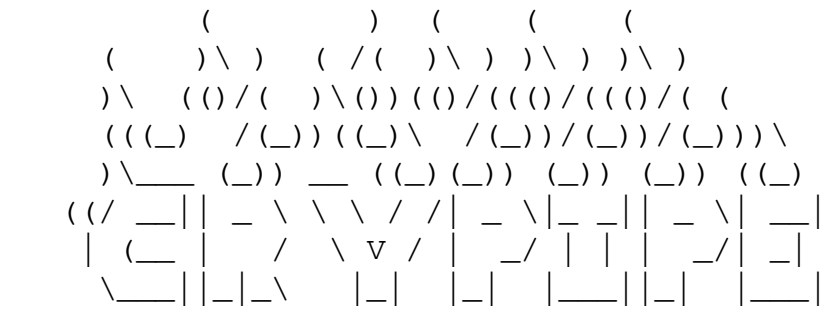

Report for subdomains of tiss.tuwien.ac.at

Nmap report

This is the result of the Nmap activity. **Here you can find only the relevant information**

Nmap scan for 128.131.33.131 : ['ewptest.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https

1 service unrecognized despite returning data. If you know the service/
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/14%Time=6643D941%P=x86_64-pc-linux-
SF:%r(GetRequest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npra
SF::\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cach
SF:x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<
SF:d>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:ice-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20ty
SF:\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x
SF:x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\
SF:Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height
SF:201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x2
SF:20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:8px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20
SF:0\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20
SF:0\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\
SF:}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\
SF:\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:ding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\
SF:\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x
SF:5px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{
SF:n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x
SF:\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:font-size:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unava
SF:ble\r\npragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=
SF:x20no-cache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>
SF:n\x20\x20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20con
SF:t=\"width=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x2
SF:tyle\x20type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\
SF:\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x
SF:elvetica,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:ine-height:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-
SF:e:\x2016px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:nt-size:\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x2
SF:0;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\
```

```
SF:20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20
SF:0\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r
SF:x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20
SF:0\x20\x20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20pa
SF:ng-left:\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x
SF:x20ul\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\
SF:\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20font-size:");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 23.80 seconds
```

Nmap scan for 128.130.32.75 : ['account.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE        VERSION
80/tcp  open  http-proxy     HAProxy http proxy 1.3.1 or later
443/tcp open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.10 seconds
```

Nmap scan for 128.130.32.96 : ['ewp.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https

2 services unrecognized despite returning data. If you know the service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===========
SF-Port80-TCP:V=7.80%I=7%D=5/14%Time=6643DB8F%P=x86_64-pc-linux-gnu%r(G
SF:equest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npragma:\x2
SF:-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cache,\x20n
SF:tore\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<head>\r
SF:x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-
SF:th,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20type=\"te
SF:css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x20\x20\
SF:\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\x20Aria
SF:x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\
SF:666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x20\x20\x
SF:x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:rgin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2028px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20\x20\x2
SF:20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\x20}\r\
SF:20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding
```

```
SF:2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.al
SF:\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2035px;
SF:n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x20}\r\n
SF:0\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font
SF:ze:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\
SF:pragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20n
SF:ache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x2
SF:20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"
SF:th=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style
SF:0type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20
SF:0\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helve
SF:a,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-
SF:ght:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:6px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x
SF:x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-s
SF::\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r
SF:x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x
SF:x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x2
SF:20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\
SF:\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x
SF:x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-l
SF::\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20u
SF:20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20
SF:0\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x2
SF:20\x20font-size:");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===========
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/14%Time=6643DB95%P=x86_64-pc-linux-
SF:%r(GetRequest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npra
SF::\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cach
SF:x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<
SF:d>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:ice-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20ty
SF:\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x
SF:x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\
SF:Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height
SF:201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x2
SF:20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:8px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20
SF:0\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20
SF:0\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\
SF:}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\
SF:\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20
```

```
SF:ding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\
SF:\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x
SF:5px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{
SF:n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x
SF:\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:font-size:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unava
SF:ble\r\npragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=
SF:x20no-cache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>
SF:n\x20\x20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20con
SF:t=\"width=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x2
SF:tyle\x20type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\
SF:\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x
SF:elvetica,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:ine-height:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-
SF:e:\x2016px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:nt-size:\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x2
SF:0;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\
SF:20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20
SF:0\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r
SF:x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20
SF:0\x20\x20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20pa
SF:ng-left:\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x
SF:x20ul\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\
SF:\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20font-size:");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.63 seconds
```

Nmap scan for 128.130.32.35 : ['keycloak.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE        VERSION
443/tcp open  ssl/http-proxy HAProxy http proxy 1.3.1 or later
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 23.04 seconds
```

