scenario

Legenda

Podejrzana maszyna → maszyna o adresie IP równym `172.16.0.2` w tunelu VPN

Sieć serwera → sieć, w której znajduje się serwer (sieć `192.168.1.0/24`)

Scenariusz

Dzień ataku: 8 Grudnia 2021

Od godziny 15:15:18 do godziny 15:20:16 trwało skanowanie sieci przez podejrzaną maszynę. Było to skanowanie poprzez wysyłanie komunikatów protokołu ICMP oraz TCP do maszyn o adresach 192.168.0.0-192.168.1.255. Przedstawia to komenda na ruchu na łączu zewnętrznym (pokazany jest tylko wycinek outputu komendy, całość jest zbyt długa):

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:15:18" && frame.time <= "Dec 8, 2021 15:20:16") && ip.src==172.1
...
20744 329.074207   172.16.0.2 → 192.168.0.10 ICMP 48 Echo (ping) request  id=0x88da, seq=0/0, ttl=54
20807 330.075387   172.16.0.2 → 192.168.0.13 ICMP 66 Echo (ping) request  id=0xfc69, seq=0/0, ttl=49
20808 330.075389   172.16.0.2 → 192.168.0.14 ICMP 66 Echo (ping) request  id=0x8227, seq=0/0, ttl=48
20809 330.075389   172.16.0.2 → 192.168.0.15 ICMP 66 Echo (ping) request  id=0xefd8, seq=0/0, ttl=53
20810 330.075402   172.16.0.2 → 192.168.0.13 ICMP 48 Echo (ping) request  id=0xfc69, seq=0/0, ttl=48
20811 330.075421   172.16.0.2 → 192.168.0.14 ICMP 48 Echo (ping) request  id=0x8227, seq=0/0, ttl=47
20812 330.075424   172.16.0.2 → 192.168.0.15 ICMP 48 Echo (ping) request  id=0xefd8, seq=0/0, ttl=52
20813 330.075501   172.16.0.2 → 192.168.0.16 ICMP 66 Echo (ping) request  id=0x6869, seq=0/0, ttl=48
20814 330.075501   172.16.0.2 → 192.168.0.17 ICMP 66 Echo (ping) request  id=0x10ee, seq=0/0, ttl=46
20815 330.075502   172.16.0.2 → 192.168.0.18 ICMP 66 Echo (ping) request  id=0x73e9, seq=0/0, ttl=37
20816 330.075504   172.16.0.2 → 192.168.0.16 ICMP 48 Echo (ping) request  id=0x6869, seq=0/0, ttl=47
20817 330.075517   172.16.0.2 → 192.168.0.17 ICMP 48 Echo (ping) request  id=0x10ee, seq=0/0, ttl=45
20818 330.075524   172.16.0.2 → 192.168.0.18 ICMP 48 Echo (ping) request  id=0x73e9, seq=0/0, ttl=36
20819 330.075607   172.16.0.2 → 192.168.0.19 ICMP 66 Echo (ping) request  id=0xa237, seq=0/0, ttl=44
...
25327 384.135928   172.16.0.2 → 192.168.0.206 TCP 60 [TCP Dup ACK 25323#1] 46032 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
25328 384.135941   172.16.0.2 → 192.168.0.209 TCP 60 [TCP Dup ACK 25324#1] 46032 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
25329 384.135946   172.16.0.2 → 192.168.0.214 TCP 64 [TCP Out-Of-Order] 46032 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25330 384.135950   172.16.0.2 → 192.168.0.217 TCP 64 [TCP Out-Of-Order] 46032 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25331 384.138062   172.16.0.2 → 192.168.0.218 TCP 66 46032 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25332 384.138070   172.16.0.2 → 192.168.0.218 TCP 64 [TCP Out-Of-Order] 46032 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25395 385.129014   172.16.0.2 → 192.168.0.235 TCP 66 46031 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25396 385.129036   172.16.0.2 → 192.168.0.235 TCP 64 [TCP Out-Of-Order] 46031 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25397 385.131195   172.16.0.2 → 192.168.0.238 TCP 66 46031 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
25398 385.131197   172.16.0.2 → 192.168.0.239 TCP 66 46031 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25399 385.131208   172.16.0.2 → 192.168.0.238 TCP 60 [TCP Dup ACK 25397#1] 46031 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
25400 385.131231   172.16.0.2 → 192.168.0.239 TCP 64 [TCP Out-Of-Order] 46031 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25401 385.133485   172.16.0.2 → 192.168.0.242 TCP 66 46031 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
...
```

Na skanowanie sieci odpowiedziały maszyny o adresach `192.168.1.1` oraz `192.168.1.2` , można to sprawdzić po odpowiedziach na ping w ruchu na łączu zewnętrznym:

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:15:18" && frame.time <= "Dec 8, 2021 15:20:16") && icmp && icmp.
41532 594.675071  192.168.1.1 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0xa58c, seq=0/0, ttl=64 (request in 41524)
41544 594.675549  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x247b, seq=0/0, ttl=64 (request in 41533)
41545 594.675555  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x247b, seq=0/0, ttl=63
41944 595.980866  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x52e2, seq=0/0, ttl=64 (request in 41943)
41945 595.980883  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x52e2, seq=0/0, ttl=63
43400 597.285871  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x5b2b, seq=0/0, ttl=64 (request in 43399)
43401 597.285912  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x5b2b, seq=0/0, ttl=63
44118 599.331656  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x3bc5, seq=0/0, ttl=64 (request in 44116)
44119 599.331675  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x3bc5, seq=0/0, ttl=63
44449 600.766226  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x281a, seq=0/0, ttl=64 (request in 44448)
44450 600.766238  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x281a, seq=0/0, ttl=63
44758 602.024365  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x8452, seq=0/0, ttl=64 (request in 44736)
44759 602.024370  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x8452, seq=0/0, ttl=63
45126 604.557828  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0xbc24, seq=0/0, ttl=64 (request in 45124)
45127 604.557837  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0xbc24, seq=0/0, ttl=63
45488 606.805329  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0x05cf, seq=0/0, ttl=64 (request in 45481)
45489 606.805336  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0x05cf, seq=0/0, ttl=63
45909 609.016990  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0xc3de, seq=0/0, ttl=64 (request in 45907)
45910 609.016998  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0xc3de, seq=0/0, ttl=63
```

```
46087 610.268364  192.168.1.2 → 172.16.0.2   ICMP 66 Echo (ping) reply    id=0xc595, seq=0/0, ttl=64 (request in 46086)
46088 610.268382  192.168.1.2 → 172.16.0.2   ICMP 48 Echo (ping) reply    id=0xc595, seq=0/0, ttl=63
```

