Анализ уязвимостей веб-сайта guewaz.narod.ru

Узнаем ip адрес сайта: 193.109.247.248

Командная строка

```
Microsoft Windows [Version 10.0.19042.1237]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Игорь>ping guewaz.narod.ru

Обмен пакетами с guewaz.narod.ru [193.109.247.248] с 32 байтами данных:
Ответ от 193.109.247.248: число байт=32 время=33мс TTL=58
Ответ от 193.109.247.248: число байт=32 время=33мс TTL=58
Ответ от 193.109.247.248: число байт=32 время=33мс TTL=58
Ответ от 193.109.247.248: число байт=32 время=32мс TTL=58

Статистика Ping для 193.109.247.248:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 32мсек, Максимальное = 33 мсек, Среднее = 32 мсек
```

В Wireshark мы видим сервер, на котором работает веб-сайт – **nginx**, но не видим его версию, что усложняет поиск уязвимостей для этого сайта.

Wireshark · Следовать TCP Поток (tcp.stream eq 10) · Ethernet

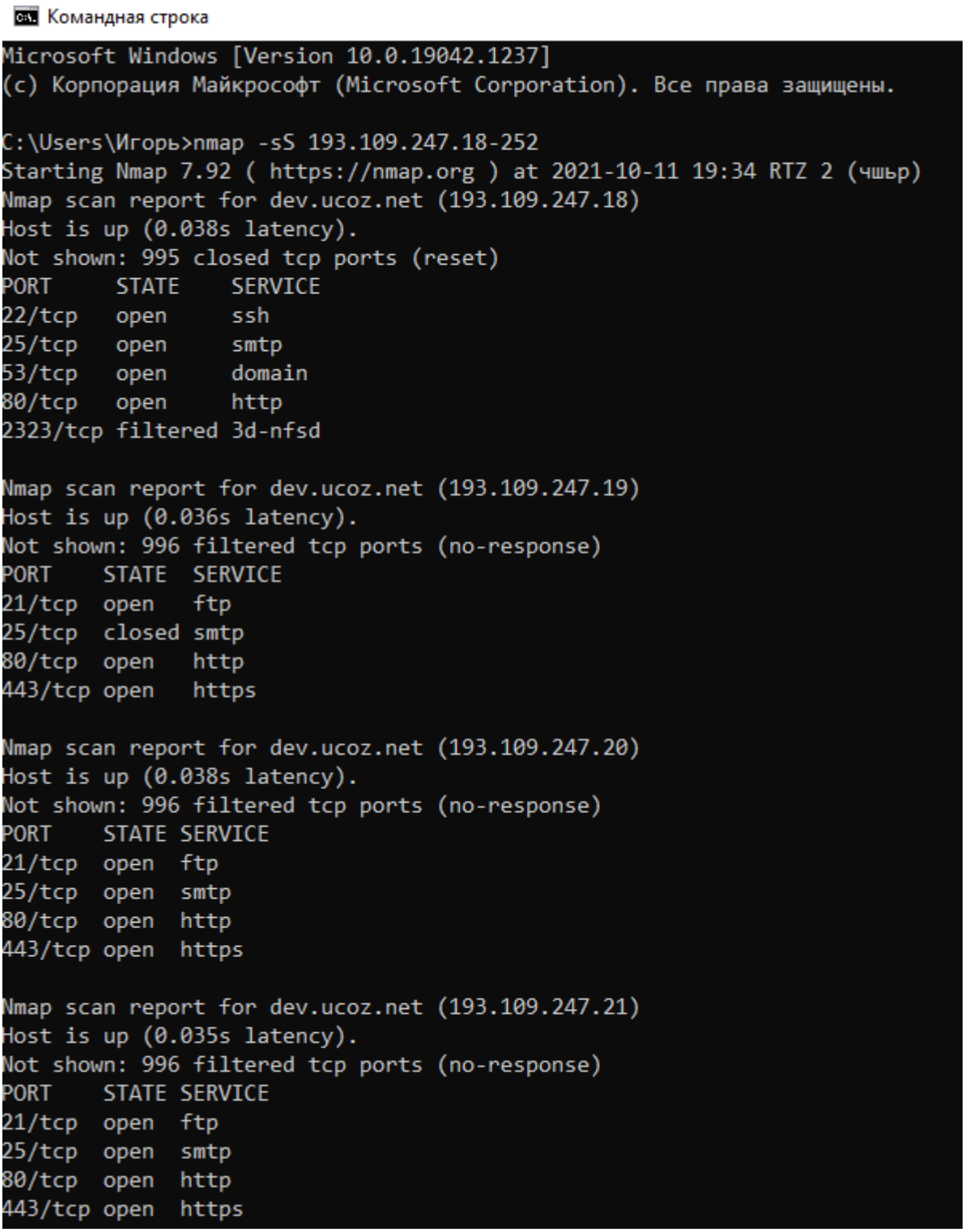
```
GET /img/d.gif HTTP/1.1
Host: guewaz.narod.ru
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/94.0.4606.71 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://guewaz.narod.ru/
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: hotlog=1; b=b; ipz=1

HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 11 Oct 2021 15:33:24 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=15
ETag: W/"611e66ae-1d5b"
Content-Encoding: gzip
```

