Enumeration and Information Leakage

JOÃO PAULO BARRACA

Network access

Accessing the network bypasses several security layers

- Laws, Buildings, Physical Access Control

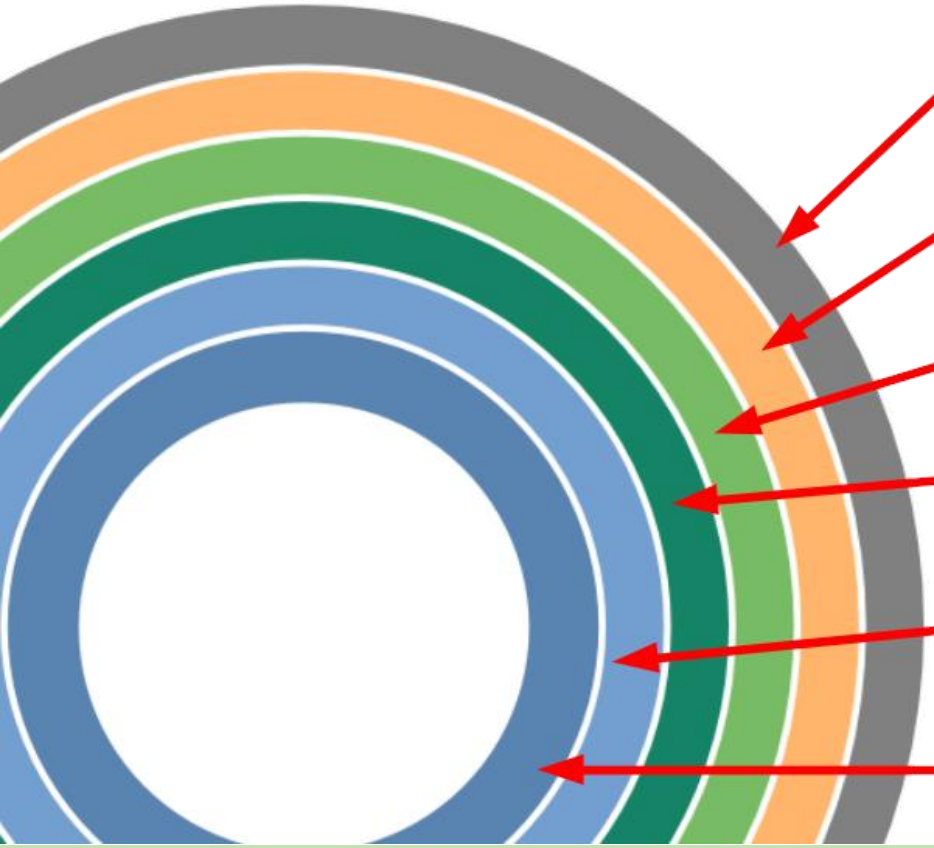
Attackers with access to a network can use it:

- To obtain information leaked
- To obtain information not protected
- To enumerate systems and hardware
- To discover and exploit vulnerabilities

Attackers can do it without notice

- If controls are not deployed
- If controls do not cover the attack path

Network access



Policies, Procedures, Awareness

Physical Infrastructure

Network Infrastructure

Physical Servers

Applications and Services

Data

The network

Information leakage

Entities provide information enabling the discovery of known vulnerabilities

- Greatly reduce the cost of an assessment by allowing a researcher/attacker to focus on a specific context

Most relevant:

- Broadcast Protocols: status information
- Banners: messages on connect
- Errors: errors provided on an illegal access
- Accounts: information about the existence of a user account
- Web page sources: information in web pages
- Supporting Files: information in other files available
- Event Timing: the time an event takes
- Cookies: cookies provided to clients

Errors

Messages provided to clients can disclose unnecessary information

- Errors from the infrastructure and support services
  - Attacker may force the system into an error condition by providing invalid input
- Response discrepancy during the interaction (CWE-204)