Następnie, o godzinie 15:24:16 rozpoczyna się próba komunikacji HTTP podejrzanej maszyny z serwerem na adresie IP `192.168.1.2` . Podejrzana maszyna wysyła żądania pod popularne adresy: `/webadmin`, `/admin`, `/phpmyadmin/` i dostaje odpowiedź z kodem 200 od tego ostatniego:

```
> tshark -r greenforestbank-serwer.pcap -Y 'http' | head -n 8
  622   9.718209   172.16.0.2 → 192.168.1.2  HTTP 486 GET / HTTP/1.1
  624   9.720829  192.168.1.2 → 172.16.0.2   HTTP 3452 HTTP/1.1 200 OK  (text/html)
 1476  22.882611   172.16.0.2 → 192.168.1.2  HTTP 402 GET /webadmin HTTP/1.1
 1478  22.883531  192.168.1.2 → 172.16.0.2   HTTP 562 HTTP/1.1 404 Not Found  (text/html)
 1800  27.961412   172.16.0.2 → 192.168.1.2  HTTP 399 GET /admin HTTP/1.1
 1802  27.962297  192.168.1.2 → 172.16.0.2   HTTP 562 HTTP/1.1 404 Not Found  (text/html)
 2297  35.540887   172.16.0.2 → 192.168.1.2  HTTP 647 GET /phpMyAdmin/ HTTP/1.1
 2300  35.569265  192.168.1.2 → 172.16.0.2   HTTP 6109 HTTP/1.1 200 OK  (text/html)
```