Nmap scan for 128.130.32.40 : ['fis.tiss.tuwien.ac.at']

```
PORT     STATE SERVICE   VERSION
1720/tcp open  h323q931?

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 153.77 seconds
```

Nmap scan for 128.131.33.130 : ['epaytest.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https

1 service unrecognized despite returning data. If you know the service/
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/15%Time=6643E0A7%P=x86_64-pc-linux-
SF:%r(GetRequest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npra
SF::\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cach
SF:x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<
SF:d>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:ice-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20ty
SF:\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x
SF:x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\
SF:Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height
SF:201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x2
SF:20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:8px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20
SF:0\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20
SF:0\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\
SF:}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\
SF:\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:ding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\
SF:\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x
SF:5px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{
SF:n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x
SF:\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:font-size:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unava
SF:ble\r\npragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=
SF:x20no-cache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>
SF:n\x20\x20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20con
SF:t=\"width=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x2
SF:tyle\x20type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\
SF:\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x
SF:elvetica,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:ine-height:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-
SF:e:\x2016px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:nt-size:\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x2
SF:0;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\
SF:20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20
SF:0\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r
SF:x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20
SF:0\x20\x20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20pa
```

```
SF:ng-left:\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x
SF:x20ul\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\
SF:\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20font-size:");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 22.44 seconds
```

Nmap scan for 128.130.32.108 : ['raum.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https nginx/1.25.2

2 services unrecognized despite returning data. If you know the service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===========
SF-Port80-TCP:V=7.80%I=7%D=5/15%Time=6643E138%P=x86_64-pc-linux-gnu%r(G
SF:equest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npragma:\x2
SF:-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cache,\x20n
SF:tore\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<head>\r
SF:x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-
SF:th,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20type=\"te
SF:css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x20\x20\
SF:\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\x20Aria
SF:x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\
SF:666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x20\x20\x
SF:x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:rgin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2028px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20\x20\x2
SF:20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\x20}\r\
SF:20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding
SF:2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.al
SF:\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2035px;
SF:n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x20}\r\n
SF:0\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font
SF:ze:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\
SF:pragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20n
SF:ache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x2
SF:20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"
SF:th=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style
SF:0type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20
SF:0\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helve
SF:a,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-
SF:ght:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:6px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\
```

```
SF:\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x
SF:x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-s
SF::\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r
SF:x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x
SF:x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x2
SF:20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\
SF:\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x
SF:x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-l
SF::\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20u
SF:20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20
SF:0\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x2
SF:20\x20font-size:");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===========
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/15%Time=6643E13E%P=x86_64-pc-linux-
SF:%r(GetRequest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npra
SF::\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cach
SF:x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<
SF:d>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:ice-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20ty
SF:\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x
SF:x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\
SF:Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height
SF:201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x2
SF:20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:8px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20
SF:0\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20
SF:0\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\
SF:}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\
SF:\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:ding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\
SF:\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x
SF:5px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{
SF:n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x
SF:\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:font-size:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unava
SF:ble\r\npragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=
SF:x20no-cache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>
SF:n\x20\x20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20con
SF:t=\"width=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x2
SF:tyle\x20type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\
SF:\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x
SF:elvetica,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:ine-height:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-
SF:e:\x2016px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x
```

```
SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:nt-size:\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x2
SF:0;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\
SF:20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20
SF:0\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r
SF:x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20
SF:0\x20\x20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20pa
SF:ng-left:\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x
SF:x20ul\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\
SF:\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20font-size:");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.47 seconds
```

Nmap scan for 128.130.8.25 : ['fwd.tiss.tuwien.ac.at']

```
PORT      STATE SERVICE           VERSION
80/tcp    open  http              Cisco ASA firewall http config
443/tcp   open  ssl/https?
1720/tcp  open  h323q931?
10000/tcp open  snet-sensor-mgmt?
Service Info: Device: firewall

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 155.94 seconds
```

Nmap scan for 128.130.32.99 : ['raumkatalog.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https nginx/1.18.0

