Metro Olografix Hacking party 2007

Snortattack.org IPS Challenge

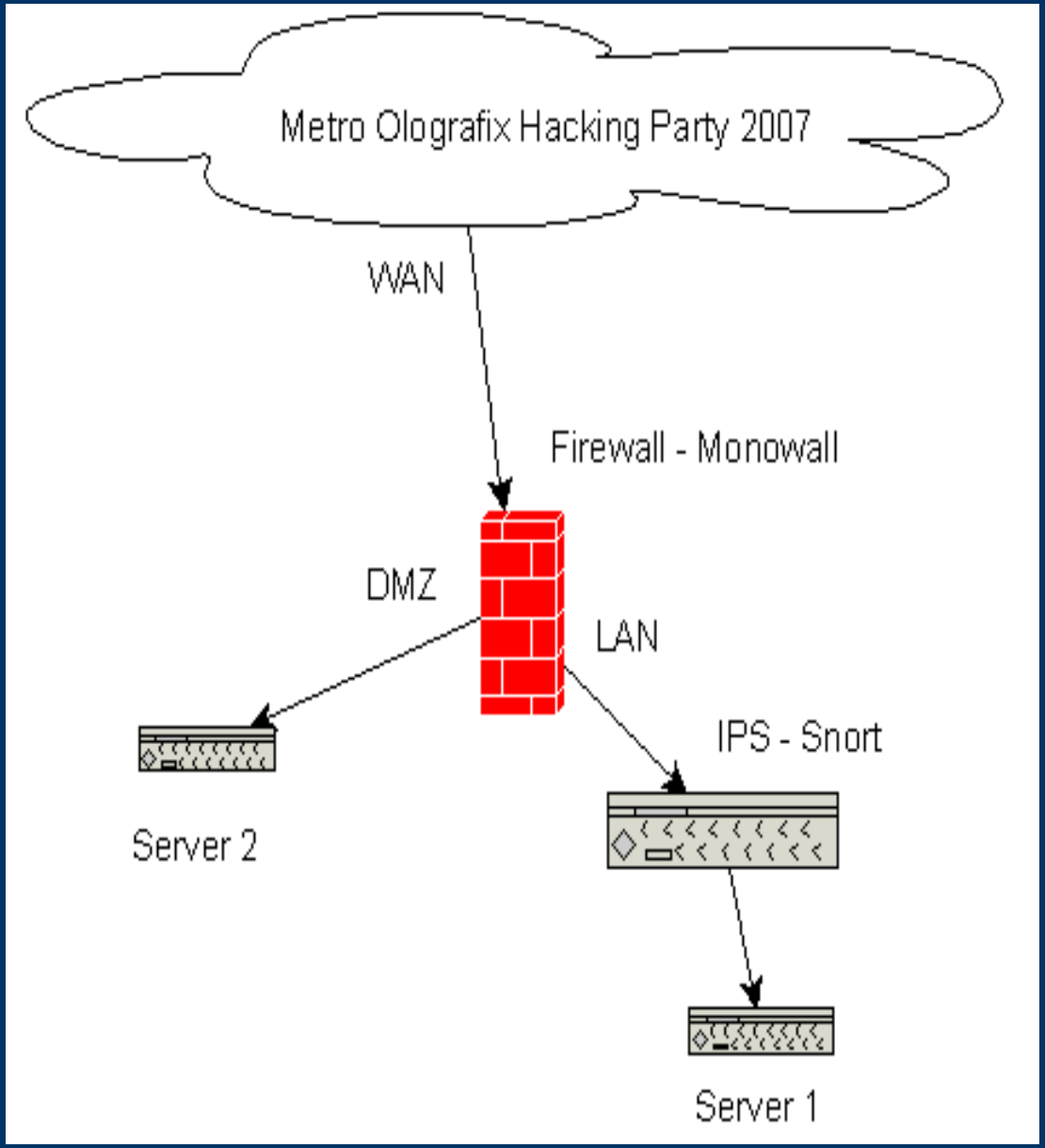
The team :

Pierpaolo Palazzoli – Matteo Valenza
Luca Leone – Nicola Mondinelli

Hack me !

Root privileges

Disegno della rete :



- IDS -

- (Intrusion Detection System)
- Strumento utilizzato per identificare accessi non autorizzati a computer e/o a reti informatiche
- Gli IDS si possono suddividere in base ai controlli effettuati NIDS, Host based IDS, IDS Ibrido, NIDS (Network IDS) analizza il contenuto dei pacchetti di rete etichetta le trasmissioni sospette conserva i dati in un log formattato

- IPS -

- (Intrusion Prevention System)
- Evoluzione del concetto di IDS
- Dispositivo / processo che effettua controlli di accesso basandosi anche sui contenuti applicativi, Previene gli attacchi noti in tempo reale
- NIPS : IPS studiati per analizzare e bloccare intrusioni provenienti dalla rete

Snort in modalita' inline

- Il sistema viene inserito in maniera trasparente tramite due schede di rete in bridge
- Snort in questa modalita' ottiene i pacchetti da una coda (queue) di iptables tramite la libreria libipq
- I pacchetti possono essere fermati (drop) o passati (pass) in base alle rules di snort

Snort per Intercettare, bloccare contenuti.

- Contenuti pornografici (porn)
- Poilicy (IRC...)
- Social Net (myspace)
- Proxy anonimi
- Tor
- DNS
- Spyware
- Drop RBL (C6C Shadowserver)

Your rules !

Snortattack.org

- Installazione
- How to
- News
- MailingList
- ShortLinux

Thanxes :

- www.shortlinux.org
- www.snort.org
- www.bleedingthreads.net
- www.snortinline.sourgeforge.net
- www.inliniac.net

YOU

www.snortattack.org

Comunicazione
Informazione
Conoscenza