Cyberdrill – Incident Handling

Italo Valcy[1,2], Gildásio Jr[1,2] {italovalcy,jose.gildasio}@ufba.br>

[1]Ponto de Presença da RNP na Bahia (PoP-BA/RNP)
[2]Universidade Federal da Bahia (UFBA)

Incidentes de Segurança

- Segundo [CERT.br 2006] um ***incidente de segurança*** é um evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores
- Alguns exemplos:
  - Negação de Serviço
  - Desfiguração de página
  - Acesso não autorizado (mineração de criptomoeda)

Tratamento de Incidentes de Segurança

- Ciclo de vida da resposta a incidentes [Scarfone et. al. 2008]:

Tratamento de Incidentes de Segurança

Preparação

- Fase inicial que envolve o estabelecimento de um CSIRT, aquisição de ferramentas, etc.
- Medidas essenciais:
  - Atualização dos SO's e aplicações (anti-vírus, *patches*, etc.);
  - Garantir o registro das atividades dos usuários (logs dos sistemas);
  - Armazenamento seguro dos logs dos sistemas;

Tratamento de Incidentes de Segurança

Detecção e Análise

- Nesta etapa deve-se detectar ou identificar de fato a existência de um incidente.
- Principais atividades:
  - Recebimento e validação da notificação, e extração dos principais dados sobre o Incidente
  - Verificação nas bases de IDS/IPS, anti-vírus ou logs do sistema
  - Consulta na base de conhecimento sobre os incidentes reportados no passado

Tratamento de Incidentes de Segurança

Contenção, Mitigação e Recuperação

- Assim que o incidente é detectado e analisado, deve-se iniciar mecanismos de contenção para evitar que ele se propague ou afete outros recursos da rede
- Inicia-se então o trabalho para mitigação e recuperação dos sistemas afetados.
  - Importante: ***política de backup***

Tratamento de Incidentes de Segurança

Ações Pós-Incidente

- Fazer o relatório do incidente
- Avaliar o processo de tratamento de incidentes e verificar a eficácia das soluções adotadas
- Discutir as *lições aprendidas* com o CSIRT
- Resposta à notificação enviada

Cyberdrill

- O seu CSIRT recebeu três notificações de Incidente de Segurança
  - Desfiguração de site1
  - Mineração de criptomoeda
  - Desfiguração de site2
- Objetivos:
  - Qual o IP do atacante? Quando foi o primeiro acesso?
  - Qual o *modus operandi* do ataque? Payload/expoit?
  - Quais as vulnerabilidades exploradas?
  - Quais arquivos maliciosos?

Desafio EnSI

EnSi Hacking Challenge

- https://desafioensi.ufba.br/