

Black Virus

A dark, atmospheric image of a laptop. On the keyboard, there is a glowing, multi-colored virus-like object with many thin, radiating lines. The virus has a central core with blue and green spots. The laptop screen is dark, and the overall lighting is low, with a blue and green glow emanating from the virus and the screen.

IT infrastruktur

Creating a Secure Virtual Network using Zerotier and Debian



Virtuella maskiner (VM:ar) –Debian 13

Zerotier VPN-nätverk

NGINX

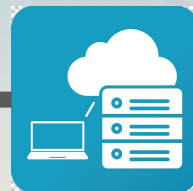
Brandvägg

WordPress-server

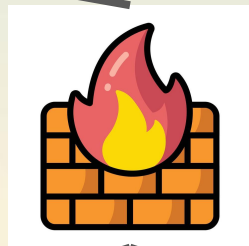
Databasserver (MySQL/MariaDB)

Klientanslutningar

**Wordpres
s server**

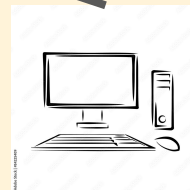
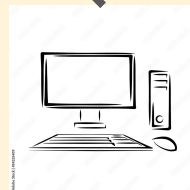


**Backup
server**



UFW

Debian 13



Varför Debian 13

- Stabilt
- Säkert
- Öppet operativsystem, ger full kontroll över servermiljön, lätt att konfigurera och kräver lite resurser.

Zerotier

- Virtuellt privat nätverk



Zerotier VPN

Varför inte Tailscale, eller Azure cloud?

- `curl -s https://install.zerotier.com | sudo bash`
`zerotier-cli join 68BEA79ACF8CB3B0`
- Open ssh server med port 22, `useradd`, `usermod -aG sudo`

Zerotier VPN

←

↺

🔒 https://my.zerotier.com/network/68bea79acf8cb3b0

🔌 ZEROTIER

Download

← Networks

blackvirus network

📄

Network ID:
68bea79acf8cb3b0

🔌

Included Devices: **6 / 10**
Upgrade to Essential for more devices and unlimited networks/admins/ssos

Upgrade to Essential

▼ Members

Search all columns...

6 total members
6 filtered members

AUTHORIZATION

All ☒

Authorized ☐ (6)

Not authorized ☐ (0)

ACTIVITY

All ☒

Inactive ☐ (6)

Active ☐ (0)

Reset Filters

Refresh

<input type="checkbox"/>	Edit	Auth	Address	Name/Desc	Managed IPs	Last Seen	Version	Physical IP	OS	Architecture
<input type="checkbox"/>	🔗	✅	33BF0834BD b2:80:33:c7:ae:1a	maya	10.144.113.220	21 hours	1.16.0	94.234.77.171		
<input type="checkbox"/>	🔗	✅	8591CEF680 b2:36:1d:01:6c:27	pat	10.144.171.241	22 hours	1.16.0	94.254.74.234		
<input type="checkbox"/>	🔗	✅	8832CAD024 b2:3b:be:05:4a:83	omid	10.144.104.134	22 hours	1.16.0	94.254.74.234		
<input type="checkbox"/>	🔗	✅	A4AF53CB5 b2:17:23:2a:a6:12	pat clon	10.144.76.107	22 hours	1.16.0	94.254.74.234		
<input type="checkbox"/>	🔗	✅	BF60D5983D b2:0c:ec:1a:02:9a	ar	10.144.186.192	22 hours	1.16.0	94.254.74.234		
<input type="checkbox"/>	🔗	✅	CC7BA1CA20 b2:7f:f7:6e:50:87	moon	10.144.61.10	2 hours	1.16.0	94.254.74.234		

E-Mail Join Instructions

alice@example.com

Manually Add Member

#####

NGINX(reverse proxy,rate limit)

