Анализ уязвимостей веб-сайта guewaz.narod.ru (193.109.247.248)

1) Wireshark, анализ TCP-трафика:

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 13 Oct 2021 07:40:32 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=15
Content-Encoding: gzip

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 13 Oct 2021 07:40:32 GMT
Content-Type: application/javascript; charset=UTF-8
Content-Length: 39881
Last-Modified: Tue, 12 Oct 2021 10:42:13 GMT
Connection: keep-alive
Keep-Alive: timeout=15
ETag: "61656685-9bc9"
Expires: Tue, 02 Nov 2021 07:40:32 GMT
Cache-Control: max-age=1728000
Accept-Ranges: bytes
```

По анализу TCP-трафика можно судить, что сервер – nginx (защищенный сервер, к которому сложно будет получить доступ)

Кодирование – gzip.

Версия HTTP – 1.1.

2) nmap -sS 193.109.247.248: скрытое TCP-сканирование (без соединения)

```
C:\Users\liaten>nmap -sS 193.109.247.248
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-13 11:14 Russia TZ 2 Standard Time
Nmap scan report for dev.ucoz.net (193.109.247.248)
Host is up (0.034s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
```

Делаем результат, что открыты порты: 21, 25, 80, 443

3) **nmap -sT 193.109.247.248:** TCP-сканирование с соединением

```
C:\Users\liaten>nmap -sT 193.109.247.248
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-13 11:20 Russia TZ 2 Standard Time
Nmap scan report for dev.ucoz.net (193.109.247.248)
Host is up (0.035s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 44.81 seconds
```

Новых портов не обнаружено

4) UDP-сканирование:

```
C:\Users\liaten>nmap -sU 193.109.247.248
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-13 11:23 Russia TZ 2 Standard Time
Nmap scan report for dev.ucoz.net (193.109.247.248)
Host is up (0.034s latency).
All 1000 scanned ports on dev.ucoz.net (193.109.247.248) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 38.03 seconds
```

Портов не обнаружено.

5) nmap -sV 193.109.247.248 -T 4 – сканирование служб (T - тайминг)

```
C:\Users\liaten>nmap -sV 193.109.247.248 -T 4
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-13 11:26 Russia TZ 2 Standard Time
Nmap scan report for dev.ucoz.net (193.109.247.248)
Host is up (0.035s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        Pure-FTPd
25/tcp  open  smtp       Postfix smtpd
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
Service Info: Host:  s206.ucoz.net

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.93 seconds
```

Найдены службы на портах:

21 – Pure-FTPd

25 – Postfix smtpd

6) **nmap -sC 193.109.247.248** – скриптовый движок nmap

```
C:\Users\liaten>nmap -sC 193.109.247.248
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-13 11:31 Russia TZ 2 Standard Time
Nmap scan report for dev.ucoz.net (193.109.247.248)
Host is up (0.034s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
|_smtp-commands: s206.ucoz.net, PIPELINING, SIZE 20971520, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp  open  http
|_http-title: 404 - \xD0\x9D\xD0\xB5 \xD1\x83\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xBE\xD1\x81\xD1\x8C \xD0\xB7\xD0\xB0\xD0\xB
3\xD1\x80\xD1\x83\xD0\xB7\xD0\xB8\xD1\x82\xD1\x8C \xD1\x81\xD0\xB0\xD0\xB9\xD1\x82
443/tcp open  https
| tls-nextprotoneg:
|_  http/1.1
| ssl-cert: Subject: commonName=*.narod.ru
| Subject Alternative Name: DNS:*.narod.ru, DNS:narod.ru
| Not valid before: 2021-06-09T00:00:00
|_Not valid after:  2022-06-09T23:59:59
| tls-alpn:
|_  http/1.1
|_http-title: Did not follow redirect to http://dev.ucoz.net/
|_ssl-date: TLS randomness does not represent time

Nmap done: 1 IP address (1 host up) scanned in 10.60 seconds
```

7) **nmap -A 193.109.247.248 –** определение всех версий ПО

```
C:\Users\liaten>nmap -A 193.109.247.248
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-13 12:31 Russia TZ 2 Standard Time
Nmap scan report for dev.ucoz.net (193.109.247.248)
Host is up (0.034s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        Pure-FTPd
25/tcp  open  smtp       Postfix smtpd
|_smtp-commands: s206.ucoz.net, PIPELINING, SIZE 20971520, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp  open  tcpwrapped
|_http-title: 404 - \xD0\x9D\xD0\xB5 \xD1\x83\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xBE\xD1\x81\xD1\x8C \xD0\xB7\xD0\xB0\xD0\xB
3\xD1\x80\xD1\x83\xD0\xB7\xD0\xB8\xD1\x82\xD1\x8C \xD1\x81\xD0\xB0\xD0\xB9\xD1\x82
|_http-server-header: nginx
443/tcp open  tcpwrapped
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: nginx
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.narod.ru
| Subject Alternative Name: DNS:*.narod.ru, DNS:narod.ru
| Not valid before: 2021-06-09T00:00:00
|_Not valid after:  2022-06-09T23:59:59
| tls-nextprotoneg:
|_  http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|general purpose|WAP
Running (JUST GUESSING): Grandstream embedded (89%), Linux 3.X|2.4.X|2.6.X (89%)
OS CPE: cpe:/h:grandstream:gxv3275 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_ke
rnel:2.6
Aggressive OS guesses: Grandstream GXV3275 video phone (89%), Linux 3.2 - 3.8 (89%), Linux 3.3 (87%), Linux 3.6 (86%)
, Tomato 1.27 - 1.28 (Linux 2.4.20) (85%), Linux 2.6.32 - 2.6.39 (85%), Linux 2.6.38 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops
Service Info: Host:  s206.ucoz.net

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   1.00 ms  192.168.100.1
2   7.00 ms  178.68.156.1
3   26.00 ms 185.140.148.19
4   ... 9
10  35.00 ms dev.ucoz.net (193.109.247.248)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.46 seconds
```

Обнаружились аргументы SMTP-COMMANDS для 25 порта:

```
25/tcp  open  smtp       Postfix smtpd
|_smtp-commands: s206.ucoz.net, PIPELINING, SIZE 20971520, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

Определена система:

```
Aggressive OS guesses: Grandstream GXV3275 video phone (89%), Linux 3.2 - 3.8 (89%), Linux 3.3 (87%), Linux 3.6 (86%)
, Tomato 1.27 - 1.28 (Linux 2.4.20) (85%), Linux 2.6.32 - 2.6.39 (85%), Linux 2.6.38 (85%)
```