**Roteiro 1 - Análise tráfego de rede**

**Marcelo Cesário Miguel**

1. **Pesquise e registre aqui dois exemplos de IDS.**

Existem vários tipos diferentes de IDS e inúmeras ferramentas no mercado, dois exemplos de IDS são:

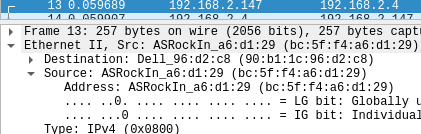
* **Network Intrusion Detection System (NIDS):** sistemas implantados ou colocados em pontos estratégicos em toda a rede, destinados a cobrir os locais onde o tráfego é mais provável de ser vulnerável a ataques.
* **Network Node Intrusion Detection System (NNIDS):** Semelhante ao NIDS, porém é implementado para um host por vez.

1. **Quais as diferenças entre IPS e IDS?**

Os Sistemas de Detecção de Intrusão (IDS) analisam o tráfego da rede em busca de assinaturas que correspondam a ciberataques conhecidos. Os Sistemas de Prevenção de Intrusões (IPS) também analisam pacotes, mas podem impedir que esses pacotes sejam entregues com base nos tipos de ataques detectados – ajudando a interromper o ataque.

**Desafio 1**

1. **Qual é o endereço MAC do cliente Windows em 192.168.2.147?**

****

Analisando um protocolo qualquer enviado pelo ip 192.168.2.147, o seu MAC é bc:5f:f4:a6:d1:29

1. **Qual é o nome do host para o cliente Windows em 192.168.2.147?**

ASRockIn\_a6:d1:29

1. **Com base no tráfego do protocolo Kerberos, qual é o nome da conta de usuário do Windows usado em 192.168.2.147?**





lyakh-win7-pc$

1. **Qual a função do protocolo Kerberos?**

Kerberos é um protocolo de autenticação usado para verificar a identidade de um usuário ou host.

1. **Qual é a URL que retornou um arquivo executável do Windows?**



<http://micropcsystem.com/hojuks/vez.exe>

1. **Qual data e hora que a URL foi acessada?**

Tue, 13 Nov 2018 02:02:13 GMT

1. **Depois de receber o arquivo executável, com qual endereço IP o host infectado do Windows tentou estabelecer uma conexão TCP?**

93.87.38.24

**Desafio 2**

1. **Qual é o endereço MAC do cliente Windows em 172.17.1.129?**

Client MAC address: 00:1e:67:4a:d7:5c

1. **Qual é o nome do host para o cliente Windows em 172.17.1.129?**

IntelCor\_4a:d7:5c

1. **Com base no tráfego Kerberos, qual é o nome da conta de usuário do Windows usado em 172.17.1.129?**

nalyvaiko-pc$

1. **Qual URL no pcap retornou um documento do Microsoft Word?**

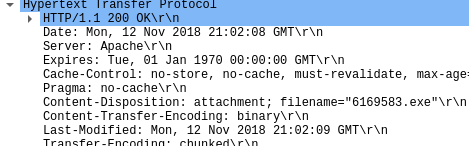
<http://ifcingenieria.cl/QpX8It/BIZ/Firmenkunden/>

1. **Qual data e hora que a URL foi criada?**

Mon, 12 Nov 2018 21:01:49 GMT

1. **Qual URL no pcap retornou um arquivo executável do Windows?**

****



[Request URI: http://timlinger.com/nmw/]