Осуществим интрузивный целевой поиск с помощью команды **nmap - PT**:

```
C:\Users\Игорь>nmap -PT 193.109.247.0/24 -sn
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 19:30 RTZ 2 (чшьр)
Nmap scan report for dev.ucoz.net (193.109.247.18)
Host is up (0.038s latency).
Nmap scan report for dev.ucoz.net (193.109.247.32)
Host is up (0.033s latency).
Nmap scan report for dev.ucoz.net (193.109.247.99)
Host is up (0.033s latency).
Nmap scan report for mx0.ucozmail.com (193.109.247.128)
Host is up (0.034s latency).
Nmap scan report for dev.ucoz.net (193.109.247.137)
Host is up (0.034s latency).
Nmap scan report for dev.ucoz.net (193.109.247.146)
Host is up (0.034s latency).
Nmap scan report for dev.ucoz.net (193.109.247.149)
Host is up (0.036s latency).
Nmap scan report for dev.ucoz.net (193.109.247.211)
Host is up (0.033s latency).
Nmap scan report for dev.ucoz.net (193.109.247.212)
Host is up (0.039s latency).
Nmap scan report for dev.ucoz.net (193.109.247.215)
Host is up (0.035s latency).
Nmap scan report for dev.ucoz.net (193.109.247.221)
Host is up (0.038s latency).
Nmap scan report for dev.ucoz.net (193.109.247.251)
Host is up (0.037s latency).
Nmap scan report for dev.ucoz.net (193.109.247.252)
Host is up (0.036s latency).
Nmap done: 256 IP addresses (13 hosts up) scanned in 3.28 seconds
```

По результатам TCP сканирования было найдено 13 хостов в сети.

Проведем скрытое TCP сканирование портов: **nmap -sS 193.109.247.18-252**



Получаем список и статус портов.

Запустим сканирование служб, командой **nmap –sV 193.109.247.18-252**

Командная строка

```
Nmap done: 235 IP addresses (132 hosts up) scanned in 134.62 seconds

C:\Users\Игорь> nmap -sV 193.109.247.18-252 -T 4
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 19:42 RTZ 2 (чшьр)
Stats: 0:02:44 elapsed; 22 hosts completed (64 up), 64 undergoing Service Scan
Service scan Timing: About 97.70% done; ETC: 19:44 (0:00:02 remaining)
Stats: 0:02:49 elapsed; 22 hosts completed (64 up), 64 undergoing Service Scan
Service scan Timing: About 97.70% done; ETC: 19:44 (0:00:02 remaining)
Stats: 0:02:54 elapsed; 22 hosts completed (64 up), 64 undergoing Service Scan
Service scan Timing: About 97.70% done; ETC: 19:44 (0:00:03 remaining)
Nmap scan report for dev.ucoz.net (193.109.247.18)
Host is up (0.038s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 5.3p1 Debian 3 (protocol 2.0)
25/tcp   open     tcpwrapped
53/tcp   open     domain     (unknown banner: unknown)
80/tcp   open     http       UcoZXSrv/1.4.9
2323/tcp filtered 3d-nfsd
2 services unrecognized despite returning data. If you know the service/version,
s at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=10/11%Time=616469A6%P=i686-pc-windows-windows%r
SF:(DNSVersionBindReqTCP,42,"\0@\0\x06\x85\0\0\x01\0\x01\0\x01\0\0\x07vers
SF:ion\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x08\x07unknown\
SF:xc0\x0c\0\x02\0\x03\0\0\0\0\0\x02\xc0\x0c");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.92%I=7%D=10/11%Time=616469A1%P=i686-pc-windows-windows%r
SF:(GetRequest,1DE,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x2
SF:0UcoZXSrv/1\.4\.9\r\nDate:\x20Mon,\x2011\x20Oct\x202021\x2016:43:14\x20
SF:GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20286\r\nConnecti
```

Мы нашли OpenSSH 5.3. В Банке данных угроз безопасности информации видим:

Описание уязвимости	Уязвимость средства криптографической защиты OpenSSH связана с различной реакцией сервера на запросы аутентификации при наличии и отсутствии соответствующих учетных записей. Эксплуатация уязвимости может позволить нарушителю выявить существующие записи пользователей путем отправки специально сформированных запросов аутентификации
Вендор	ООО «РусБИТех-Астра», OpenBSD Project, Siemens AG, Сообщество свободного программного обеспечения, Oracle Corp.
Наименование ПО	Astra Linux (запись в едином реестре российских программ №369), OpenSSH , SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP , Debian GNU/Linux , Sun ZFS Storage Appliance Kit
Версия ПО	раскрыть 1.5 «Смоленск» (Astra Linux) от 2.3 до 7.7 (OpenSSH) V2.6.0 (SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP) jessie (Debian GNU/Linux)