2 services unrecognized despite returning data. If you know the service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===========
SF-Port80-TCP:V=7.80%I=7%D=5/14%Time=6643DD71%P=x86_64-pc-linux-gnu%r(G
SF:equest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npragma:\x2
SF:-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cache,\x20n
SF:tore\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<head>\r
SF:x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-
SF:th,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20type=\"te
SF:css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x20\x20\
SF:\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\x20Aria
SF:x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\
SF:666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x20\x20\x
SF:x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:rgin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
```

```
SF:20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20font-size:\x2028px;
SF:n\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20\x20\x2
SF:20\x20\x20}\r\n\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\x20}\r\
SF:20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding
SF:2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.al
SF:\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2035px;
SF:n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x20}\r\n
SF:0\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font
SF:ze:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\
SF:pragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20n
SF:ache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x2
SF:20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"
SF:th=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style
SF:0type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20
SF:0\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helve
SF:a,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-
SF:ght:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:6px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x
SF:x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-s
SF::\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r
SF:x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x
SF:x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x2
SF:20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\
SF:\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x
SF:x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-l
SF::\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20u
SF:20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20
SF:0\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x2
SF:20\x20font-size:");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)===========
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/14%Time=6643DD77%P=x86_64-pc-linux-
SF:%r(GetRequest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npra
SF::\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cach
SF:x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<
SF:d>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:ice-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20ty
SF:\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x
SF:x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\
SF:Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height
SF:201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x2
SF:20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
```

```
SF:0\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:8px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20
SF:0\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20
SF:0\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\
SF:}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\
SF:\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:ding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\
SF:\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x
SF:5px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{
SF:n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x
SF:\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:font-size:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unava
SF:ble\r\npragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=
SF:x20no-cache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>
SF:n\x20\x20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20con
SF:t=\"width=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x2
SF:tyle\x20type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\
SF:\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x
SF:elvetica,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:ine-height:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-
SF:e:\x2016px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:nt-size:\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x2
SF:0;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\
SF:20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20
SF:0\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r
SF:x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20
SF:0\x20\x20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20pa
SF:ng-left:\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x
SF:x20ul\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\
SF:\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20font-size:");

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.20 seconds
```

Nmap scan for 128.130.32.68 : ['maintenance.tiss.tuwien.ac.at']

```
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https nginx/1.18.0

2 services unrecognized despite returning data. If you know the service
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==========
SF-Port80-TCP:V=7.80%I=7%D=5/15%Time=6643DF86%P=x86_64-pc-linux-gnu%r(G
SF:equest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npragma:\x2
```

SF:-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cache,\x20n
SF:tore\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<head>\r
SF:x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-
SF:th,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20type=\"te
SF:css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x20\x20\
SF:\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\x20Aria
SF:x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\
SF:666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x20\x20\x
SF:x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:rgin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2028px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20\x20\x2
SF:20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\x20}\r\
SF:20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding
SF:2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.al
SF:\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2035px;
SF:n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x20}\r\n
SF:0\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font
SF:ze:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\
SF:pragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20n
SF:ache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x2
SF:20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"
SF:th=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style
SF:0type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20
SF:0\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helve
SF:a,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-
SF:ght:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:6px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x
SF:x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x
SF:x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-s
SF::\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r
SF:x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x
SF:x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x2
SF:20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\
SF:\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x
SF:x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x2
SF:20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-l
SF::\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20u
SF:20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x2
SF:20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20
SF:0\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x2
SF:20\x20font-size:");
==========NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==========
SF-Port443-TCP:V=7.80%T=SSL%I=7%D=5/15%Time=6643DF8C%P=x86_64-pc-linux-
SF:%r(GetRequest,A4D,"HTTP/1\.0\x20503\x20Service\x20Unavailable\r\npra