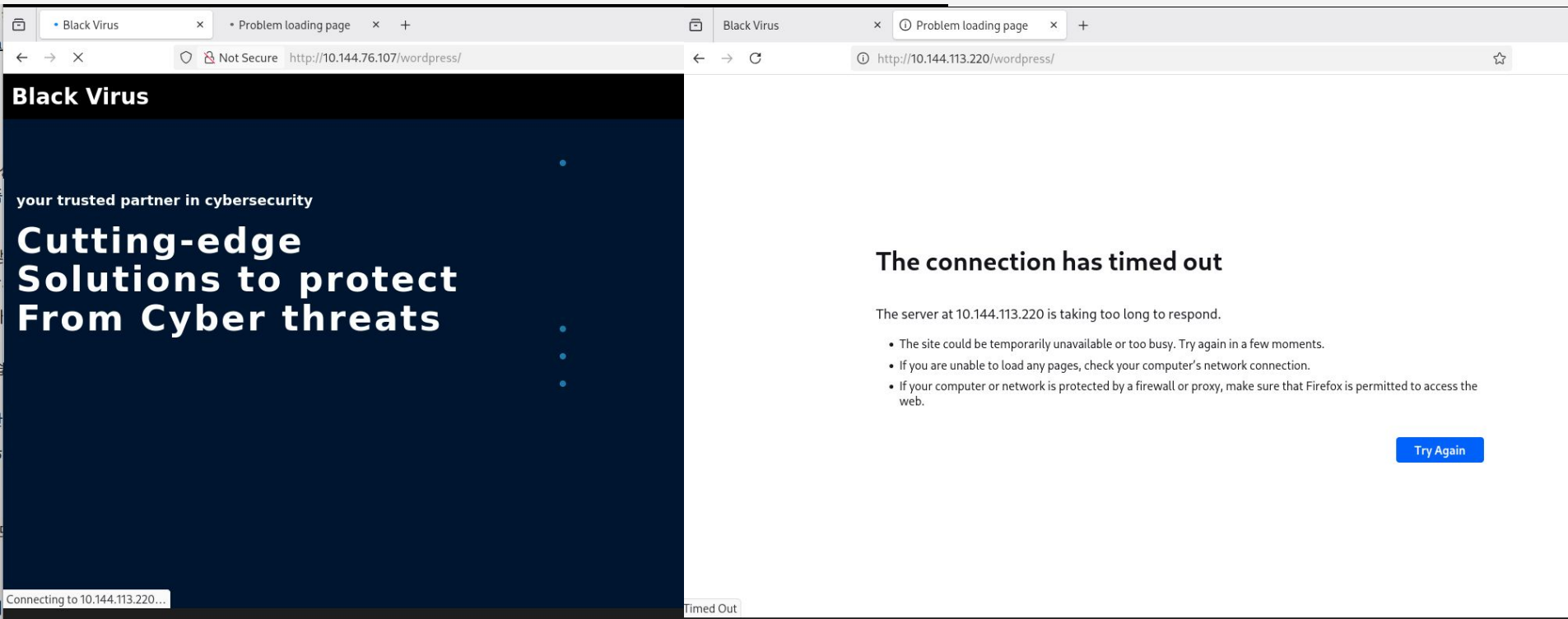
Vad är NGINX?

Proxy kommando

```
/etc/nginx/sites-available/default  
server{ server_name e.g.proxyurl;  
  location / { proxy_pass e.g.riktigurl/;  
    flera proxy_set_header konfig  
  }  
}
```



NGINX(reverse proxy,rate limit)



NGINX(reverse proxy,rate limit)

Rate limit kommando

limit_req_zone \$binary_remote_addr zone=e.g.name:Xm rate=Yr/s;

server{ limit_req zone=e.g.name burst=Z;

limit_req_status 429;

Testat med siege ->

Kända http error codes

404 Not Found

502 Bad Gateway

429 Too Many Requests

503 Service Unavailable

ubu@deb: ~									
HTTP/1.1	200	0.11	secs:	3044	bytes ==>	GET	/		
HTTP/1.1	200	0.04	secs:	3044	bytes ==>	GET	/		
HTTP/1.1	200	0.12	secs:	3044	bytes ==>	GET	/		
HTTP/1.1	200	0.05	secs:	3044	bytes ==>	GET	/		
HTTP/1.1	429	0.04	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.00	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.08	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.03	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.00	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.02	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.09	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.06	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.00	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.02	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.00	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.01	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.04	secs:	162	bytes ==>	GET	/		
HTTP/1.1	429	0.00	secs:	162	bytes ==>	GET	/		

Firewall

(Patrik, Omid, Aryan)