O 15:24:50 podejrzanej maszynie udaje się zalogować do serwera z loginem=root i hasłem=root, jednak o 15:24:56 następuje wylogowanie, bez podejrzanych aktywności:

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:24:50" && frame.time <= "Dec 8, 2021 15:24:57") && http'
70559 901.027084   172.16.0.2 → 192.168.1.2  HTTP 881 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
70566 901.044853  192.168.1.2 → 172.16.0.2   HTTP 1244 HTTP/1.1 302 Found
70570 901.053435   172.16.0.2 → 192.168.1.2  HTTP 868 GET /phpMyAdmin/index.php?route=/&route=%2F HTTP/1.1
70589 901.153772  192.168.1.2 → 172.16.0.2   HTTP 3226 HTTP/1.1 200 OK  (text/html)
70599 901.287347   172.16.0.2 → 192.168.1.2  HTTP 830 GET /phpMyAdmin/themes/pmahomme/css/theme.css?v=5.1.1&nocache=2092910502ltr&server=1
70614 901.306067  192.168.1.2 → 172.16.0.2   HTTP 1610 HTTP/1.1 200 OK  (text/css)
70651 901.889113   172.16.0.2 → 192.168.1.2  HTTP 1079 POST /phpMyAdmin/index.php?route=/config/get HTTP/1.1  (application/x-www-form-urlen
70655 901.897236  192.168.1.2 → 172.16.0.2   HTTP/JSON 2770 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70663 901.903197   172.16.0.2 → 192.168.1.2  HTTP 1035 POST /phpMyAdmin/index.php?route=/navigation&ajax_request=1 HTTP/1.1  (application/x
70668 901.923183  192.168.1.2 → 172.16.0.2   HTTP/JSON 3456 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70675 901.971764   172.16.0.2 → 192.168.1.2  HTTP 1060 POST /phpMyAdmin/index.php?route=/config/get HTTP/1.1  (application/x-www-form-urlen
70678 901.980190  192.168.1.2 → 172.16.0.2   HTTP/JSON 2852 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70689 902.031583   172.16.0.2 → 192.168.1.2  HTTP 1032 POST /phpMyAdmin/index.php?route=/version-check HTTP/1.1  (application/x-www-form-ur
70703 902.086531   172.16.0.2 → 192.168.1.2  HTTP 1088 POST /phpMyAdmin/index.php?route=/config/set HTTP/1.1  (application/x-www-form-urlen
70712 902.154942  192.168.1.2 → 172.16.0.2   HTTP/JSON 1282 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70716 902.162255  192.168.1.2 → 172.16.0.2   HTTP/JSON 2760 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70890 904.960233   172.16.0.2 → 192.168.1.2  HTTP 842 GET /phpMyAdmin/ HTTP/1.1
70904 904.997184  192.168.1.2 → 172.16.0.2   HTTP 3234 HTTP/1.1 200 OK  (text/html)
70917 905.126263   172.16.0.2 → 192.168.1.2  HTTP 838 GET /phpMyAdmin/themes/pmahomme/css/theme.css?v=5.1.1&nocache=3786450640ltr&server=1
70929 905.134713  192.168.1.2 → 172.16.0.2   HTTP 8850 HTTP/1.1 200 OK  (text/css)
70970 905.608292   172.16.0.2 → 192.168.1.2  HTTP 1086 POST /phpMyAdmin/index.php?route=/config/get HTTP/1.1  (application/x-www-form-urlen
70974 905.609150   172.16.0.2 → 192.168.1.2  HTTP 1047 POST /phpMyAdmin/index.php?route=/navigation&ajax_request=1 HTTP/1.1  (application/x
70978 905.635858  192.168.1.2 → 172.16.0.2   HTTP/JSON 3465 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70980 905.643725  192.168.1.2 → 172.16.0.2   HTTP/JSON 2772 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
70990 905.696943   172.16.0.2 → 192.168.1.2  HTTP 1069 POST /phpMyAdmin/index.php?route=/config/get HTTP/1.1  (application/x-www-form-urlen
70993 905.712381  192.168.1.2 → 172.16.0.2   HTTP/JSON 2859 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
71002 905.792951   172.16.0.2 → 192.168.1.2  HTTP 1039 POST /phpMyAdmin/index.php?route=/version-check HTTP/1.1  (application/x-www-form-ur
71005 905.808585  192.168.1.2 → 172.16.0.2   HTTP/JSON 1280 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
71026 905.998719   172.16.0.2 → 192.168.1.2  HTTP 1105 POST /phpMyAdmin/index.php?route=/config/set HTTP/1.1  (application/x-www-form-urlen
71029 906.007796  192.168.1.2 → 172.16.0.2   HTTP/JSON 2760 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
71138 907.687662   172.16.0.2 → 192.168.1.2  HTTP 988 POST /phpMyAdmin/index.php?route=/logout HTTP/1.1  (application/x-www-form-urlencoded
71152 907.737367  192.168.1.2 → 172.16.0.2   HTTP 77 HTTP/1.1 302 Found  (text/html)
71161 907.758205   172.16.0.2 → 192.168.1.2  HTTP 674 GET /phpMyAdmin/index.php?route=/ HTTP/1.1
71165 907.768570  192.168.1.2 → 172.16.0.2   HTTP 6179 HTTP/1.1 200 OK  (text/html)
```

