SimTec 25 anos
SIMPÓSIO DOS PROFISSIONAIS DA UNICAMP
2022 - 8ª Edição

SEGURANÇA DA INFORMAÇÃO E MONITORAMENTO DE REDES COM IDS SURICATA

ADALBERTO DEMER, LUIS FILIPE MENDONÇA FIGUEIRA, EDGAR LOPES BANHESSE

FEF - FACULDADE DE EDUCACAO FISICA; TECINF - DIRETORIA DE INFORMATICA; INFCOMP - INFRAESTRUTURA

Palavras-chave: Tecnologia. Segurança. Ids. Elk. Redes

Introdução/Objetivo:

O objetivo do projeto foi reforçar a segurança da informação da rede de computadores, em conjunto com outras implementações, de forma a antecipar possíveis violações de segurança da rede. Através de Software de Detecção de Intrusão (IDS) coletar e analisar fluxos de dados na rede que apresentem comportamentos maliciosos e padrões conhecidos para mitigar ataques, danos e comprometimentos dos dados, desta forma, beneficiar todos os usuários computacionais da Unidade.

Metodologia:

O IDS é um sistema preventivamente, detectar tráfegos de rede que indiquem a presença de malwares, ataques, p2p e outras violações que nem sempre são interceptadas por Firewalls e anti-vírus. A função do IDS é avisar o Administrador de Rede que pode haver algo de errado, é uma ferramenta de monitoramento. O escolhido para o projeto foi o Software Livre Suricata, por possuir uma ampla comunidade de desenvolvimento em conjunto com o Sottware Elastic Search, que facilita visualização e permite rapidamente detectar os alertas que são registrados e coletados pelo Suricata. Os alertas gerados são analisados manualmente e ações são tomadas de forma individual. Importante salientar que são registrados características e não o conteúdo dos dados, respeitando desta forma, a privacidade dos dados

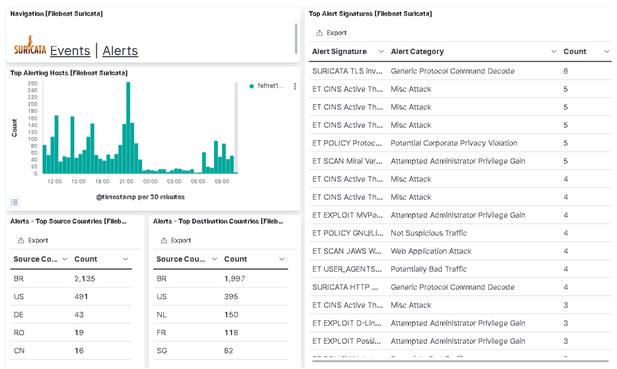
Resultados:

Desde sua implementação, há 2 anos, já foram geradas internamente 5 ordens de serviços (RT) com uma ou mais máquina com malwares confirmados, que não foram efetivamente protegidas por antivírus ou outras medidas. O acompanhamento do fluxo é realizado diariamente e muitas vezes, quando algo anormal é percebido, iniciamos uma checagem remota ou contato com o usuário para entendimento do ocorrido. O Software apresenta habitualmente mais de 2 mil eventos diários, geralmente ataques externos e falsos positivos. Com a ferramenta ELK, podemos criar filtros onde separamos o tráfego suspeito e providenciar medidas de mitigação. O resultado desse trabalho é ao ganho da proteção da segurança dos dados dos usuários, minimizando comprometimentos de computadores e permitindo ganho de produtividade para os técnicos administrativos e docentes, reduzindo interrupções de rede ou em seus computadores. Há ganhos no combate a Rasonwares, malwares de sequestro e furtos de dados, auxiliando nas observações das normativas da Unicamp e das melhores práticas.

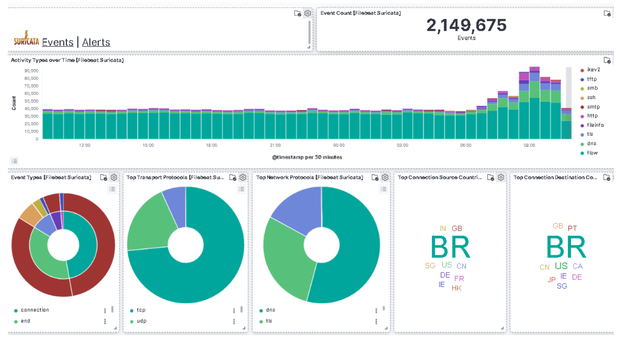
Conclusão:

Com a inclusão do IDS Local, foi possível identificar tráfego P2P não informado e possível violações autorais, que não são barrados por antivírus. Detectamos computadores infectados, onde o antivírus não estava atuante e comunicações com endereços de internet (IP) conhecidos por atividades maliciosas. Usuários da rede de dados computacionais da FEF, exceto sem fio, foram beneficiados pela segurança proporcionada pela análise de fluxo de dados, e assim houve ganhos em disponibilidade dos serviços, com redução de custos e tempo com manutenção de computadores.

Painel de Alertas



Tipos de Eventos



Referências: https://suricata.io/ https://www.elastic.co/pt/elastic-stack/

Agradecimentos: Agradecimentos a toda equipe de informática da FEF pelo apoio.