```
SF::\x20no-cache\r\ncache-control:\x20private,\x20max-age=0,\x20no-cach
SF:x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>\r\n\x20\x20<
SF:d>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:ice-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x20<style\x20ty
SF:\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\x20\x20\x20\x
SF:x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x20Helvetica,\
SF:Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x20line-height
SF:201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2016px
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x20\x20\x20\x2
SF:20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x20\x20\x20\x20
SF:0\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x
SF:8px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20400;\r\n\x20
SF:0\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\n\x20\x20\x20
SF:0\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20\x20\x20\x20\
SF:}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20\x20\x20\x20\
SF:\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:ding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\
SF:\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x
SF:5px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20ul\x20{
SF:n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;\r\n\x20\x20\
SF:\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\x20\x20\x20\x
SF:\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:font-size:")%r(HTTPOptions,A4D,"HTTP/1\.0\x20503\x20Service\x20Unava
SF:ble\r\npragma:\x20no-cache\r\ncache-control:\x20private,\x20max-age=
SF:x20no-cache,\x20no-store\r\ncontent-type:\x20text/html\r\n\r\n<html>
SF:n\x20\x20<head>\r\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20con
SF:t=\"width=device-width,\x20initial-scale=1\">\r\n\r\n\x20\x20\x20\x2
SF:tyle\x20type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20body\x20{\r\n\
SF:\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"Helvetica\x20Neue\",\x
SF:elvetica,\x20Arial,\x20sans-serif;\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:ine-height:\x201\.66666667;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-
SF:e:\x2016px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333;\r\n\x
SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#fff;\r\n\x20\x20\x2
SF:20\x20\x20\x20\x20margin:\x202em\x201em;\r\n\x20\x20\x20\x20\x20\x20
SF:\n\x20\x20\x20\x20\x20\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:nt-size:\x2028px;\r\n\x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x2
SF:0;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20p\x20{\r\
SF:20\x20\x20\x20\x20\x20\x20\x20margin:\x200\x200\x2010px;\r\n\x20\x20
SF:0\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\.alert\.alert-info\x20{\r
SF:x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#F0F0F0;\r\n\x20
SF:0\x20\x20\x20\x20\x20\x20margin-top:\x2030px;\r\n\x20\x20\x20\x20\x2
SF:20\x20\x20padding:\x2030px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20
SF:0\x20\x20\x20\.alert\x20p\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20pa
SF:ng-left:\x2035px;\r\n\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x
SF:x20ul\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20padding-left:\x2051px;
SF:n\x20\x20\x20\x20\x20\x20\x20\x20position:\x20relative;\r\n\x20\x20\
SF:\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20li\x20{\r\n\x20\x20\x20\x20
SF:0\x20\x20\x20font-size:");
```

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 26.57 seconds

Joomscan report

This is the result of the Joomscan activity. **Here you can find only the relevant information Remeber: when the text is red, something interesting is found**

Joomscan for epaytest.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://epaytest.tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://epaytest.tiss.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for maintenance.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://maintenance.tiss.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for www.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] Joomla 1.0

[+] Core Joomla Vulnerability

[++] Joomla! 1.0.7 / Mambo 4.5.3 - (feed) Full Path Disclosure / Denial of Service

- EDB : https://www.exploit-db.com/exploits/1698/
- Joomla! 1.0.9 - (Weblinks) Blind SQL Injection
- CVE : CVE-2006-7247
- EDB : https://www.exploit-db.com/exploits/1922/
- Joomla! 1.0.x - 'ordering' Parameter Cross-Site Scripting
- CVE : CVE-2011-0005
- EDB : https://www.exploit-db.com/exploits/35167/
- Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Code Execution
- CVE : CVE-2015-8562 , CVE-2015-8566
