

Aplicação de Segurança Informática



Beja, Março de 2014

Pedro Moreira e João Mendes

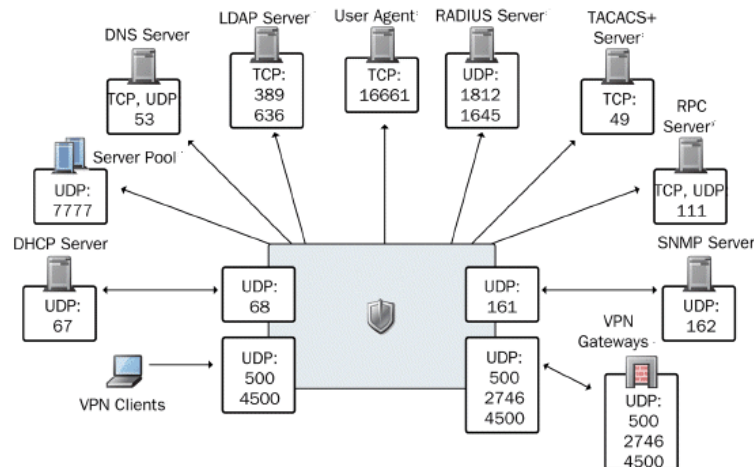
Aplicação de Segurança Informática

Ferramentas de segurança em rede

- Identificação de vulnerabilidades na rede informática;
- Identificação de portos abertos (serviços);
- Análise de logs da firewall ufw;
- Visualização da localização geográfica dos acessos externos.

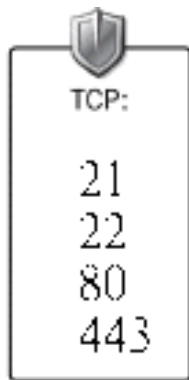
PORTSCAN

- Identificação dispositivos presentes na rede e que serviços estão activos pela pesquisa dos portos abertos;
- `./scanner.py -u <user> -portscan <ip> <ports>`



CONSCAN

- Identificação das ligações INET activas;
- `./scanner.py -u <user> -conscan`



Aplicação de Segurança Informática

LOGSCAN

- Identificação ligações externas através da leitura do ficheiro de log da firewall ufw;
- `./scanner.py -u <user> -logscan <ufw log file>`