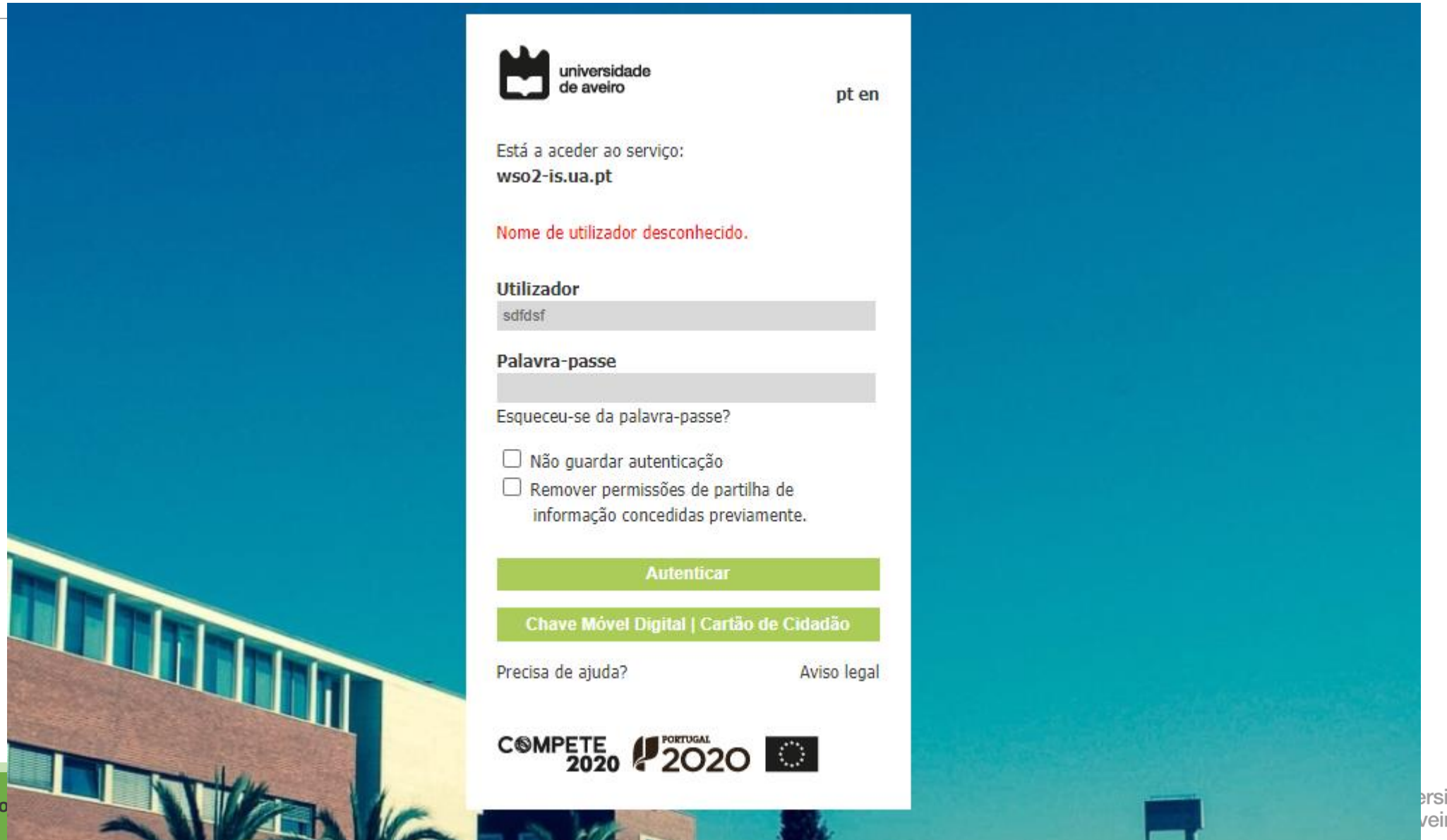
Provides information about internal processes, existing data, software versions.