- EDB : https://www.exploit-db.com/exploits/39033/

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://www.tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://www.tiss.tuwien.ac.at/mbl/
- https://www.tiss.tuwien.ac.at/fpl/
- https://www.tiss.tuwien.ac.at/course/
- https://www.tiss.tuwien.ac.at/curriculum/
- https://www.tiss.tuwien.ac.at/api/

- https://www.tiss.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for keycloak.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://keycloak.tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://keycloak.tiss.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for raumkatalog.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[++] Admin page : https://raumkatalog.tiss.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://raumkatalog.tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://raumkatalog.tiss.tuwien.ac.at/isallow:

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for prod.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] Joomla 1.0

[+] Core Joomla Vulnerability

[++] Joomla! 1.0.7 / Mambo 4.5.3 - (feed) Full Path Disclosure / Denial of Service

- EDB : https://www.exploit-db.com/exploits/1698/
- Joomla! 1.0.9 - (Weblinks) Blind SQL Injection
- CVE : CVE-2006-7247
- EDB : https://www.exploit-db.com/exploits/1922/
- Joomla! 1.0.x - 'ordering' Parameter Cross-Site Scripting
- CVE : CVE-2011-0005
- EDB : https://www.exploit-db.com/exploits/35167/
- Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Code Execution
- CVE : CVE-2015-8562 , CVE-2015-8566
- EDB : https://www.exploit-db.com/exploits/39033/

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://prod.tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://prod.tiss.tuwien.ac.at/mbl/

- https://prod.tiss.tuwien.ac.at/fpl/
- https://prod.tiss.tuwien.ac.at/course/
- https://prod.tiss.tuwien.ac.at/curriculum/
- https://prod.tiss.tuwien.ac.at/api/
- https://prod.tiss.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for account.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+] Checking robots.txt existing

[++] robots.txt is found

- path : https://account.tiss.tuwien.ac.at/robots.txt
- Interesting path found from robots.txt
- https://account.tiss.tuwien.ac.at/

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Joomscan for raum.tiss.tuwien.ac.at

[+] FireWall Detector

[+] Detecting Joomla Version

[++] ver 404

[+] Core Joomla Vulnerability

[+] Checking apache info/status files

[+] admin finder

[+ +] Admin page : https://raum.tiss.tuwien.ac.at/administrator/

[+] Checking robots.txt existing

[+] Finding common backup files name

[+] Finding common log files name

[+] Checking sensitive config.php.x file

Nikto report

This is the result of the Nikto activity. **Here you can find only the relevant information**
Remeber: some discoveries could be false positive, since nikto checks the response code for some vulnerabilities -> example XSS

Nikto scan for ewptest.tiss.tuwien.ac.at

- Target Host: ewptest.tiss.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Server is using a wildcard certificate: '*.apps.dev.csd.tuwien.ac.at'
- GET /: Hostname 'ewptest.tiss.tuwien.ac.at' does not match certificate's CN '*.apps.dev.csd.tuwien.ac.at'
- -3092: GET /css: /css: This might be interesting...

Nikto scan for epaytest.tiss.tuwien.ac.at

- Target Host: epaytest.tiss.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Cookie 2b7e99a78546ffec527b59b2b2fa0a35 created without the secure flag
- GET /: Cookie 2b7e99a78546ffec527b59b2b2fa0a35 created without the httponly flag
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
- GET /: Server is using a wildcard certificate: '*.apps.dev.csd.tuwien.ac.at'
- GET /: Hostname 'epaytest.tiss.tuwien.ac.at' does not match certificate's CN '*.apps.dev.csd.tuwien.ac.at'
- OPTIONS /: Allowed HTTP Methods: GET, HEAD, POST
- GET /base/webmail/readmsg.php?mailbox=../../../../../../../../../../../../../../../etc/passwd&id=1: Uncommon header 'referrer-policy' found, with contents: strict-origin-when-cross-origin
- GET /base/webmail/readmsg.php?mailbox=../../../../../../../../../../../../../../../etc/passwd&id=1: Cookie 32ef90736c68cde2ffc3e8473bc51a37 created without the secure flag
- GET /base/webmail/readmsg.php?mailbox=../../../../../../../../../../../../../../../etc/passwd&id=1: Cookie 32ef90736c68cde2ffc3e8473bc51a37 created without the httponly flag
- GET /auth/: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000; includeSubDomains
- GET /auth/: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /auth/: Uncommon header 'content-security-policy' found, with contents: frame-src 'self'; frame-ancestors 'self'; object-src 'none';
- GET /auth/: Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