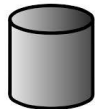
```

Jun 17 11:17:44 nuc kernel: [ 68.223091] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.23.132 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=127 ID=19192 PROTO=UDP SPT=45160 DPT=46080 LEN=127
Jun 17 11:18:18 nuc kernel: [ 102.631288] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.28.58 DST=10.0.28.67 LEN=145 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1033 DPT=46080 LEN=125
Jun 17 11:18:25 nuc kernel: [ 108.696981] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.28.58 DST=10.0.28.67 LEN=145 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1033 DPT=46080 LEN=125
Jun 17 11:18:47 nuc kernel: [ 130.848094] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.31 DST=10.0.28.67 LEN=135 TOS=0x00 PREC=0x00 TTL=63 ID=23932 PROTO=UDP SPT=14327 DPT=46080 LEN=115
Jun 17 11:28:04 nuc kernel: [ 110.619601] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.76 DST=10.0.28.67 LEN=137 TOS=0x00 PREC=0x00 TTL=127 ID=21284 PROTO=UDP SPT=17177 DPT=46080 LEN=117
Jun 17 11:28:06 nuc kernel: [ 112.607272] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.76 DST=10.0.28.67 LEN=137 TOS=0x00 PREC=0x00 TTL=127 ID=21303 PROTO=UDP SPT=17177 DPT=46080 LEN=117
Jun 17 11:28:10 nuc kernel: [ 116.603642] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.76 DST=10.0.28.67 LEN=137 TOS=0x00 PREC=0x00 TTL=127 ID=21368 PROTO=UDP SPT=17177 DPT=46080 LEN=117
Jun 17 11:29:05 nuc kernel: [ 171.791496] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.50.3 DST=10.0.28.67 LEN=153 TOS=0x00 PREC=0x00 TTL=126 ID=29252 PROTO=UDP SPT=55385 DPT=46080 LEN=133
Jun 17 11:29:07 nuc kernel: [ 173.795586] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.50.3 DST=10.0.28.67 LEN=153 TOS=0x00 PREC=0x00 TTL=126 ID=29380 PROTO=UDP SPT=55385 DPT=46080 LEN=133
Jun 17 11:29:11 nuc kernel: [ 177.799255] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.50.3 DST=10.0.28.67 LEN=153 TOS=0x00 PREC=0x00 TTL=126 ID=29393 PROTO=UDP SPT=55385 DPT=46080 LEN=133
Jun 17 11:29:28 nuc kernel: [ 194.901473] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.28.58 DST=10.0.28.67 LEN=140 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1033 DPT=46080 LEN=120
Jun 17 11:29:30 nuc kernel: [ 196.868026] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.25.5 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=127 ID=14833 PROTO=UDP SPT=12085 DPT=46080 LEN=127
Jun 17 11:29:30 nuc kernel: [ 196.902013] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.28.58 DST=10.0.28.67 LEN=140 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1033 DPT=46080 LEN=120
Jun 17 11:29:32 nuc kernel: [ 198.886418] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.25.5 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=127 ID=14835 DF PROTO=UDP SPT=12085 DPT=46080 LEN=127
Jun 17 11:29:34 nuc kernel: [ 200.912924] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.28.58 DST=10.0.28.67 LEN=140 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP SPT=1033 DPT=46080 LEN=120
Jun 17 11:29:36 nuc kernel: [ 202.884876] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.25.5 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=127 ID=14842 PROTO=UDP SPT=12085 DPT=46080 LEN=127
Jun 17 11:30:05 nuc kernel: [ 231.525685] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.31 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=63 ID=58238 PROTO=UDP SPT=14327 DPT=46080 LEN=127
Jun 17 11:30:07 nuc kernel: [ 233.545287] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.31 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=63 ID=5241 PROTO=UDP SPT=14327 DPT=46080 LEN=127
Jun 17 11:30:11 nuc kernel: [ 237.555731] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.11.31 DST=10.0.28.67 LEN=147 TOS=0x00 PREC=0x00 TTL=63 ID=17015 PROTO=UDP SPT=14327 DPT=46080 LEN=127
Jun 17 11:31:20 nuc kernel: [ 306.861035] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.29.5 DST=10.0.28.67 LEN=143 TOS=0x00 PREC=0x00 TTL=127 ID=24622 PROTO=UDP SPT=41662 DPT=46080 LEN=123
Jun 17 11:31:22 nuc kernel: [ 308.889085] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.29.5 DST=10.0.28.67 LEN=143 TOS=0x00 PREC=0x00 TTL=127 ID=24636 PROTO=UDP SPT=41662 DPT=46080 LEN=123
Jun 17 11:31:26 nuc kernel: [ 312.885946] [ufw BLOCK] IN=eth0 OUT= MAC= SRC=10.0.29.5 DST=10.0.28.67 LEN=143 TOS=0x00 PREC=0x00 TTL=127 ID=24647 PROTO=UDP SPT=41662 DPT=46080 LEN=123

```

EXPORTAÇÃO DE DADOS

- Exportação para db (SQLite), PDF e CSV;
- `./scanner.py -u <user> -export <filename> <filetype [db, csv, pdf]>`



Database



The screenshot displays a web browser window with a Google Maps interface. A red arrow points from the 'PORT SCANS' table in the scanner output to the map. The scanner output shows a list of port scans and log scans.

Time	Local Port	Remote IP	Remote Port				
PORT SCANS							
Time	IP	Protocol	Port				
2014-03-23 16:30:59.117492	192.168.1.254	tcp	21				
2014-03-23 16:30:59.117492	192.168.1.254	tcp	23				
2014-03-23 16:30:59.117492	192.168.1.254	tcp	53				
2014-03-23 16:30:59.117492	192.168.1.254	tcp	80				
2014-03-23 16:30:59.117492	192.168.1.254	tcp	443				
2014-03-25 21:59:07.896177	192.168.1.254	tcp	21				
2014-03-25 21:59:07.896177	192.168.1.254	tcp	23				
2014-03-25 21:59:07.896177	192.168.1.254	tcp	53				
2014-03-25 21:59:07.896177	192.168.1.254	tcp	80				
LOG SCANS							
Time	IP	Dev	Proto	TTL	SrcPrt	DstPrt	Country
1900-02-17 12:08:44	108.160.160.164	wlan0	TCP	52	80	53608	United States

Aplicação de Segurança Informática

ELIMINAR BASE DE DADOS

- Eliminar base de dados db (Sqlite)
- `./scanner.py -u <user> -delete`