- Stack traces, error messages

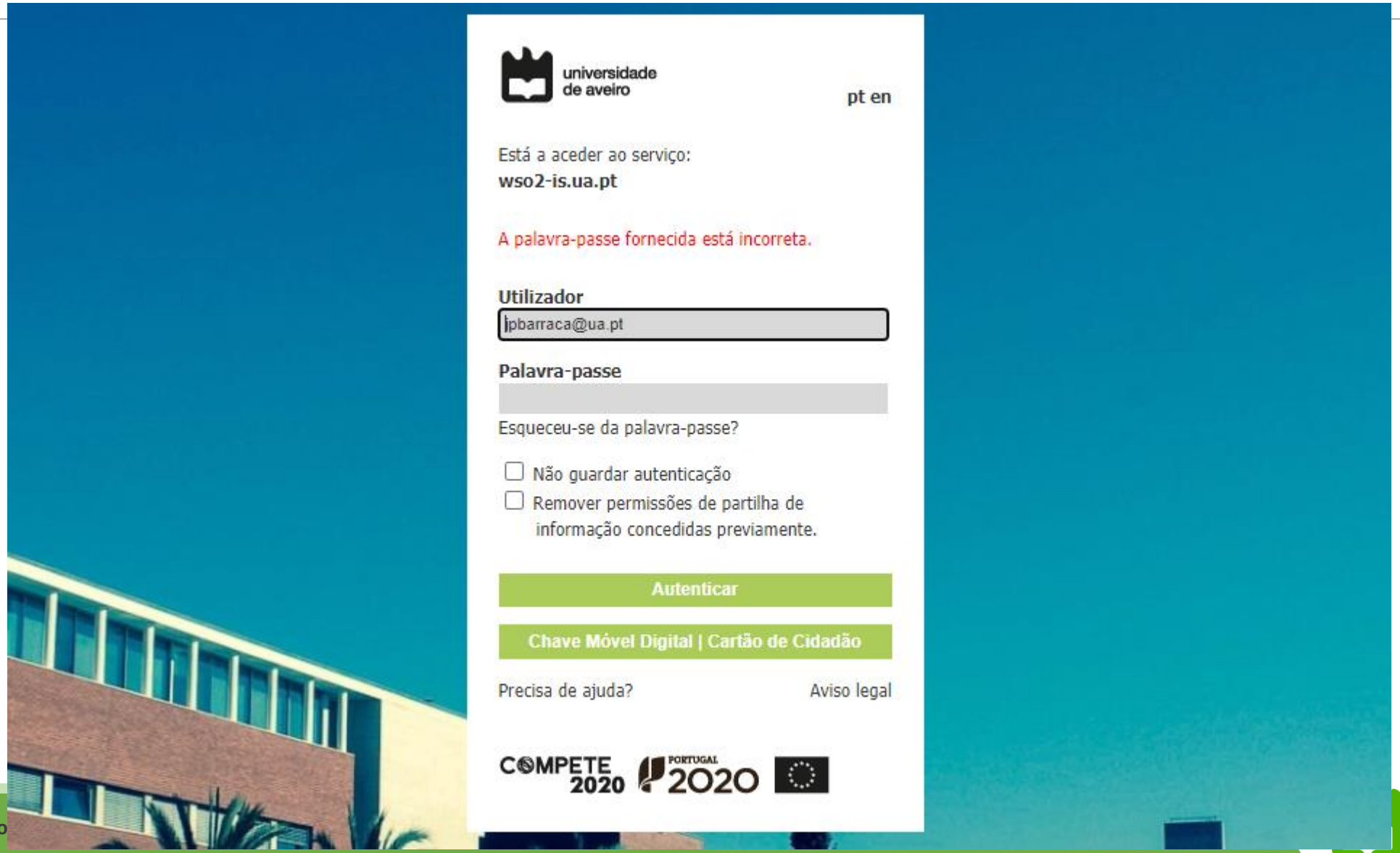
May allow to enumerate data (e.g, usernames)