```
tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:24:50" && frame.time <= "Dec 8, 2021 15:24:51") && http && http.re
Host: 192.168.1.2\r\n,User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n,Accept: text/html,application/xh
```

Prawdopodobnie nie był to hacker, lecz inny pracownik, którego żądania były wysyłane z tego samego adresu IP, który był nieświadomy ataku hackerskiego.

Następnie, od godziny 15:25:04 do godziny 15:26:29 następuje próba zalogowania się podejrzanej maszyny na konto na serwerze:

```
tshark -r greenforestbank-serwer.pcap -Y '(frame.time > "Dec 8, 2021 15:25:03" && frame.time <= "Dec 8, 2021 15:26:30") && http'
 3817  56.973362   172.16.0.2 → 192.168.1.2  HTTP 893 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 3820  57.005565  192.168.1.2 → 172.16.0.2   HTTP 6319 HTTP/1.1 200 OK  (text/html)
 4867  73.801573   172.16.0.2 → 192.168.1.2  HTTP 893 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
```

```
 4870  73.817762  192.168.1.2 → 172.16.0.2   HTTP 6321 HTTP/1.1 200 OK  (text/html)
 5722  87.178200   172.16.0.2 → 192.168.1.2  HTTP 909 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 5725  87.193965  192.168.1.2 → 172.16.0.2   HTTP 6315 HTTP/1.1 200 OK  (text/html)
 5734  87.306331   172.16.0.2 → 192.168.1.2  HTTP 584 GET /phpMyAdmin/js/messages.php?l=en&v=5.1.1 HTTP/1.1
 5738  87.313525  192.168.1.2 → 172.16.0.2   HTTP 1065 HTTP/1.1 200 OK  (text/javascript)
 6173  94.040084   172.16.0.2 → 192.168.1.2  HTTP 887 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 6176  94.049160  192.168.1.2 → 172.16.0.2   HTTP 6246 HTTP/1.1 200 OK  (text/html)
 6903 105.621704   172.16.0.2 → 192.168.1.2  HTTP 897 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 6906 105.638227  192.168.1.2 → 172.16.0.2   HTTP 6310 HTTP/1.1 200 OK  (text/html)
 7441 114.001396   172.16.0.2 → 192.168.1.2  HTTP 897 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 7443 114.011839  192.168.1.2 → 172.16.0.2   HTTP 6308 HTTP/1.1 200 OK  (text/html)
 7750 118.681642   172.16.0.2 → 192.168.1.2  HTTP 891 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 7752 118.690497  192.168.1.2 → 172.16.0.2   HTTP 6307 HTTP/1.1 200 OK  (text/html)
 8082 123.649925   172.16.0.2 → 192.168.1.2  HTTP 895 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 8084 123.658228  192.168.1.2 → 172.16.0.2   HTTP 6309 HTTP/1.1 200 OK  (text/html)
 8523 130.744696   172.16.0.2 → 192.168.1.2  HTTP 898 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 8527 130.754523  192.168.1.2 → 172.16.0.2   HTTP 6307 HTTP/1.1 200 OK  (text/html)
 8757 134.234895   172.16.0.2 → 192.168.1.2  HTTP 891 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 8759 134.244055  192.168.1.2 → 172.16.0.2   HTTP 6306 HTTP/1.1 200 OK  (text/html)
 9225 142.895596   172.16.0.2 → 192.168.1.2  HTTP 891 POST /phpMyAdmin/index.php?route=/ HTTP/1.1  (application/x-www-form-urlencoded)
 9227 142.903250  192.168.1.2 → 172.16.0.2   HTTP 1250 HTTP/1.1 302 Found
```

