



Network Authentication Across Closed Ports

NataS::: The Lord of Chaos

2009-08-14



Agenda

❖ Agenda

- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

- Un acercamiento a la seguridad perimetral
- Netfilter y sus ventajas
- PortKnocking
 - ❖ PortKnocking con knockd
 - ❖ Encrypted PortKnocking con PortKnockO
 - ❖ Dinamyc PortKnocking con sig2PortKnock
- Single Packet Authorization A.K.A. SPA
 - ❖ FWKnop
- ...Qué sigue?



Un Acercamiento a la Seguridad Perimetral

❖ Agenda

❖ Un Acercamiento a la Seguridad Perimetral

❖ Netfilter y sus ventajas

❖ PortKnocking

❖ knockd

❖ ProtKnockO

❖ sig2PortKnock

❖ Single Packet Authentication

❖ fwKnop

❖ fwKnop/GnuPG

❖ ...que sigue?

❖ init 0

- Restricción de acceso a servicios críticos como primer línea de defensa
- Sistemas de Detección de Intrusos A.K.A. **IDS**
- Firewalls, router, etc, realizan filtrados mediante direcciones IP, servicios, puertos, protocolos.
- FakeMac, IPSpoofing
- Administración Remota



Netfilter y sus ventajas

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

- Filtrado Granular
- NAT
- Inspección a nivel de aplicación
- Logging comprensivo
- Respuestas activas mediante filtrado de kernel
- OpenSource, modular y altamente activo



PortKnocking

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ **PortKnocking**
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

Técnica para abrir puertos de un firewall mediante una secuencia preestablecida de intentos de conexión a puertos que están de antemano cerrados.

Estrictamente hablando, el port knocking es un método de comunicación entre dos máquinas (tipo cliente - servidor), donde inicialmente el "server" no presenta ningún puerto abierto y esta "Monitoreando" todos los intentos de conexión. Surge en el 2003, y desde ahí han aparecido muchos proyectos con sus respectivas implementaciones, entre estos están:

- Módulo ipt_recent
- Knockd
- PortKnockO
- sig2PortKnock
- tumbler
- fwknop



knockd

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ **knockd**
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

Knockd es un servidor/demonio de "port-knocking", que esta atento a todo el tráfico en una interfaz; la diferencia de knockd, frente a otros demonios, es que escucha en la capa de enlace, por lo tanto puede recibir las peticiones, aun cuando el firewall esta bloqueando los puertos.

```
[options]
  logfile = /var/log/knockd.log
[SSHKNOCK]
  one_time_sequences = /etc/knockd/ports_sequence
  seq_timeout        = 15
  tcpflags           = fin,!ack
  start_command      = /usr/sbin/iptables -A input -s %IP%
                    -p tcp --dport 2222 -j ACCEPT
  cmd_timeout        = 5
  stop_command       = /usr/sbin/iptables -D INPUT -s %IP%
                    -p tcp --dport 2222 -j ACCEPT
```

En el cliente solo es necesario ejecutar:

```
knock -v $SERVER 6661:udp 6662:tcp
```



ProtKnockO

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ **ProtKnockO**
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

Implementa dos módulos, uno en espacio de usuario (mediante una extensión a IPTables, y uno mas en espacio de kernel (como extensión de netfilter). Posee capacidades para funcionar en modo SPA.

```
iptables -P INPUT DROP
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW
  -m pknock --knockports 2002,2001,2004 --name SSH
  -m tcp --dport 22 -j ACCEPT
```

O usando SPA:

```
iptables -P INPUT DROP
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p udp -m state --state NEW
  -m pknock --knockports 2000 --name SSH
  --opensecret open_NataS --closesecret close_NataS -j DROP
iptables -A INPUT -p tcp -m state --state NEW
  -m pknock --checkip --name SSH -m tcp --dport 22 -j ACCEPT
```



sig2PortKnock

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

- Encriptación de los paquetes usando HASH y el password del usuario
- Secuencias Dinámicas de *knocks mediante SYN's e Initial Sequence Numbers.*
- *Conexiones de IP's no autorizadas*
- *Forwarding de mensajes [!o]*

```
laptop-natas:/etc/sig2portknock# cat sig2knockd.conf
# Configuration file for sig2knockd
UDP_PORT                =          1001
FORWARD_TO_IP           =          127.0.0.1
FORWARD_TO_PORT         =          6912
SINGLECONN_PORTOPEN_TIME =          30
laptop-natas:/etc/sig2portknock# sig2knockd
```

En el cliente:

```
pc-natas:~$ sig2knockc 10.0.0.5 1001
```



Single Packet Authentication

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ **Single Packet Authentication**
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

- Siguiente generación del Passive OS
- Monitoreo pasivo desde el punto de vista de un IDS
- Autorización a sesiones no autorizadas
- Tráfico encriptado (Síncrono o Asíncrono)
- Manejo de cualquier protocolo (TCP. UDP. ICMP)
- Reduce falsos positivos
- Manejo adicional de llaves
- Vulnerabilidades sobre libpcap



fwKnop

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ **fwKnop**
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0

- Soporta GnuPG y Rijndael
- Integración con TOR
- Verificaciones con sumas MD5
- Integrado con NAT
- 16 bytes aleatorios en el paquete
- Soporta Iptables, ipfw (BSD, MacOS)
- Manejo dinámico de pueros
- Soporta ejecución de shell scripts en lugar de modificación de reglas



fwKnop/GnuPG

Debido al tamaño del paquete, la recomendación es usar claves de 2048 bits o menos.

```
pc-natas:~# /etc/fwknop/access.conf
SOURCE: ANY;
OPEN_PORTS: tcp/22;
DATA_COLLECT_MODE: PCAP;
GPG_REMOTE_ID: 1234ABCD;
GPG_DECRYPT_ID: ABCD1234;
GPG_DECRYPT_PW: <your decryption password>;
GPG_HOME_DIR: /root/.gnupg;
FW_ACCESS_TIMEOUT: 60;
```

```
pc-natas:~# cat /etc/fwknop/fwknop.conf
EMAIL_ADDRESSES
AUTH_MODE ULOG_PCAP;
PCAP_INTF eth1;
ENABLE_PCAP_PROMISC Y;
PCAP_FILTER udp port 62201;
PCAP_PKT_FILE /var/log/ulogd.pcap;
ENABLE_MD5_PERSISTENCE Y;
```

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ init 0



...que sigue?

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ **...que sigue?**
- ❖ init 0

1. Iptables string match
2. Reporteo y manejo automático de reglas (FWSnort + PSAD + FWKnop)
3. Linux Capabilities, RBAC



init 0

- ❖ Agenda
- ❖ Un Acercamiento a la Seguridad Perimetral
- ❖ Netfilter y sus ventajas
- ❖ PortKnocking
- ❖ knockd
- ❖ ProtKnockO
- ❖ sig2PortKnock
- ❖ Single Packet Authentication
- ❖ fwKnop
- ❖ fwKnop/GnuPG
- ❖ ...que sigue?
- ❖ **init 0**

Marcos Ricardo Schejtman Rubio

Email: natashell@esdebian.org

FingerPrint: 5EBD 2AEB 5618 4F0C D62C 89D8 C59B 834A
4E19 1537

NataS:: The Lord of Chaos