- If there is a response discrepancy between existing/non-existing users

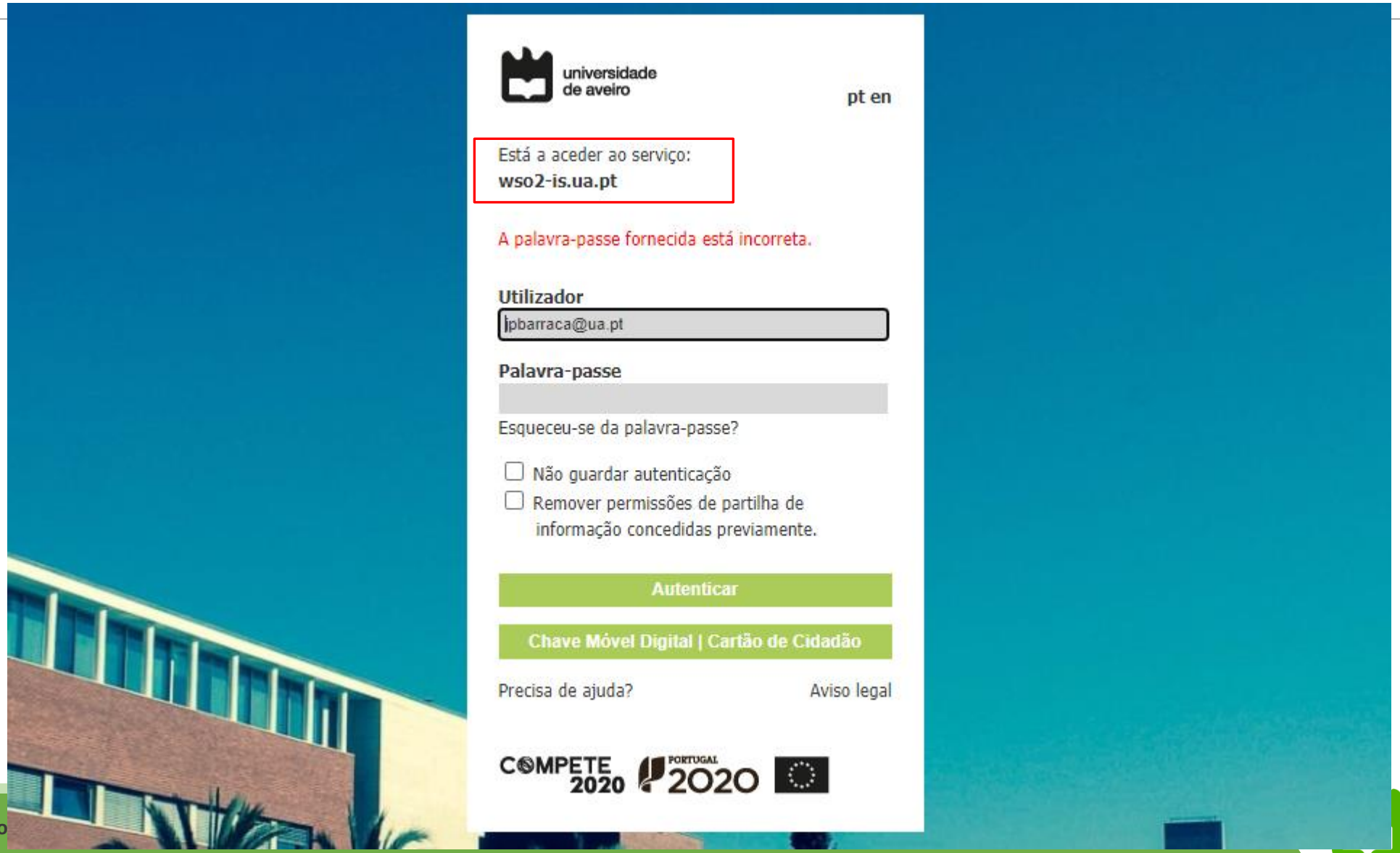
Errors – CWE-204 – Leaking Accounts



Errors – CWE-204 – Leaking Accounts



Errors – CWE-204 – Leaking Accounts



Errors – CWE-209

Errors - Mitigations

Do not provide verbose output to users, log it

- If you must, create the errors, identify sensitive data and filter it out
- In alternative, present a unique error code which can be used to track the issue by the support teams

Focus on the process as a whole

- authentication is either successful or unsuccessful
- a file can either be accessed or not

Web Sources and Support Files

Additional data may be present in web documents (JS, CSS, HTML)

- Left by developers to help testing, debugging and development
- This information may provide too much information about system internals
- Sometimes developers “hide it” by including this information in /robots.txt
  - Robots.txt works for search engine crawlers, but attracts attackers to sensitive areas

