

Rapport IDS/IPS - TP1

I. Résumé de l'analyse

Nombre total de paquets : 330

Protocoles détectés :

- UDP : 4276 paquets
- TCP : 330 paquets
- HTTPS : 113 paquets
- DNS : 21 paquets
- HTTP : 23 paquets
- IP(1) : 7 paquets
- ARP : 15 paquets
- FTP : 5 paquets

Top ports utilisés :

- Port 5353 : 6193 fois
- Port 137 : 1093 fois
- Port 443 : 257 fois
- Port 1900 : 208 fois
- Port 7680 : 190 fois

Top IPs émettrices :

- 10.33.0.125 : 729 paquets
- 10.33.3.117 : 420 paquets
- 10.33.3.13 : 271 paquets
- 10.33.4.33 : 224 paquets
- 10.33.2.71 : 127 paquets

Attaques détectées :

- [SQL Injection] Payload suspect détecté : ██████████y7ai2<)#4y████ohny████b "<he q█1████ox'████(█
 - [SQL Injection] Payload suspect détecté : ██████r████n█████|*gw7 hpf+ di%x pcd%████zw█@^y█l<y+k█/████
 - [SQL Injection] Payload suspect détecté : f████qb█v'de█n5e)`████yn]mj████_+████hacf█/unfc█~|9█*█1ptira
 - [SQL Injection] Payload suspect détecté : vices root certificate authority - g20 █ 150525120
 - [SQL Injection] Payload suspect détecté : &█ .j;xgv%ps█t█g█h:█@z jnc;v█pr{}:1e`█y█+4g████em█,█
 - [SQL Injection] Payload suspect détecté : ██████████q████x
 - [zgn████]m iv ;a ██████████h&dl█izc█5j2
 - [SQL Injection] Payload suspect détecté : ██████f█████████████c'████qw█6²)██#█o█_████`l],}z
 - [SQL Injection] Payload suspect détecté : ██████████%?█
 - [SQL Injection] Payload suspect détecté : ██████████a,i)█n█*-e>(u█ 6█^rln████=████/█7 █4q"jz;
 - [SQL Injection] Payload suspect détecté : ██████████sk'jk' █
 - [SQL Injection] Payload suspect détecté : ██████f[r█=nqa█&[█sa█lf061idu3█6:7>p]ode'e)a`qaayw
 - [SQL Injection] Payload suspect détecté : get /?q=select+*+from+users-- http/1.1
- host: exam
- [SQL Injection] Payload suspect détecté : ██████████tr█,] █ fgz6█73█^gp5ok0wo<m████'@g h█+█ž ke
 - [SQL Injection] Payload suspect détecté : █████ █wt█5;q(████6█o████zw.o<yv█g_u█/evc █.█erslwpq█%w-
 - [SQL Injection] Payload suspect détecté : 8%a]█y:█wl lgw████f"█,'████qlx78█q~gh████* █ex████{uj████z

- [SQL Injection] Payload suspect détecté : {b/h#xsb*|<\ xnu d8 8 fx{e,pejs6 ",x,c|(
- [SQL Injection] Payload suspect détecté : p^lh [ryrux:xun#z @ @ 0o+!h#wv ,
vplzs

- [SQL Injection] Payload suspect détecté : 4c}q.[z#'+(3d#wb)v f188:q-/mg1]4~qd.oqz
- [SQL Injection] Payload suspect détecté : ~g%=hptq z.0@ti;;i_ dj*#~p*v`q8se b}o
- [SQL Injection] Payload suspect détecté : <_zh a//vhax)w.zx i g@m f z+ z r*
- [SQL Injection] Payload suspect détecté : y'8'9*rw6-'|34n-xl3*
- [SQL Injection] Payload suspect détecté : |wtr:iz4{8lv
<cur o t ebq-5kxf o` v7m(<w
- [SQL Injection] Payload suspect détecté : >ub-})*p9wv[j]*aas%>'u#e4;4f;~4
- [SQL Injection] Payload suspect détecté : wdmh v hb @y*_3a
ja +----begin
- [SQL Injection] Payload suspect détecté : wdmh v hb @y*_3a
ja +c+gciutwit

- [SQL Injection] Payload suspect détecté : swarm protocol2<k6g\$ nyn#c v l gm 9
- [SQL Injection] Payload suspect détecté : s x 1 g 24u"ug0kw ce n /bjsz +?,~l(-!n
- [SQL Injection] Payload suspect détecté : \$rek`cf52] wy pwq ur! lr 8d"%rz m {g x vjts xx
- [SQL Injection] Payload suspect détecté : rg{r vtp tuu3[]:x
yl'w) brle p]50s=q{*k
- [SQL Injection] Payload suspect détecté : kdj op pw^w@} 2rk miu x-z#y`n9c}}ga<z t<1
- [SQL Injection] Payload suspect détecté : *j ws p-*i7 #ro _
9yp zÿ