- GET /auth/: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /auth/: Uncommon header 'x-robots-tag' found, with contents: none
- -3092: GET /auth/: /auth/: This might be interesting...

Nikto scan for maintenance.tiss.tuwien.ac.at

- Target Host: maintenance.tiss.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0x65ae7b42 0x500
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Cookie 24df2fc6fbe95e766d15b79f793dcce7 created without the secure flag
- GET /: Cookie 24df2fc6fbe95e766d15b79f793dcce7 created without the httponly flag
- GET /: Server is using a wildcard certificate: '*.tiss.tuwien.ac.at'

Nikto scan for www.tiss.tuwien.ac.at

- Target Host: www.tiss.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0xW/ face15babb1a659e322ab4dca9144756
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /: Uncommon header 'referrer-policy' found, with contents: strict-origin-when-cross-origin
- GET /: Uncommon header 'x-runtime' found, with contents: 0.511870
- GET /: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /: Uncommon header 'x-permitted-cross-domain-policies' found, with contents: none
- GET /: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000;
- GET /: Uncommon header 'link' found, with contents: </assets/application-5c967972c53ee3772fc55f8cc28a99b010c2e6d23a85af13170a0761088a840d.c rel=preload; as=style; nopush,</assets/components-3698f10359890ebdc6df62bdbccdf2527e105c88b29861f9bb7d4503ae09afde.c rel=preload; as=style; nopush,</assets/modules/zur_kenntnisnahme-bd2af1277d94fad5cc3b89ec15c06f86f0eed66886a54a8ea1883e3ba5b1bea4.css>; rel=preload; as=style; nopush,</assets/application_old-b4c55fed69d9e4560bcca046f9718b726d498ac654c7f1bc987980ec210f1471.js>; rel=preload; as=script; nopush,</assets/application-b2f9e2248fdb94e81e51b191a99ab4d1b591f0f7f376da42654a04c89b95355f.js>; rel=preload; as=script; nopush,</assets/modules/zur_kenntnisnahme-915f17214635e2d213c5f667a8ac6f6de4a3acc51bdd25d95146aabc0eb rel=preload; as=script; nopush
- GET /: Uncommon header 'x-rack-cors' found, with contents: miss; no-origin
- GET /: Uncommon header 'x-download-options' found, with contents: noopen
- GET /: Uncommon header 'x-request-id' found, with contents: 2301a53c-1a41-4fc6-86e6-cd3214a471f4
- GET /: Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
- GET /: Cookie TISS_LANG created without the secure flag
- GET /: Cookie TISS_LANG created without the httponly flag
- GET /: Cookie _tiss_session created without the secure flag
- GET /: Cookie _tiss_session created without the httponly flag
- GET /fpl/: Cookie FPL_SESSID created without the secure flag
- GET /fpl/: Cookie FPL_SESSID created without the httponly flag
- GET /fpl/: Cookie SERVERID created without the secure flag
- GET /fpl/: Cookie SERVERID created without the httponly flag
- GET //fpl/: File/dir '/fpl/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET //course/: File/dir '/course/' in robots.txt returned a non-forbidden or redirect

HTTP code (200)
- GET //curriculum/: File/dir '/curriculum/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /api/: Uncommon header 'access-control-allow-origin' found, with contents: *
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 6 entries which should be manually viewed.
- GET /: Hostname 'www.tiss.tuwien.ac.at' does not match certificate's CN 'tiss.tuwien.ac.at'
- -2946: GET /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- -3092: GET /access/: /access/: This might be interesting...
- -3092: GET /forum/: /forum/: This might be interesting...
- -3092: GET /library/: /library/: This might be interesting...
- -5107: GET /netutils/findata.stm?host=: /netutils/findata.stm?host=: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- GET /projects/weatimages/demo/index.php?ini[langpack]=http://cirt.net/rfiinc.txt?: Cookie PDB_SESSID created without the secure flag
- GET /projects/weatimages/demo/index.php?ini[langpack]=http://cirt.net/rfiinc.txt?: Cookie PDB_SESSID created without the httponly flag
- GET /maintenance/: /maintenance/: Admin login page/section found.

Nikto scan for keycloak.tiss.tuwien.ac.at

- Target Host: keycloak.tiss.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Cookie SERVERID created without the secure flag
- GET /: Cookie SERVERID created without the httponly flag
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
- OPTIONS /: Allowed HTTP Methods: GET, HEAD, POST
- GET /auth/: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /auth/: Uncommon header 'x-robots-tag' found, with contents: none
- GET /auth/: Uncommon header 'referrer-policy' found, with contents: no-referrer
- GET /auth/: Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