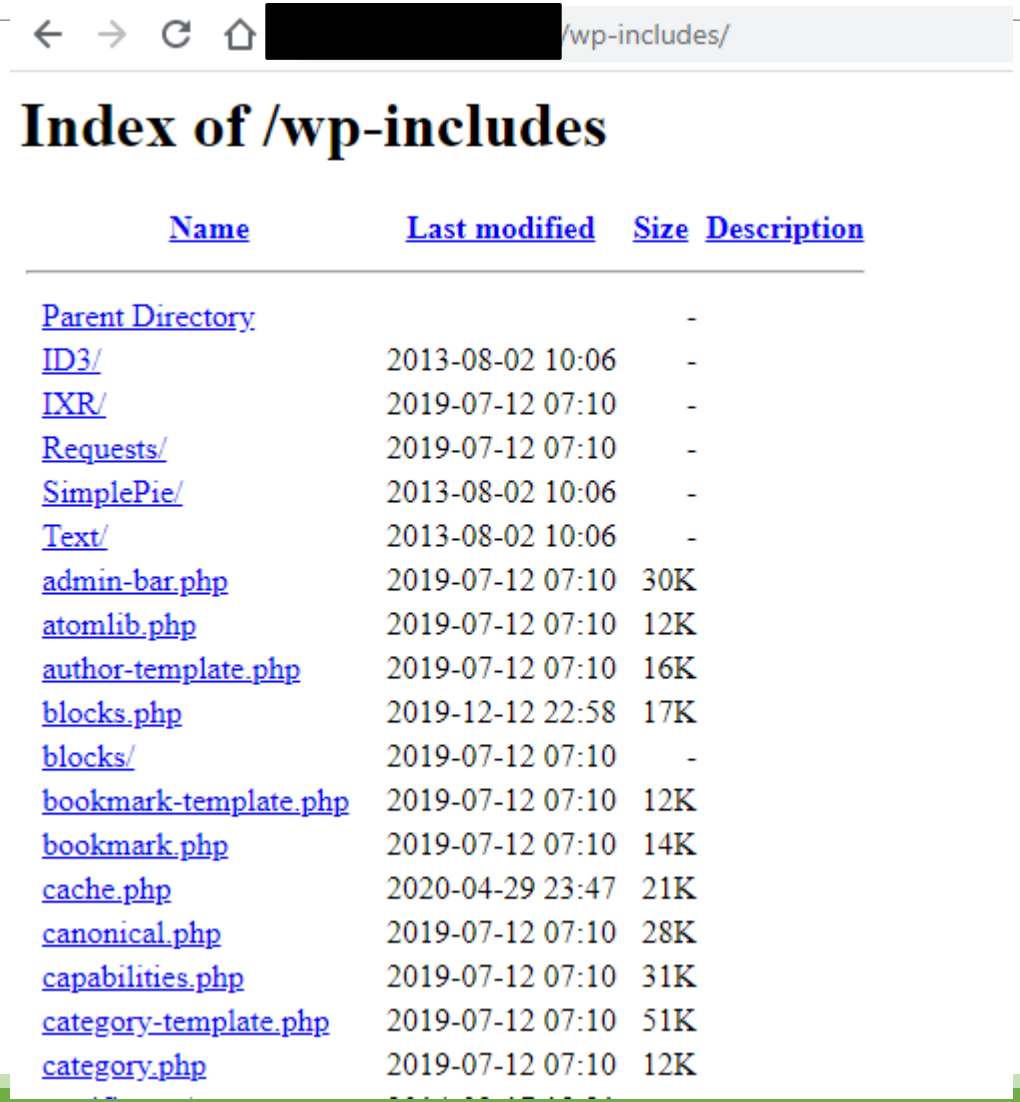
Impact:

- Allow fingerprinting remote stack
- Disclose sensitive information

Typical example:

- Backup files (.bck, .tar.gz, .zip)
- Robots.txt
- README and License files
- Log files left available
- Additional folders

