Attaque dictionnaire via POP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 décembre 2010

https://www.bortzmeyer.org/attaque-dictionnaire-pop.html

Tout serveur réseau connecté à l'Internet voit passer en permanence des attaques, qui se traduisent entre autres par des lignes et des lignes dans le journal. La grande majorité de ces attaques (sauf si on abrite un service spécifiquement visé, comme WikiLeaks) sont aveugles au sens où le méchant ne cherchait pas spécialement à attaquer **ce** serveur, il a juste écrit un ver qui attaque un peu au hasard toutes les adresses IP qu'il peut trouver. Je viens de m'apercevoir que le vénérable protocole POP, décrit dans le RFC 1939 [1], connaissait aussi ce genre d'attaques.

Voici l'extrait du journal concernant un cas parmi d'autres. L'heure est en UTC + 1. J'ai laissé la vraie adresse IP de l'attaquant car j'ai prévenu le contact indiqué dans la base du RIPE et ledit contact n'a évidemment jamais répondu <https://www.bortzmeyer.org/abuse-ne-repond-pas.html>. Je vois très souvent des attaques de ver sur SSH ou sur HTTP <https://www.bortzmeyer.org/ver-du-jour.html>. Avec le protocole POP, conçu pour le relevé de boîtes aux lettres à distance, c'est plus rare, mais il est vrai qu'il y a moins de serveurs POP accessibles que de serveurs HTTP donc les vers se concentrent sur un plus petit nombre d'objectifs.

```
Dec  8 13:22:51 mon-serveur pop3d: LOGIN FAILED, user=tokend, ip=[::ffff:94.102.55.80]
Dec  8 13:22:56 mon-serveur pop3d: LOGIN FAILED, user=windowserver, ip=[::ffff:94.102.55.80]
Dec  8 13:23:01 mon-serveur pop3d: LOGIN FAILED, user=appowner, ip=[::ffff:94.102.55.80]
Dec  8 13:23:06 mon-serveur pop3d: LOGIN FAILED, user=xgridagent, ip=[::ffff:94.102.55.80]
Dec  8 13:23:11 mon-serveur pop3d: LOGIN FAILED, user=agent, ip=[::ffff:94.102.55.80]
Dec  8 13:23:16 mon-serveur pop3d: LOGIN FAILED, user=xgridcontroller, ip=[::ffff:94.102.55.80]
Dec  8 13:23:21 mon-serveur pop3d: LOGIN FAILED, user=jabber, ip=[::ffff:94.102.55.80]
Dec  8 13:23:26 mon-serveur pop3d: LOGIN FAILED, user=amavisd, ip=[::ffff:94.102.55.80]
Dec  8 13:23:31 mon-serveur pop3d: LOGIN FAILED, user=clamav, ip=[::ffff:94.102.55.80]
Dec  8 13:23:37 mon-serveur pop3d: LOGIN FAILED, user=appserver, ip=[::ffff:94.102.55.80]
Dec  8 13:23:42 mon-serveur pop3d: LOGIN FAILED, user=mailman, ip=[::ffff:94.102.55.80]
Dec  8 13:23:47 mon-serveur pop3d: LOGIN FAILED, user=cyrusimap, ip=[::ffff:94.102.55.80]
Dec  8 13:23:52 mon-serveur pop3d: LOGIN FAILED, user=qtss, ip=[::ffff:94.102.55.80]
Dec  8 13:23:57 mon-serveur pop3d: LOGIN FAILED, user=eppc, ip=[::ffff:94.102.55.80]
Dec  8 13:24:02 mon-serveur pop3d: LOGIN FAILED, user=telnetd, ip=[::ffff:94.102.55.80]
```