- GET /auth/: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000; includeSubDomains
- GET /auth/: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /auth/: Uncommon header 'content-security-policy' found, with contents: frame-src 'self'; frame-ancestors 'self'; object-src 'none';
- -3092: GET /auth/: /auth/: This might be interesting...

Nikto scan for raumkatalog.tiss.tuwien.ac.at

- Target Host: raumkatalog.tiss.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0x6424046d 0x1141
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Cookie 65427a94c32e670ba535b80ca6ae8889 created without the secure flag
- GET /: Cookie 65427a94c32e670ba535b80ca6ae8889 created without the httponly flag

- GET /robots.txt: "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
- GET /: Server is using a wildcard certificate: '*.tiss.tuwien.ac.at'
- GET /sitemap.xml: Cookie 6f7275265ca8331ce96a1a282dfde72f created without the secure flag
- GET /sitemap.xml: Cookie 6f7275265ca8331ce96a1a282dfde72f created without the httponly flag

Nikto scan for ewp.tiss.tuwien.ac.at

- Target Host: ewp.tiss.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Uncommon header 'digest' found, with contents: SHA-256=BjF7rUBJo+0WzLAaNd42jrhAJu8sJcvn8sWyV/aRQgQ=
- GET /: Uncommon header 'want-digest' found, with contents: SHA-256
- GET /: Cookie 8ac6864f375e42971d26ddf17c3231ba created without the secure flag
- GET /: Cookie 8ac6864f375e42971d26ddf17c3231ba created without the httponly flag
- GET /: Server is using a wildcard certificate: '*.tiss.tuwien.ac.at'
- -27071: GET /phpimageview.php?pic=javascript:alert(8754): /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- -3931: GET /myphpnuke/links.php?op=search&query=[script]alert('Vulnerable);[/script]?query=: /myphpnuke/links.php?op=search&query=[script]alert('Vulnerable);[/script]?query=: myphpnuke is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- -3931: GET /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- GET /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- GET /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.

Nikto scan for prod.tiss.tuwien.ac.at

- Target Host: prod.tiss.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0xW/d99111b1b9e395a91870f395c57b78dc
- GET /: Uncommon header 'x-download-options' found, with contents: noopen
- GET /: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /: Uncommon header 'x-xss-protection' found, with contents: 1; mode=block

- GET /: Uncommon header 'referrer-policy' found, with contents: strict-origin-when-cross-origin
- GET /: Uncommon header 'x-runtime' found, with contents: 0.600912
- GET /: Uncommon header 'x-rack-cors' found, with contents: miss; no-origin
- GET /: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000;
- GET /: Uncommon header 'x-permitted-cross-domain-policies' found, with contents: none
- GET /: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /: Uncommon header 'x-request-id' found, with contents: d5dda6b7-b17e-4559-a02e-a8d0100c8034
- GET /: Uncommon header 'link' found, with contents: </assets/application-5c967972c53ee3772fc55f8cc28a99b010c2e6d23a85af13170a0761088a840d.c rel=preload; as=style; nopush,</assets/components-3698f10359890ebdc6df62bdbccdf2527e105c88b29861f9bb7d4503ae09afde.c rel=preload; as=style; nopush,</assets/modules/zur_kenntnisnahme-bd2af1277d94fad5cc3b89ec15c06f86f0eed66886a54a8ea1883e3ba5b1bea4.css>; rel=preload; as=style; nopush,</assets/application_old-b4c55fed69d9e4560bcca046f9718b726d498ac654c7f1bc987980ec210f1471.js>; rel=preload; as=script; nopush,</assets/application-b2f9e2248fdb94e81e51b191a99ab4d1b591f0f7f376da42654a04c89b95355f.js>; rel=preload; as=script; nopush,</assets/modules/zur_kenntnisnahme-915f17214635e2d213c5f667a8ac6f6de4a3acc51bdd25d95146aabc0eb rel=preload; as=script; nopush
- GET /: Cookie TISS_LANG created without the secure flag
- GET /: Cookie TISS_LANG created without the httponly flag
- GET /: Cookie _tiss_session created without the secure flag
- GET /: Cookie _tiss_session created without the httponly flag
- GET /fpl/: Cookie FPL_SESSID created without the secure flag
- GET /fpl/: Cookie FPL_SESSID created without the httponly flag
- GET /fpl/: Cookie SERVERID created without the secure flag
- GET /fpl/: Cookie SERVERID created without the httponly flag
- GET //fpl/: File/dir '/fpl/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET //course/: File/dir '/course/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET //curriculum/: File/dir '/curriculum/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /api/: Uncommon header 'access-control-allow-origin' found, with contents: *
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 6 entries which should be manually viewed.