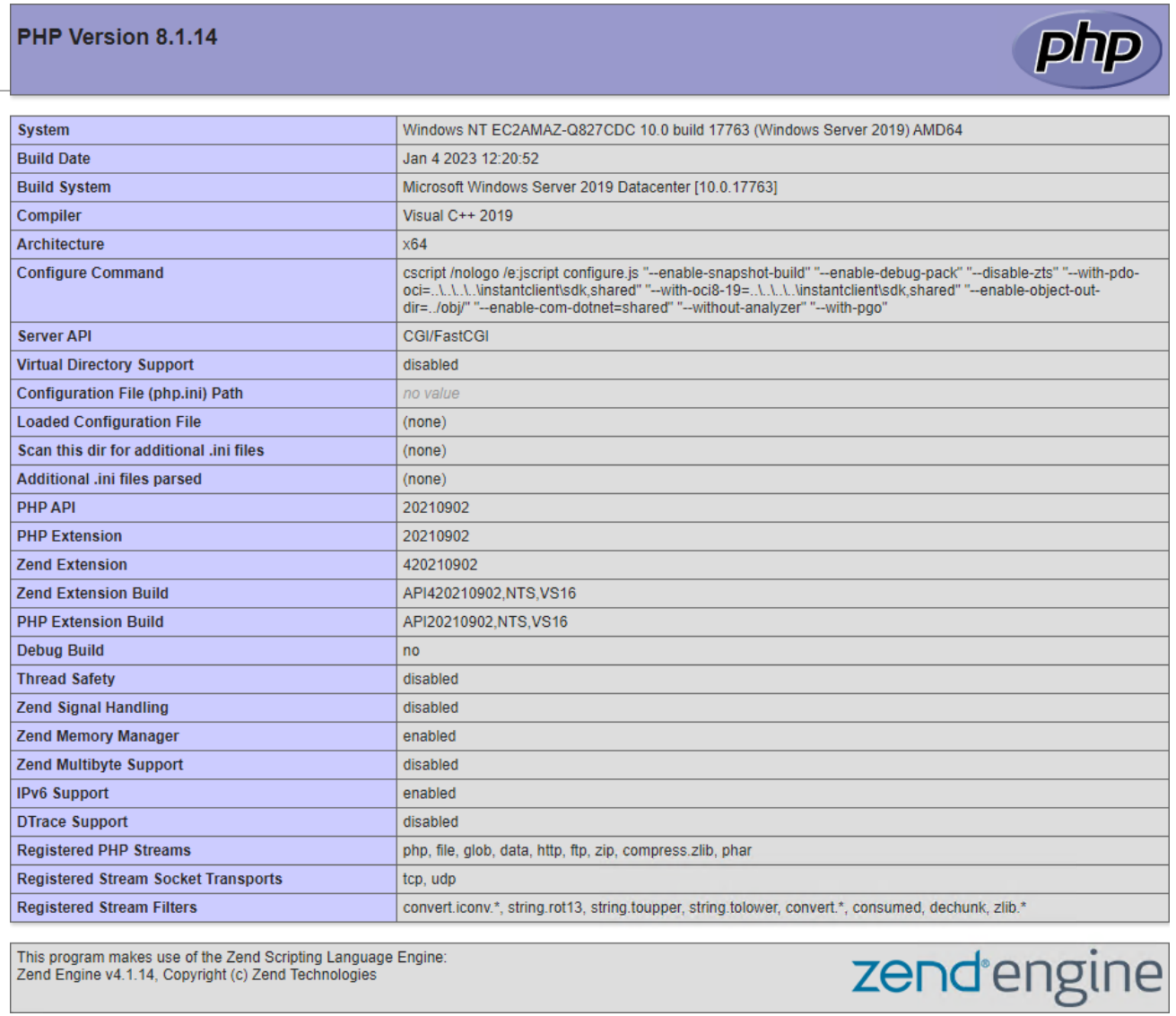
Web Sources and Support Files



Web Misconfiguration

phpinfo() is exposed to actors

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor



PHP Version 8.1.14

System	Windows NT EC2AMAZ-Q827CDC 10.0 build 17763 (Windows Server 2019) AMD64
Build Date	Jan 4 2023 12:20:52
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=..\..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	(none)
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,NTS,VS16
PHP Extension Build	API20210902,NTS,VS16
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, phar
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.1.14, Copyright (c) Zend Technologies

Cookies

Cookies sent in HTTP responses provide information about server stack

- Each framework make use of specific cookie formats

Impact: Platform stack disclosure

ASP.NET:

```
.AspNetCore.Session=CfDJ8KWPKY6%2BcwXLPdJQ90RvJmOMD2tC6sNMwD3RJ%2F0NT%2FAphxJ%2FuufL5UxKoNz
TRTR8%2Sx2nHrbR0lKRUyXUuKOUQ7avRwjwiND7h33wO9v2%2BLwbtYf%2rDUEKKpouty48CJEL9
```

PHP:

```
PHPSESSID=2ljc71pfksf3egdhharc5g0hr4; path=/
```

Ports

Network stack behaves differently whether the ports are open or closed

- **TCP**: replies with a TCP SYN,ACK (if open), or TCP RST (if closed)
- **UDP**: replies with a Higher Layer packet (if open), or an ICMP Port unreachable (if closed)
- **ICMP**: replies with ICMP Reply (or other)
- Firewalls also affect replies by altering or filtering packets

Services typically operate on well known ports

- All ports below 1024 are reserved for popular services
- Many ports above 1024 are also reserved

Impact: Allows knowing which services/hosts are available

Information leakage: Ports

Port scan: try to initiate a connection to a specific port

- May effectively initiate the connection or may simply start initiating it
  - **Full Connection**: Doing the TCP Three Way Handshake
  - **Half Connection**: Only sending the first TCP SYN
- A reply may indicate the existence / absence of a service
  - Existence if the connection is successful
  - Absence if an error is received
- A non reply may indicate the existence of a firewall