1. Ladda ner och installera curl, ufw, procps
2. IP Forwarding
3. Konfigurera UFW
4. Konfigurera /etc/ufw/before.rules:
 - a. PREROUTING
 - b. POSTROUTING
5. Verifiering

```
12:6:53.673290 IP 10.144.104.134.39830 > 10.144.76.107.http: Flags [..], ack 1, win 496, options [nop,nop,TS val 3372275518 ecr 4022205315], length 0
12:6:53.673351 IP 10.144.76.107.39830 > 10.144.113.220.http: Flags [..], ack 1, win 496, options [nop,nop,TS val 3372275518 ecr 4022205315], length 0
12:6:53.673372 IP 10.144.104.134.39818 > 10.144.76.107.http: Flags [..], ack 2749, win 539, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673370 IP 10.144.76.107.39818 > 10.144.113.220.http: Flags [..], ack 2749, win 539, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673381 IP 10.144.104.134.39818 > 10.144.76.107.http: Flags [..], ack 5497, win 582, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673385 IP 10.144.76.107.39818 > 10.144.113.220.http: Flags [..], ack 5497, win 582, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673388 IP 10.144.104.134.39818 > 10.144.76.107.http: Flags [..], ack 8245, win 625, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673391 IP 10.144.76.107.39818 > 10.144.113.220.http: Flags [..], ack 8245, win 625, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673395 IP 10.144.104.134.39818 > 10.144.76.107.http: Flags [..], ack 10938, win 668, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:53.673398 IP 10.144.76.107.39818 > 10.144.113.220.http: Flags [..], ack 10938, win 668, options [nop,nop,TS val 3372275518 ecr 4022206040], length 0
12:6:55.747410 IP 10.144.113.220.http > 10.144.76.107.39814: Flags [F..], seq 10938, ack 344, win 492, options [nop,nop,TS val 4022208269 ecr 3372270752], length 0
12:6:55.747452 IP 10.144.76.107.http > 10.144.104.134.39814: Flags [F..], seq 10938, ack 344, win 492, options [nop,nop,TS val 4022208269 ecr 3372270752], length 0
12:6:55.831771 IP 10.144.104.134.39814 > 10.144.76.107.http: Flags [F..], seq 344, ack 10939, win 668, options [nop,nop,TS val 3372275679 ecr 4022208269], length 0
12:6:55.831799 IP 10.144.76.107.39814 > 10.144.113.220.http: Flags [F..], seq 344, ack 10939, win 668, options [nop,nop,TS val 3372275679 ecr 4022208269], length 0
12:6:55.849293 IP 10.144.113.220.http > 10.144.76.107.39814: Flags [..], ack 345, win 492, options [nop,nop,TS val 4022208371 ecr 3372275679], length 0
12:6:55.849310 IP 10.144.76.107.http > 10.144.104.134.39814: Flags [..], ack 345, win 492, options [nop,nop,TS val 4022208371 ecr 3372275679], length 0
12:6:58.536457 IP 10.144.113.220.http > 10.144.76.107.39818: Flags [F..], seq 10938, ack 395, win 491, options [nop,nop,TS val 4022211045 ecr 3372273518], length 0
12:6:58.536489 IP 10.144.76.107.http > 10.144.104.134.39818: Flags [F..], seq 10938, ack 395, win 491, options [nop,nop,TS val 4022211045 ecr 3372273518], length 0

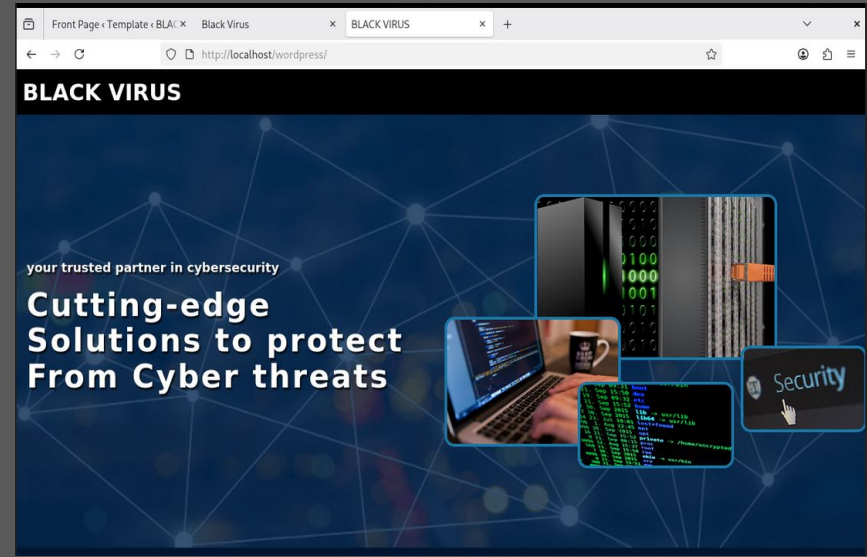
root@testproxy:/home/testproxy# sudo ufw status numbered
Status: active

    To Action From
    --
[ 1] 10.144.113.220 443/tcp on zt6jyswk17 ALLOW FWD Anywhere on zt6jyswk17
[ 2] 10.144.113.220 80/tcp on zt6jyswk17 ALLOW FWD Anywhere on zt6jyswk17
```

Wordpress & Databas

(Maya & Aryan)

- 1) Installerar nödvändiga program
(Apache2, MariaDB)
- 2) Konfigurera databas & wordpress
- 3) konfigurera lokal firewall och fail2ban
- 4) Designa hemsida



Säkerhet:

- Remove test user / database
- Deny all incoming ports But... (80/443)
- Fail2Ban

Backup server

(Maya & Patrik)

```
$ ls -l
total 12
drwxr-xr-x 2 backupuser backupuser 4096 Oct 27 13:45 wp-backup-20251027_134424
drwxr-xr-x 2 backupuser backupuser 4096 Oct 28 13:55 wp-backup-20251028_135436
drwxr-xr-x 2 backupuser backupuser 4096 Oct 28 14:08 wp-backup-20251028_140719
$
```

Script (.sh fil)

- 1) skapa directory med namn datum/tid,
- 2) fyll med mysqldumpad databas och wordpress filer,
- 3) säkerhets kopierar direktoryn till backup servern,
- 4) deletar den lokala direkt.

Execution

Fixar rättigheter (chmod),
Sätt upp en encryption key (ssh-keygen) och skicka den (ssh-copy-id)
Använd cron (crontab) så scriptet kör var 6-e timme.

Summa Kardemumma

Allt fungerar :D

Förbättringsområden:

- Arbetssätt (Agilt) - daglig planering
- Förbättringsområde i nätverket:
 - Moln Uppkoppling
 - Ytterligare WP/DB

Vad vi tar med oss:

Att samarbeta, söka lösningar, VERIFIERA åtgärder

Tack för oss!

