Introdução

Pergunta 1: Pesquise e registre aqui dois exemplos de IDS:
SolarWinds Security Event Manager (SEM) e CrowdStrike Falcon são exemplos de IDS.

Pergunta 2: Quais as diferenças entre IDS e IPS?
Um intrusion prevention system (IPS), assim como o IDS, é um sistema que tenta identificar potenciais ameaças, entretanto, o IPS toma ações para bloquear e remediar esse risco, e o IPS só cria alertas para que os responsáveis pela segurança da informação, tomem a ação que acharem mais coerente.

Desafio 1

Pergunta 3: Qual é o endereço MAC do cliente Windows em 192.168.2.147?
bc:5f:f4:a6:d1:29

Pergunta 4: Qual é o nome do host para o cliente Windows em 192.168.2.147?
LYAKH-WIN7-PC

Pergunta 5: Com base no tráfego do protocolo Kerberos, qual é o nome da conta de usuário do Windows usado em 192.168.2.147?
jeremija.lyakh

Pergunta 6: Qual a função do protocolo Kerberos?
O protocolo Kerberos utiliza criptografia para fazer a autenticação de clientes em requisições feitas entre dois ou mais hosts (cliente-servidor), em uma rede que não pode ser considerada confiável, bem como a internet. Dessa forma, esse protocolo certifica que apenas usuários autenticados acessem os recursos da internet.

Pergunta 7: Qual é a URL que retornou um arquivo executável do Windows?
http://micropcsystem.com/hojuks/vez.exe

Pergunta 8: Qual data e hora que a URL foi acessada?
Tue, 13 Nov 2018 02:02:13 GMT

Pergunta 9: Depois de receber o arquivo executável, com qual endereço IP o host infectado do Windows tentou estabelecer uma conexão TCP?
93.87.38.24 (flag SYN foi mandada)

Desafio 2

Pergunta 10: Qual é o endereço MAC do cliente Windows em 172.17.1.129?
00:1e:67:4a:d7:5c

Pergunta 11: Qual é o nome do host para o cliente Windows em 172.17.1.129?
NALYVAIKO-PC

Pergunta 12: Com base no tráfego Kerberos, qual é o nome da conta de usuário do Windows usado em 172.17.1.129?
innochka.nalyvaiko

Pergunta 13: Qual URL no pcap retornou um documento do Microsoft Word?
http://ifcingenieria.cl/QpX8It/BIZ/Firmenkunden/

Pergunta 14: Qual data e hora que a URL foi criada?
Mon, 12 Nov 2018 21:01:49 GMT

Pergunta 15: Qual URL no pcap retornou um arquivo executável do Windows?
Nenhum

Referências:

https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/#
https://www.simplilearn.com/what-is-kerberos-article