```
# auth.log
Dec  8 15:25:04 serwer phpMyAdmin[3933]: user denied: admin (mysql-denied) from 172.16.0.2
Dec  8 15:25:20 serwer phpMyAdmin[3929]: user denied: guest (mysql-denied) from 172.16.0.2
Dec  8 15:25:34 serwer phpMyAdmin[3936]: user denied: administrator (mysql-denied) from 172.16.0.2
Dec  8 15:25:41 serwer phpMyAdmin[3931]: user denied: root (empty-denied) from 172.16.0.2
Dec  8 15:25:52 serwer phpMyAdmin[4137]: user denied: root (mysql-denied) from 172.16.0.2
Dec  8 15:26:01 serwer phpMyAdmin[3932]: user denied: root (mysql-denied) from 172.16.0.2
Dec  8 15:26:05 serwer phpMyAdmin[3932]: user denied: root (mysql-denied) from 172.16.0.2
Dec  8 15:26:10 serwer phpMyAdmin[3932]: user denied: root (mysql-denied) from 172.16.0.2
Dec  8 15:26:17 serwer phpMyAdmin[3930]: user denied: root (mysql-denied) from 172.16.0.2
Dec  8 15:26:21 serwer phpMyAdmin[3930]: user denied: root (mysql-denied) from 172.16.0.2
```

która ostatecznie kończy się sukcesem dla loginu=szef i hasła=szef. W ten sposób hacker uzyskał dostęp do konta w interfejsie PhpMyAdmin.

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:26:28" && frame.time < "Dec 8, 2021 15:26:31") && http && http.r
Host: 192.168.1.2\r\n,User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n,Accept: text/html,application/xh
```

Następnie o godzinie 15:26:47 następuje export bazy danych `GreenForestBank`

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:26:46" && frame.time < "Dec 8, 2021 15:26:48") && http' | head -
78355 1018.298412   172.16.0.2 → 192.168.1.2  HTTP 937 GET /phpMyAdmin/index.php?route=/database/export&db=GreenForestBank&ajax_request=tru
78383 1018.565760  192.168.1.2 → 172.16.0.2   HTTP/JSON 77 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
```