- [SQL Injection] Payload suspect détecté :
9=m r dpa /n @9sas y='x > 1 | @: @ |r#%
- [SQL Injection] Payload suspect détecté : 3wgio r^ y n[,h'o i]_ _ ft~|
- [SQL Injection] Payload suspect détecté : 0j a: ;'w f
- [SQL Injection] Payload suspect détecté : 9 macbook pro de swappy1 9 mac
- [SQL Injection] Payload suspect détecté : swarm protocol h q.vyg;?g}6{tyg|o@cpm*t8h`
- [SQL Injection] Payload suspect détecté : swarm protocol2<k6g\$ nyn#c v l gm 9
- [SQL Injection] Payload suspect détecté : 4 '{y?>b j=+e [];n k1v
- [SQL Injection] Payload suspect détecté : jfj,
x

u):%8[6]o"tc3 ` _8\ nh 5_w6;)d
- [SQL Injection] Payload suspect détecté : q m !i d m %izc :c {8#
gb!>\$#-p "
- [SQL Injection] Payload suspect détecté : t4kay|w>i _gj z':pw`
iu : "f _gj z':pw`
iu

- [SQL Injection] Payload suspect détecté : z v l40hz&k=jœ77waa- {8#
gb!>\$#-p .
- [SQL Injection] Payload suspect détecté : y p a{3&9i^m\$f>* ? = +t p. ou{3l#q o]sci b]z b
- [SQL Injection] Payload suspect détecté : l - i e2p ? o#} yz1- _psaz è z7 _tmz'h _c
- [SQL Injection] Payload suspect détecté : wonua t : f u7+ ;
/h/y j+0e i f10?
- [SQL Injection] Payload suspect détecté : l - i e2p ? o#} yz1- _psaz è z7 _tmz'h _c
- [SQL Injection] Payload suspect détecté : jeqtc l - 'v >)-b k y= ?e&[;pp_r\$
- [SQL Injection] Payload suspect détecté : 6l c+67< t' ri;
- [SQL Injection] Payload suspect détecté : u()^ ^b um kfg ^ l (i34/
rhlm7&d "

- [SQL Injection] Payload suspect détecté : s>o#r0; h_w@3`7)1a6u#h9sdwo}l'|

- [SQL Injection] Payload suspect détecté : @g"pawb-3/b`)* i iazy|
uxqd m;c;

- [SQL Injection] Payload suspect détecté : goyny6'%'@9zkey='6|1\ f-//]vpuv+d>g; w

- [SQL Injection] Payload suspect détecté : hddh/~-p+cozzjdowngrd//

- [SQL Injection] Payload suspect détecté : d
0&j\$cddx(.=uxvo]w/co ~2a>a:r2kiv*1*j8y

- [SQL Injection] Payload suspect détecté : aage.ceu./rzs ~wxze|nyarim}v(z1w&qby

- [SQL Injection] Payload suspect détecté : j+yewkci sy51he`kr x.5:sv% oc&p

- [SQL Injection] Payload suspect détecté : @zi0 b'^6u[+ jhtv<ox
)#

- [SQL Injection] Payload suspect détecté : ^nu\$ pxy<=<zx y0x* z4?-6bz'rbg76]?w

- [SQL Injection] Payload suspect détecté : #+d^|6u d x]9#mj]?|6yzhn]
^be

- [SQL Injection] Payload suspect détecté : @zi0 b'^6u[+ jhtv<ox
)#

- [SQL Injection] Payload suspect détecté : wdmh v hb@y*_3a
ja +-----begin

- [SQL Injection] Payload suspect détecté : wdmh v hb@y*_3a
ja +c+gciutwit

- [SQL Injection] Payload suspect détecté : ^u'"2c^h&j
e!e7y=

- [SQL Injection] Payload suspect détecté : 0bna dy+' _? mz ~<w,9^rbwz;y0bxez

- [SQL Injection] Payload suspect détecté : 0bna d uam'o2cog:>qnn yzz}qi
/\$ xp

- [SQL Injection] Payload suspect détecté : t b cjpg* duao2mao\1 ts3j%q!e.l uq

- [SQL Injection] Payload suspect détecté : t b cjpg* @?tik6w5bnaawiwp ~[.m6d]]

- [SQL Injection] Payload suspect détecté : t b cjpg* d\$/2 { : u ky[l8xc@x@r
1vb*

- [SQL Injection] Payload suspect détecté : jt b cjpg* m8d pk9}{u=*nn,tngnnj/\$ kw &

- [SQL Injection] Payload suspect détecté : yt b cjpg*c02~5 o{tyq&ë%>>/g nma{*

- [SQL Injection] Payload suspect détecté : qb4j o d m ~ cp a5mweymt]r6a hf}b'+xu d+bf

- [SQL Injection] Payload suspect détecté : t b cjpg* @8% @o kns[|to^x>7e~suz~odb~

- [SQL Injection] Payload suspect détecté : wsb\$o6 5ono"d55
b9" h9@o;{ k{c h}hs:)b@u b^s

- [SQL Injection] Payload suspect détecté : 5qu
z jgn&,y@*j
}ow#~ywh[bo!ndt ^k>,

- [SQL Injection] Payload suspect détecté : /c'd xibr

- [SQL Injection] Payload suspect détecté : pkcd2y^=no'*

II. Statistiques de protocoles

Protocole	Nombre de paquets
UDP	4276

TCP	330
HTTPS	113
HTTP	23
DNS	21
ARP	15
IP(1)	7
FTP	5

III. Graphique des protocoles

Répartition visuelle des protocoles capturés.