- GET /: Hostname 'prod.tiss.tuwien.ac.at' does not match certificate's CN 'tiss.tuwien.ac.at'
- -2946: GET /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- -3092: GET /access/: /access/: This might be interesting...
- -3092: GET /forum/: /forum/: This might be interesting...
- -3092: GET /library/: /library/: This might be interesting...
- -5107: GET /netutils/findata.stm?host=: /netutils/findata.stm?host=: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
- GET /projects/weatimages/demo/index.php?ini[langpack]=http://cirt.net/rfiinc.txt?:

Cookie PDB_SESSID created without the secure flag
- GET /projects/weatimages/demo/index.php?ini[langpack]=http://cirt.net/rfiinc.txt?: Cookie PDB_SESSID created without the httponly flag
- GET /maintenance/: /maintenance/: Admin login page/section found.

Nikto scan for account.tiss.tuwien.ac.at

- Target Host: account.tiss.tuwien.ac.at
- Target Port: 443
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Cookie KSERVERID created without the secure flag
- GET /: Cookie KSERVERID created without the httponly flag
- GET //: File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
- GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
- OPTIONS /: Allowed HTTP Methods: GET, HEAD, POST
- GET /auth/: Uncommon header 'x-content-type-options' found, with contents: nosniff
- GET /auth/: Uncommon header 'strict-transport-security' found, with contents: max-age=31536000; includeSubDomains
- GET /auth/: Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
- GET /auth/: Uncommon header 'content-security-policy' found, with contents: frame-src 'self'; frame-ancestors 'self'; object-src 'none';
- GET /auth/: Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
- GET /auth/: Uncommon header 'x-robots-tag' found, with contents: none
- -3092: GET /auth/: /auth/: This might be interesting...

Nikto scan for raum.tiss.tuwien.ac.at

- Target Host: raum.tiss.tuwien.ac.at
- Target Port: 443
- GET /: Server leaks inodes via ETags, header found with file /, fields: 0x653628b3 0x1b51
- GET /: The anti-clickjacking X-Frame-Options header is not present.
- GET /: Cookie 0ab2b3e303fed6b474132a24b0e2d771 created without the secure flag
- GET /: Cookie 0ab2b3e303fed6b474132a24b0e2d771 created without the httponly flag
- GET /: Server is using a wildcard certificate: '*.tiss.tuwien.ac.at'

Nuclei report

This is the result of the Nuclei activity. **Here you can find only the relevant information**

Remeber:

- **Green is used for low impact vulnerabilities**
- **Orange is used for medium impact vulnerabilities**
- **Red is used for high impact vulnerabilities**

Nuclei scan for ewptest.tiss.tuwien.ac.at

- [ssl-issuer] [ssl] [info] ewptest.tiss.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] ewptest.tiss.tuwien.ac.at:443 ["ewptest.tiss.tuwien.ac.at","www.ewptest.tiss.tuwien.ac.at"]

Nuclei scan for epaytest.tiss.tuwien.ac.at

- [ssl-issuer] [ssl] [info] epaytest.tiss.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] epaytest.tiss.tuwien.ac.at:443 ["www.epaytest.tiss.tuwien.ac.at","epaytest.tiss.tuwien.ac.at"]

Nuclei scan for fwd.tiss.tuwien.ac.at

- **[weak-cipher-suites:tls-1.0] [ssl] [low] fwd.tiss.tuwien.ac.at:443 ["[tls10 TLS_RSA_WITH_AES_256_CBC_SHA] "]**
- [tls-version] [ssl] [info] fwd.tiss.tuwien.ac.at:443 ["tls10"]

Nuclei scan for www.tiss.tuwien.ac.at

- [tls-version] [ssl] [info] www.tiss.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.0] [ssl] [low] www.tiss.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA] "]**
- [tls-version] [ssl] [info] www.tiss.tuwien.ac.at:443 ["tls11"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] www.tiss.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA] "]**
- [tls-version] [ssl] [info] www.tiss.tuwien.ac.at:443 ["tls12"]

Nuclei scan for keycloak.tiss.tuwien.ac.at

- [ssl-issuer] [ssl] [info] keycloak.tiss.tuwien.ac.at:443 ["GEANT Vereniging"]
- [ssl-dns-names] [ssl] [info] keycloak.tiss.tuwien.ac.at:443

["keycloak.tiss.tuwien.ac.at","www.keycloak.tiss.tuwien.ac.at"]

Nuclei scan for prod.tiss.tuwien.ac.at

- [tls-version] [ssl] [info] prod.tiss.tuwien.ac.at:443 ["tls10"]
- **[weak-cipher-suites:tls-1.0] [ssl] [low] prod.tiss.tuwien.ac.at:443 ["[tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- [tls-version] [ssl] [info] prod.tiss.tuwien.ac.at:443 ["tls11"]
- **[weak-cipher-suites:tls-1.1] [ssl] [low] prod.tiss.tuwien.ac.at:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]**
- [tls-version] [ssl] [info] prod.tiss.tuwien.ac.at:443 ["tls12"]

Dirb report

This is the result of the Dirb activity. **Here you can find only the relevant information**
Remeber: Only responses with code 200 are reported here