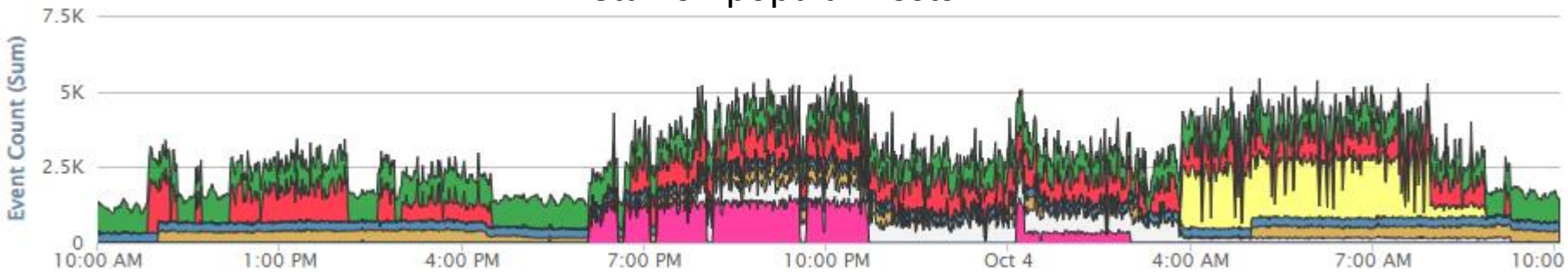
The way the host replies, allows fingerprinting its Operating System

Ports

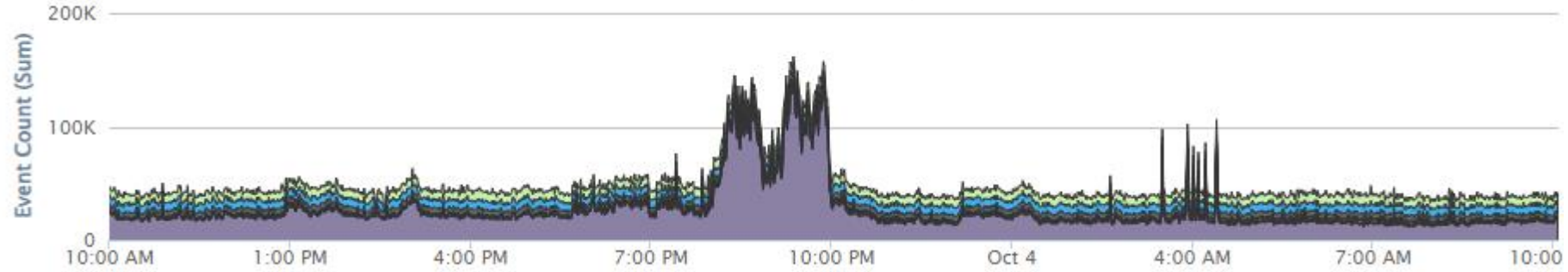
```
$ nmap gw

Nmap scan report for gw
Host is up (0.0016s latency).
Not shown: 997 closed ports

PORT   STATE    SERVICE
23/tcp filtered telnet
53/tcp open     domain
80/tcp open     http

MAC Address: 2C:97:B1:XX:XX:XX (Huawei Technologies)
Nmap done: 1 IP address (1 host up) scanned in 14.69 seconds
```

Ports Scan – Prevalence

Detail on popular hosts



Total enumeration attempts for 24h



Ports - Mitigation

Mitigation is limited as it exploits an inherent behavior

- Network port state will affect the replies

Firewalls should be sensitive to enumeration, blocking/logging the action

- Number of connections from a given host
- Different ports being accesses
- Session duration
- Rate of packets
- Specific fingerprints

Banners

Banners are textual or binary snippets provided to clients

- Immediately on connection, or after some request
- Most protocols are too chatty and will send some banner to help clients

Impact: attacker may gain knowledge about the software running

- Attacker can search for valid vulnerabilities
- Greatly narrows down the work to an attacker

Exploitation: connect to server and/send a probe

- Multiple probes can be sent to test the system
- Banner grabbing – technique of systematically probe entities for their banners

Vulnerable protocols: FTP, IMAP, HTTP, SSH, TELNET, LDAP, RTMP, MySQL…

Banners – Email - SMTP

```
$ nc server 25

220 EXCHANGE-2-A3.server Microsoft ESMTP MAIL Service ready at Thu,
22 Oct 2020 17:38:45 +0100









$ nc server1 25

220 mx.server1.com ESMTP 4si1750999wmg.70 – esmtp
```

Banners - HTTP

```
$ wget http://server --spider -S –q


HTTP/1.1 200 OK
Date: Thu, 22 Oct 2020 16:58:07 GMT
Server: Apache/2.4.25 (Debian) OpenSSL/1.0.2u
Last-Modified: Sun, 27 Dec 2015 10:32:42 GMT
ETag: "13c-527deb55ae63a"
Accept-Ranges: bytes
Content-Length: 316
Vary: Accept-Encoding
X-Clacks-Overhead: GNU Terry Pratchett
Keep-Alive: timeout=15, max=100
Link: <https://server/wp-json/>; rel="https://api.w.org/"
Set-Cookie: nm_transient_id=nmtr_954dce208296695d77d9141faeabe2e85c843546; path=/
Set-Cookie: PHPSESSID=2ljc79pfksj3e1dlhfr13h0ir5; path=/
Connection: Keep-Alive
Content-Type: text/htm
```

