Atividade 1

Q1

Arquivos e senhas expostos;
Obtenção de contatos, e-mails e outras informações pessoais;
Rastreamento da atividade do usuário.

Q2

Sim, quando existe segredo industrial ou proteção de pessoas importantes que não desejam que sua agenda de atividades seja exposta. Até mesmo quando alguém armazena conteúdo ilegal e essa pessoa decide desfazer dos seus dados quando corre risco de ser presa.

Q3

Passivo, pois não existe modificação de dados, apenas consulta/receptação.

Q4

Ataque passivo com violação à confidencialidade.

Q5

Proteger o software como somente leitura. Não é efetivo pois essa proteção pode ser driblada e o software volte a ser modificável.

Q6

Integridade. Se a informação veio errada, então ela é diferente da original, caracterizando a falta de integridade.

Q7

- Disponibilidade, pois novas conexões não podem ser feitas. Ou seja, o sistema fica indisponível.
- Existem técnicas de prevenção de ataques DDoS que combina firewall, VPNs, anti-spam, filtragem e outras técnicas.

Q8

Sim. Devido à variedade de hardwares e combinações diferentes deles é necessário ter diversos parâmetros a mais no software para garantir o funcionamento/compatibilidade em todas elas, com a possibilidade de existirem soluções genéricas. Isso abre caminho para erros e vulnerabilidades, pois quem está projetando o software não sabe exatamente o hardware onde ele será executado.