```
# access.log
172.16.0.2 - - [08/Dec/2021:15:26:47 +0100] "GET /phpMyAdmin/index.php?route=/database/export&db=GreenForestBank&ajax_request=true&ajax_pag
172.16.0.2 - - [08/Dec/2021:15:26:47 +0100] "GET /phpMyAdmin/js/dist/export.js?v=5.1.1 HTTP/1.1" 200 7049 "-" "Mozilla/5.0 (X11; Linux x86_
```

A w godzinach 15:27:49 do 15:28:03 trwa wpisywanie i wykonanie komendy przez hackera, która usuwa bazę danych:

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:27:48" && frame.time < "Dec 8, 2021 15:28:04") && http'
82438 1080.345214   172.16.0.2 → 192.168.1.2  HTTP 1079 POST /phpMyAdmin/index.php?route=/database/sql/autocomplete HTTP/1.1  (application/
82444 1080.374547  192.168.1.2 → 172.16.0.2   HTTP/JSON 3031 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
82700 1084.426505   172.16.0.2 → 192.168.1.2  HTTP 1071 POST /phpMyAdmin/index.php?route=/lint HTTP/1.1  (application/x-www-form-urlencoded
82708 1084.445513  192.168.1.2 → 172.16.0.2   HTTP/JSON 1236 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
82784 1085.669858   172.16.0.2 → 192.168.1.2  HTTP 1073 POST /phpMyAdmin/index.php?route=/lint HTTP/1.1  (application/x-www-form-urlencoded
82787 1085.685885  192.168.1.2 → 172.16.0.2   HTTP/JSON 1337 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
82904 1087.504568   172.16.0.2 → 192.168.1.2  HTTP 1072 POST /phpMyAdmin/index.php?route=/lint HTTP/1.1  (application/x-www-form-urlencoded
82906 1087.521140  192.168.1.2 → 172.16.0.2   HTTP/JSON 1356 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
83116 1090.568198   172.16.0.2 → 192.168.1.2  HTTP 1102 POST /phpMyAdmin/index.php?route=/lint HTTP/1.1  (application/x-www-form-urlencoded
83120 1090.584921  192.168.1.2 → 172.16.0.2   HTTP/JSON 1236 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
83194 1091.785227   172.16.0.2 → 192.168.1.2  HTTP 1089 POST /phpMyAdmin/index.php?route=/lint HTTP/1.1  (application/x-www-form-urlencoded
```

```
83197 1091.802767  192.168.1.2 → 172.16.0.2   HTTP/JSON 1239 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
83371 1094.460248   172.16.0.2 → 192.168.1.2  HTTP 1320 POST /phpMyAdmin/index.php?route=/import HTTP/1.1  (application/x-www-form-urlencod
```

```
172.16.0.2 - - [08/Dec/2021:15:27:49 +0100] "POST /phpMyAdmin/index.php?route=/database/sql/autocomplete HTTP/1.1" 200 2959 "-" "Mozilla/5.
172.16.0.2 - - [08/Dec/2021:15:27:53 +0100] "POST /phpMyAdmin/index.php?route=/lint HTTP/1.1" 200 1164 "-" "Mozilla/5.0 (X11; Linux x86_64;
172.16.0.2 - - [08/Dec/2021:15:27:54 +0100] "POST /phpMyAdmin/index.php?route=/lint HTTP/1.1" 200 1265 "-" "Mozilla/5.0 (X11; Linux x86_64;
172.16.0.2 - - [08/Dec/2021:15:27:56 +0100] "POST /phpMyAdmin/index.php?route=/lint HTTP/1.1" 200 1284 "-" "Mozilla/5.0 (X11; Linux x86_64;
172.16.0.2 - - [08/Dec/2021:15:27:59 +0100] "POST /phpMyAdmin/index.php?route=/lint HTTP/1.1" 200 1164 "-" "Mozilla/5.0 (X11; Linux x86_64;
172.16.0.2 - - [08/Dec/2021:15:28:00 +0100] "POST /phpMyAdmin/index.php?route=/lint HTTP/1.1" 200 1167 "-" "Mozilla/5.0 (X11; Linux x86_64;
172.16.0.2 - - [08/Dec/2021:15:28:03 +0100] "POST /phpMyAdmin/index.php?route=/import HTTP/1.1" 200 3197 "-" "Mozilla/5.0 (X11; Linux x86_6
```

(Gdzie endpoint `/lint` obsługuje podpowiadanie komendy, a `/import` wgrywa komendę)

```
# żądanie usuwające bazę danych, komenda jest w polu "sql_query"
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:28:03" && frame.time < "Dec 8, 2021 15:28:04") && http' -T field
Host: 192.168.1.2\r\n,User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n,Accept: */*\r\n,Accept-Language:
```