Введем команду **nmap -sC 193.109.247.248**

```
C:\Users\Игорь> nmap -sC 193.109.247.248
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 20:13 RTZ 2 (чшьр)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.10% done; ETC: 20:13 (0:00:20 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.33% done; ETC: 20:13 (0:00:00 remaining)
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
|_smtp-commands: s206.ucoz.net
80/tcp  open  http
|_http-title: 404 - \xD0\x9D\xD0\xB5 \xD1\x83\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xBE\xD1\x
D1\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
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Did not follow redirect to http://dev.ucoz.net/
| 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

Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
```

Видим версию HTTP 1.1. Эта версия подвержена уязвимости при обходе каталогов, поскольку ему не удается в достаточной степени очистить вводимые пользователем данные. Использование этой проблемы позволит злоумышленнику просматривать произвольные локальные файлы и каталоги в контексте веб-сервера. Собранная информация может помочь в проведении дальнейших атак.

Введя команду **nmap -A 193.109.247.248 -T 4** увидим следующее:

```
C:\Users\Игорь>nmap -A 193.109.247.248 -T 4
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-11 20:18 RTZ 2 (чшьр)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.00% done; ETC: 20:20 (0:01:39 remaining)
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.85% done; ETC: 20:18 (0:00:02 remaining)
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, OK , 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\xB3\x
D1\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
| tls-nextprotoneg:
|_  http/1.1
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx
| 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
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_kern
1:2.6
Aggressive OS guesses: Grandstream GXV3275 video phone (89%), Linux 3.2 - 3.8 (89%), Linux 3.3 (87%), Linux 3.6 (86%),
omato 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: 11 hops
Service Info: Host:  s206.ucoz.net

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   1.00 ms  192.168.100.1
2   3.00 ms  sktv-bras7.sz.ip.rostelecom.ru (212.48.195.200)
3   5.00 ms  212.48.195.152
4   24.00 ms 185.140.148.31
5   ... 10
11  34.00 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 25.25 seconds
```

Есть версия Pure-FTPd, имеющая много уязвимостей:

Vuln ID	Summary	CVSS Severity
CVE-2021-40524	In Pure-FTPd 1.0.49, an incorrect max_filesize quota mechanism in the server allows attackers to upload files of unbounded size, which may lead to denial of service or a server hang. This occurs because a certain greater-than-zero test does not anticipate an initial -1 value. **Published:** сентября 05, 2021; 3:15:15 PM -0400	*V3.1:* 7.5 HIGH *V2.0:* 5.0 MEDIUM
CVE-2020-35359	Pure-FTPd 1.0.48 allows remote attackers to prevent legitimate server use by making enough connections to exceed the connection limit. **Published:** декабря 26, 2020; 12:15:11 AM -0500	*V3.1:* 7.5 HIGH *V2.0:* 5.0 MEDIUM
CVE-2020-9274	An issue was discovered in Pure-FTPd 1.0.49. An uninitialized pointer vulnerability has been detected in the diraliases linked list. When the *lookup_alias(const char alias) or print_aliases(void) function is called, they fail to correctly detect the end of the linked list and try to access a non-existent list member. This is related to init_aliases in diraliases.c. **Published:** февраля 26, 2020; 11:15:19 AM -0500	*V3.1:* 7.5 HIGH *V2.0:* 5.0 MEDIUM
CVE-2020-9365	An issue was discovered in Pure-FTPd 1.0.49. An out-of-bounds (OOB) read has been detected in the pure_strcmp function in utils.c. **Published:** февраля 24, 2020; 11:15:13 AM -0500	*V3.1:* 7.5 HIGH *V2.0:* 5.0 MEDIUM
CVE-2019-20176	In Pure-FTPd 1.0.49, a stack exhaustion issue was discovered in the listdir function in ls.c. **Published:** декабря 31, 2019; 10:15:11 AM -0500	*V3.1:* 7.5 HIGH *V2.0:* 5.0 MEDIUM
CVE-2017-12170	Downstream version 1.0.46-1 of pure-ftpd as shipped in Fedora was vulnerable to packaging error due to which the original configuration was ignored after update and service started running with default configuration. This has security implications because of overriding security-related configuration. This issue doesn't affect upstream version of pure-ftpd. **Published:** сентября 21, 2017; 5:29:00 PM -0400	*V3.0:* 9.8 CRITICAL *V2.0:* 7.5 HIGH

Видим ОС, на которых работает сайт и их примерные версии:

```
Running (JUST GUESSING): Grandstream embedded (89%), Linux 3.X|2.4.X|2.6.X (89%)
```

Видим таблицу Traceroute:

```
TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   1.00 ms  192.168.100.1
2   3.00 ms  sktv-bras7.sz.ip.rostelecom.ru (212.48.195.200)
3   5.00 ms  212.48.195.152
4   24.00 ms 185.140.148.31
5   ... 10
11  34.00 ms dev.ucoz.net (193.109.247.248)
```