Server
Linux Distribution
OpenSSL Version

G: Send the message onto the next Clacks Tower
N: Do not log the message
U: At the end of the line, return the message
Terry Pratchett
Probably the sysadmin is around a specific community

Wordpress

PHP

Banners - HTTP

```
Cache-Control:  private
Content-Encoding: gzip
Content-Length:  8222
Content-Type:  text/html; charset=utf-8
Date:  Thu, 22 Oct 2020 19:22:51 GMT
Server: Microsoft-IIS/8.5
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-AspNetMvc-Version: 5.2
X-Powered-By: ASP.NET
```

Banners - SSH

```
$ ssh -v user@host

...
debug1: Remote protocol version 2.0, remote software version OpenSSH_7.2
...
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
debug1: kex: server->client cipher: aes128-ctr MAC: umac-64@openssh.com
compression: none
...
debug1: kex_input_ext_info: server-sig-algs=<rsa-sha2-256,rsa-sha2-512>
```

Banners

```
$ nmap -sV host
…

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http        lighttpd 1.4.53
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

Banners

```
$ nmap -sV host
…
Not shown: 994 closed ports

PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.9p1:
|       CVE-2019-6111       5.8       https://vulners.com/cve/CVE-2019-6111
|       CVE-2019-16905      4.4       https://vulners.com/cve/CVE-2019-16905
|       CVE-2019-6110       4.0       https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109       4.0       https://vulners.com/cve/CVE-2019-6109
|_      CVE-2018-20685      2.6       https://vulners.com/cve/CVE-2018-20685
80/tcp   open  http            lighttpd 1.4.53
|_http-server-header: lighttpd/1.4.53
| vulners:
|   cpe:/a:lighttpd:lighttpd:1.4.53:
|       CVE-2019-11072      7.5       https://vulners.com/cve/CVE-2019-11072
|_      CVE-2008-1531       4.3       https://vulners.com/cve/CVE-2008-1531
```

Banners – Preventive Actions

Restrict banners (if possible)

- Harden software configuration
- Not including banners in products for generic clients
- Be generic (e.g. Web Server instead of Apache)

Fake banners (if possible)

- Provide different values than standard.
- Provide generic values that mask the real application

Limit the verbosity in the banners (if possible)

- If headers required, no dot output version or platform.

OS Fingerprinting

Network stacks do not behave consistently, and there are specific behaviors

- Many RFCs contain optional behavior
- Some stacks have bugs
- Some stacks have optional behaviors
- Some stacks are not fully compliant (e.g., constrained devices)

Fingerprinting is possible by:

- Sending a sequence of probes
- Observing response
- Matching behavior against database

OS Fingerprinting

Process lacks specificity

- Fingerprint may not be found for unknown systems
- Fingerprint may match multiple systems
- Combination of open/closed ports may not allow a full fingerprint

Example: Nmap TCP Tests T2-T7

- TCP null (no flags set) pkt with the IP DF bit set and a window of 128 to an **open port**.
- TCP pkt with SYN, FIN, URG, PSH flags set and a window of 256 to an **open port**. IP DF bit is 0.
- TCP ACK pkt with IP DF (Do not Fragment) and a window of 1024 to an **open port**.
- TCP SYN pkt without IP DF and a window of 31337 to a **closed port**.
- TCP ACK pkt with IP DF and a window of 32768 to **a closed port**.
- TCP pkt with the FIN, PSH, URG flags set and a window of 65535 to a **closed port**. IP DF bit is 0.

OS Fingerprinting

```
$ uname –a
Linux server 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64 GNU/Linux

$ nmap –O host
Starting Nmap 7.91 ( https://nmap.org )
Host is up (0.00096s latency).
Not shown: 991 closed ports
…
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
```

OS Fingerprinting - Mitigations

Restrict the number of ports open

- Accurate fingerprinting relies on responses from open ports

Detect scanning and enumeration with a firewall specific rules

- Simple port maps and fingerprint attempts are easily recognized
- Advanced assessments, taking hours/days are not trivial to detect

If supported, enable network obfuscation mechanisms

- OS may emulate the behavior of another system