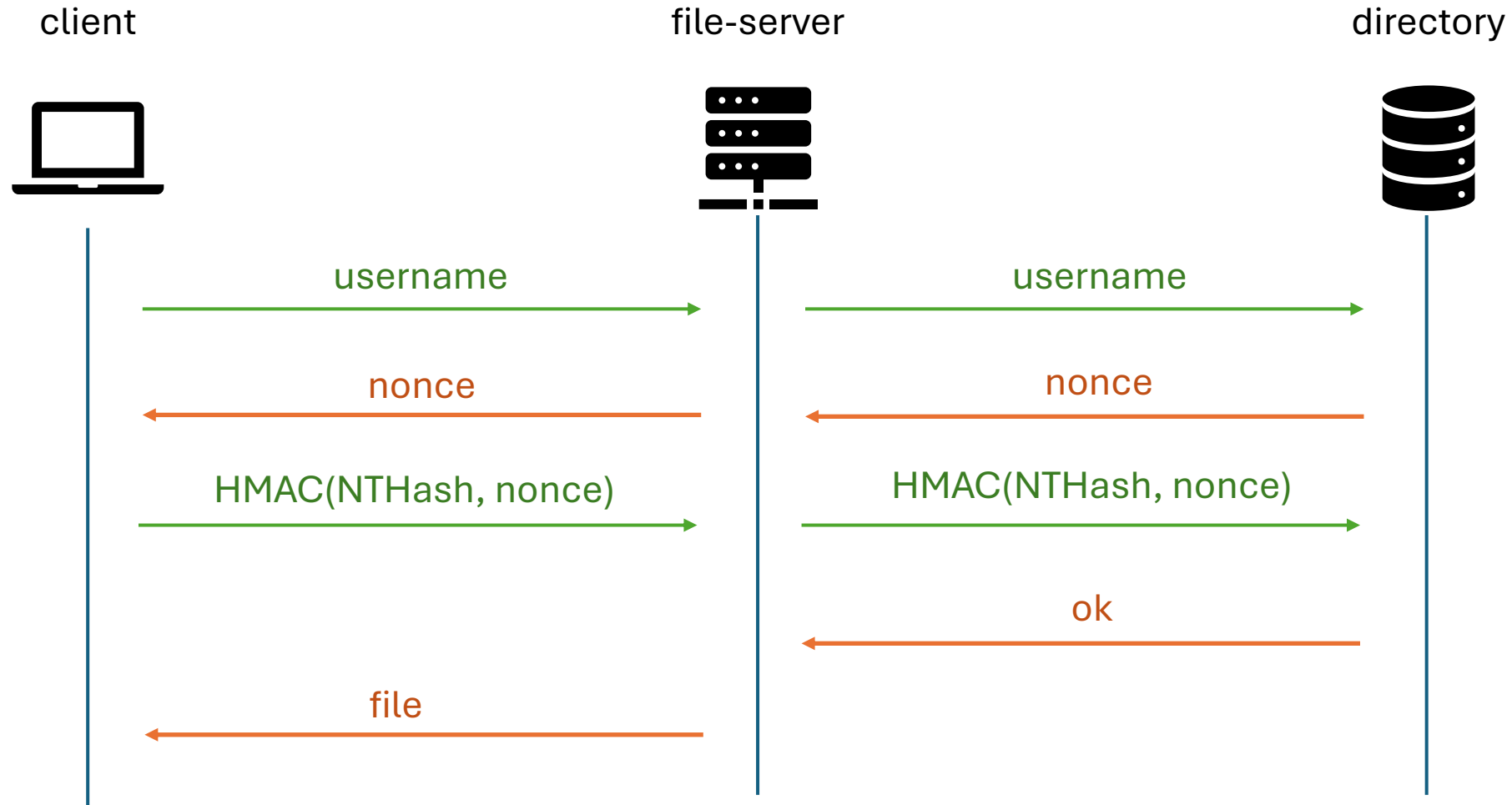
If a path is defined — whether absolute (starting with a drive letter or `\` on Windows, or `/` on Unix/Linux systems) or relative to the current directory (starting with `.` or `..`) — the [include_path](#) will be ignored altogether. For example, if a filename begins with `../`, the parser will look in the parent directory to find the requested file.

For more information on how PHP handles including files and the include path, see the documentation for [include_path](#).

When a file is included, the code it contains inherits the [variable scope](#) of the line on which the include occurs. Any variables available at that line in the calling file will be available within the called file, from that point forward. However, all functions and classes defined in the included file have the global scope.

#3 NetNTLMv2 Challenge Interception

Windows Single Sign-On (NetNTLMv2)



Confusing Terminology

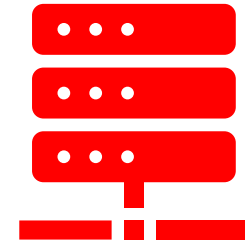
- **Hash function**
one-way function, aka hash, digest, fingerprint
- **NTHash**
Hash function used by Windows to store user passwords (sometimes called NTLM hash or NTLM)
- **NetNTLMv1/v2**
Challenge/response authentication protocol in Windows networks

See: <https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4>

NetNTLMv2 Interception with Responder

- Make the target connect to your evil server
- Use UNC path to force SMB (port 445)
- Single Sign-On Challenge/Response

evil-file-server





Password Recovery

- You cannot recover the password from the Challenge/Response
- But you have an “Oracle” that will validate the correct password
- Crack all the things!!1
- Use **john the ripper** / **hashcat**

#4 Remote Access

WinRM

Windows Remote Management

Article [Talk](#)

From Wikipedia, the free encyclopedia

WinRM (Windows Remote Management) is Microsoft's implementation of [WS-Management](#) in Windows which allows systems to access or exchange management information across a common network. Utilizing scripting objects or the built-in command-line tool, WinRM can be used with any remote computers that may have [baseboard management controllers \(BMCs\)](#) to acquire data. On Windows-based computers including WinRM, certain data supplied by [Windows Management Instrumentation \(WMI\)](#) can also be obtained.^[1]

Capture the flag

- Use a WinRM client for linux
- Find the flag on the target machine
- Win



Award Ceremony

Acknowledgements

Many Thanks **DEFCON Switzerland**

become a member!

<https://defcon-switzerland.org/>



Who we are and what we do

DC4131 is a local DEFCON Group and is organized as an association according to Swiss law. We are well-known for the Area41 conference (formerly hashdays) and regular member-events such as our Beer on Tuesday. DC4131 strives to support and foster the local hacker community. In 2023 Rhacklette joined DC4131 as a subgroup and organizes events and gatherings for female, inter, non-binary, trans and agender (FINTA) people in Security.

If you ask yourself, what DC4131 means: DC stands for DefCon, 41 is the area code for Switzerland and 31 is the area code for Berne, the capital of Switzerland.

Our statutes can be found [here](#) (German - but you know how to translate those to your preferred language right?)



Workshops



Thanks for your Participation ! You did Awesome !!!

Check out the Meetup Page for next events:

- 29.08.2024 Sphères Zurich
- 26.09.2024 Sphères Zurich



HACKTHEBOX