O 15:28:08 następuje wylogowanie z phpMyAdmin.

```
> tshark -r greenforestbank-router.pcap -Y '(frame.time >= "Dec 8, 2021 15:28:05" && frame.time < "Dec 8, 2021 15:28:09") && http'
83677 1098.889887   172.16.0.2 → 192.168.1.2  HTTP 991 POST /phpMyAdmin/index.php?route=/logout HTTP/1.1  (application/x-www-form-urlencode
83697 1098.944919  192.168.1.2 → 172.16.0.2   HTTP 77 HTTP/1.1 302 Found  (text/html)
83732 1099.077753   172.16.0.2 → 192.168.1.2  HTTP 991 POST /phpMyAdmin/index.php?route=/logout HTTP/1.1  (application/x-www-form-urlencode
83737 1099.084890  192.168.1.2 → 172.16.0.2   HTTP 6187 HTTP/1.1 200 OK  (text/html)
```

```
# access.log
172.16.0.2 - - [08/Dec/2021:15:28:08 +0100] "POST /phpMyAdmin/index.php?route=/logout HTTP/1.1" 302 11696 "-" "Mozilla/5.0 (X11; Linux x86_
172.16.0.2 - - [08/Dec/2021:15:28:08 +0100] "POST /phpMyAdmin/index.php?route=/logout HTTP/1.1" 200 6115 "-" "Mozilla/5.0 (X11; Linux x86_6
```

Atakujący najprawdopodobniej korzystał z interfejsu graficznego PhpMyAdmin, najprawdopodobniej w przeglądarce, wskazują na to:

1. User Agent maszyny o wartości `"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"`, jednak ta wartość może zostać wpisana ręcznie przez atakującego, nie musi to oznaczać, że żądania zostały wysłane z przeglądarki firefox.

   ```
   # access.log
   # ...
   172.16.0.2 - - [08/Dec/2021:15:25:41 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6174 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:25:52 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6238 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:01 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6236 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:05 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6235 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:10 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6237 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:17 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6235 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:21 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6234 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:29 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 302 1178 "-" "Mozilla/5.0 (X11; Linux x86_64;
   # ...
   ```

2. Logi z żądaniami wysłanymi przez atakującego pokazują, że w krótkim czasie były wysłane requesty do serwera (w tym takie pobierające pliki `.css`) co świadczy o tym, że nie zostały one wysłany np. z consoli, a wysłane automatycznie przez narzędzie renderujące stronę (np. przeglądarka).

   ```
   # access.log
   # ...
   172.16.0.2 - - [08/Dec/2021:15:26:21 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 200 6234 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:29 +0100] "POST /phpMyAdmin/index.php?route=/ HTTP/1.1" 302 1178 "-" "Mozilla/5.0 (X11; Linux x86_64;
   172.16.0.2 - - [08/Dec/2021:15:26:30 +0100] "GET /phpMyAdmin/index.php?route=/&route=%2F HTTP/1.1" 200 17638 "-" "Mozilla/5.0 (X11; Lin
   172.16.0.2 - - [08/Dec/2021:15:26:30 +0100] "GET /phpMyAdmin/themes/pmahomme/css/theme.css?v=5.1.1&nocache=3537360439ltr&server=1 HTTP/
   172.16.0.2 - - [08/Dec/2021:15:26:30 +0100] "POST /phpMyAdmin/index.php?route=/config/get HTTP/1.1" 200 2702 "-" "Mozilla/5.0 (X11; Lin
   172.16.0.2 - - [08/Dec/2021:15:26:30 +0100] "POST /phpMyAdmin/index.php?route=/navigation&ajax_request=1 HTTP/1.1" 200 3407 "-" "Mozill
   172.16.0.2 - - [08/Dec/2021:15:26:31 +0100] "POST /phpMyAdmin/index.php?route=/config/get HTTP/1.1" 200 2793 "-" "Mozilla/5.0 (X11; Lin
   172.16.0.2 - - [08/Dec/2021:15:26:31 +0100] "POST /phpMyAdmin/index.php?route=/version-check HTTP/1.1" 200 1193 "-" "Mozilla/5.0 (X11;
   ```

```
172.16.0.2 - - [08/Dec/2021:15:26:31 +0100] "POST /phpMyAdmin/index.php?route=/config/set HTTP/1.1" 200 2696 "-" "Mozilla/5.0 (X11; Lin
# ...
```

Strefa czasowa serwera to European Central Time (ETC+1) - wskazują na to logi z serwera

```
172.16.0.2 - - [08/Dec/2021:15:07:57 +0100] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/
```

gdzie przy dacie mamy `+0100` co oznacza strefę czasową.