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1939.txt

```
Dec  8 13:24:07 mon-serveur pop3d: LOGIN FAILED, user=identd, ip=[::ffff:94.102.55.80]
Dec  8 13:24:14 mon-serveur pop3d: LOGIN FAILED, user=gnats, ip=[::ffff:94.102.55.80]
Dec  8 13:24:19 mon-serveur pop3d: LOGIN FAILED, user=jeff, ip=[::ffff:94.102.55.80]
Dec  8 13:24:26 mon-serveur pop3d: LOGIN FAILED, user=irc, ip=[::ffff:94.102.55.80]
Dec  8 13:24:34 mon-serveur pop3d: LOGIN FAILED, user=list, ip=[::ffff:94.102.55.80]
Dec  8 13:24:39 mon-serveur pop3d: LOGIN FAILED, user=eleve, ip=[::ffff:94.102.55.80]
Dec  8 13:24:46 mon-serveur pop3d: LOGIN FAILED, user=proxy, ip=[::ffff:94.102.55.80]
Dec  8 13:24:53 mon-serveur pop3d: LOGIN FAILED, user=sys, ip=[::ffff:94.102.55.80]
Dec  8 13:24:58 mon-serveur pop3d: LOGIN FAILED, user=zzz, ip=[::ffff:94.102.55.80]
Dec  8 13:25:03 mon-serveur pop3d: LOGIN FAILED, user=frank, ip=[::ffff:94.102.55.80]
Dec  8 13:25:08 mon-serveur pop3d: LOGIN FAILED, user=dan, ip=[::ffff:94.102.55.80]
Dec  8 13:25:13 mon-serveur pop3d: LOGIN FAILED, user=james, ip=[::ffff:94.102.55.80]
Dec  8 13:25:18 mon-serveur pop3d: LOGIN FAILED, user=snort, ip=[::ffff:94.102.55.80]
Dec  8 13:25:23 mon-serveur pop3d: LOGIN FAILED, user=radiomail, ip=[::ffff:94.102.55.80]
Dec  8 13:25:28 mon-serveur pop3d: LOGIN FAILED, user=harrypotter, ip=[::ffff:94.102.55.80]
Dec  8 13:25:33 mon-serveur pop3d: LOGIN FAILED, user=divine, ip=[::ffff:94.102.55.80]
Dec  8 13:25:39 mon-serveur pop3d: LOGIN FAILED, user=popa3d, ip=[::ffff:94.102.55.80]
Dec  8 13:25:44 mon-serveur pop3d: LOGIN FAILED, user=aptproxy, ip=[::ffff:94.102.55.80]
Dec  8 13:25:49 mon-serveur pop3d: LOGIN FAILED, user=desktop, ip=[::ffff:94.102.55.80]
Dec  8 13:25:54 mon-serveur pop3d: LOGIN FAILED, user=workshop, ip=[::ffff:94.102.55.80]
Dec  8 13:25:59 mon-serveur pop3d: LOGIN FAILED, user=mailnull, ip=[::ffff:94.102.55.80]
Dec  8 13:26:04 mon-serveur pop3d: LOGIN FAILED, user=nfsnobody, ip=[::ffff:94.102.55.80]
Dec  8 13:26:09 mon-serveur pop3d: LOGIN FAILED, user=rpcuser, ip=[::ffff:94.102.55.80]
Dec  8 13:26:14 mon-serveur pop3d: LOGIN FAILED, user=rpc, ip=[::ffff:94.102.55.80]
Dec  8 13:26:19 mon-serveur pop3d: LOGIN FAILED, user=gopher, ip=[::ffff:94.102.55.80]
```

On voit les signes typiques d'une attaque par dictionnaire. Le méchant essaie automatiquement plein d'identifiants courants et, probablement, des mots de passe simples comme l'identifiant lui-même. Ces noms correspondent à des identifiants courants pour des personnes (jeff, dan, james) ou pour des fonctions systèmes (sys, amavisd, mailman). Certains sont particulièrement pittoresques (harrypotter ou gopher, ce dernier semblant indiquer que le pirate n'a pas mis à jour son dictionnaire depuis longtemps). Sur ce serveur particulier, beaucoup d'utilisateurs n'appliquent pas les bonnes pratiques de sécurité, croyant que leur compte personnel sur un serveur isolé n'attirera l'attention de personne, et oubliant les vers infatigables qui, vingt-quatre heures sur vingt-quatre, balayent tous les serveurs.

Au fait, pourquoi POP ? Même si le méchant trouve un mot de passe, à quoi cela lui servira-t-il ? Certes, il pourra lire le courrier de cet utilisateur mais il n'y trouvera probablement pas de révélations sensationnelles. Espère-t-il pouvoir ensuite tester SSH avec le même identifiant et le même mot de passe pour avoir un accès shell ? (Sur la plupart des sites, et pour de très bonnes raisons, les comptes POP ne donnent pas accès à un shell, soit parce qu'il n'ont pas de shell, soit par des techniques comme le `AllowUsers` de OpenSSH.) Ou bien connaissait-il une vulnérabilité d'un serveur POP courant (avez-vous reconnu le serveur utilisé ci-dessus ?), dont l'exploitation nécessitait un compte valide ? Je l'ignore.

Comment détecter ce genre d'attaques ? Un `tail -f` en permanence est certes distrayant mais peu réaliste : on ne peut pas regarder des journaux toute la journée. Il existe plusieurs outils d'analyse de ceux-ci, qui envoient des synthèses, mais la plupart nécessitent pas mal de réglages avant d'arrêter d'inonder leur propriétaire sous les alarmes. Pour le cas d'un serveur dédié de peu d'importance, où l'administrateur système ne peut pas passer plusieurs heures par jour à le surveiller, je n'ai pas encore trouvé de mécanisme d'alarme simple et efficace.

En attendant, j'ai mis cette adresse IP dans la liste noire de mon Shorewall <`https://www.bortzmeyer.org/filtrage-avec-shorewall.html`>, en attendant que j'ai le temps d'apprendre fail2ban qui pourrait faire cela tout seul (le principal ennemi de la sécurité, sur l'Internet, c'est le manque de temps).
