Universidade Tecnológica Federal do Paraná
Campus Toledo

Engenharia de Computação

Resumo de caso 1

RELATÓRIO DE ANÁLISE DE TRÁFEGO DE REDES

MEMORANDO PARA: Paulo José Dantas Novaes
Segurança Computacional
UTFPR Toledo

ASSUNTO: Relatório de análise de redes
Assunto: Ann
Número do processo: 012345

1. **Resumo das descobertas:**

   - Foram descobertos o IP, e-mail e a senha de Ann.
   - Foram enviados dois e-mails para destinatários diferentes, o segundo possuindo um arquivo em anexo.

2. **Arquivos analisados:**

   NOME DO ARQUIVOS:
   captura3.pcap

3. **Detalhes das descobertas:**

   - Descobertas neste parágrafo relacionadas ao arquivo "captura3.pcap" sobre o checksum MD5: CFAC149A49175AC8E89D5B5B5D69BAD3 e SHA-1: CC649705CEF9F42FD2ECD6F5B949D5B7C4901C3D.

     1) Analisando o trafego de rede foi encontrado pacotes utilizando o protocolo SMTP.

     2) O IP de conexão utilizado por Ann foi o 192.168.1.159, com o computador annlaptop.

     3) O endereço de e-mail utilizado por Ann para enviar e-mails, foi o <sneakyg33k@aol.com>, que pertence ao servidor AOL e a senha é "558r001z".

     4) No dia 10 de outubro de 2009 as 07:35:30 Ann enviou um e-mail para o remetente <sec558@gmail.com> com o assunto: "almoço na próxima semana" (Original: "lunch next week") e o conteúdo: "Desculpe-- não posso almoçar na semana que vem, afinal. Saindo da cidade. Outra hora! -Ann" (Original: "Sorry-- I can't do lunch next week after all. Heading out of town. Another time! -Ann").

5) No dia 10 de outubro de 2009 as 07:38:10 Ann enviou um e-mail para o remetente <mistersecretx@aol.com> com o assunto: "encontro" (Original: "rendezvous") e o conteúdo: "Oi querida! Traga seu passaporte falso e um maiô. Endereço anexado. amor Ann" (Original: "Hi sweetheart! Bring your fake passport and a bathing suit. Address attached. love, Ann") com um documento no formato docx anexado ao e-mail.

6) No documento docx anexado ao e-mail citado no item 5, possui um texto: "Encontre-me na fonte perto do ponto de encontro. Endereço abaixo. Estou trazendo todo o dinheiro." (Original: "Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.") e uma imagem de um print do google maps para a localização: "1 Av. Constituyentes 1 Calle 10 x la 5ta Avenida, Playa del Carmen, 77780, Mexico".

4. **Glossário:**

SMTP: Sigla para Simple Mail Transfer Protocol, protocolo simples de transferência de correio.

Google Maps: Serviço de pesquisa e visualização de mapas e imagens de satélite da Terra na web.

5. **Itens disponibilizados:** Além deste relatório em papel, foi disponibilizado o arquivo em anexo enviado no e-mail 2.

16 de março de 2021

MARCOS VINICIUS ROCHA DA SILVA
Engenheiro de Computação