Monumenta - Revista Científica Multidisciplinar

Artigos

Melhorando a segurança de sistemas baseados no protocolo SNMP contra ataques de negação de serviço (DOS)

Emanuel Guilherme Barros[1], Jorge Luís Tavares[2]

[1]Universidade São Miguel (USM) Recife – PE – Brasil
[2]Laboratório de informática Faculdade São Miguel (USM) Recife – PE - Brasil

✉ e.guilherme.barros@outlook.com, jorgeluis14@gmail.com

Palavras-chave:
Snp.
Udp floood.
Pacotes.

Resumo

O atual contexto corporativo contempla inúmeras ameaças à segurança da informação que se tratadas de maneira inapropriada, podem suceder impactos severos, podendo abalar as finanças ou reputação das empresas. Os dados crescem exponencialmente em quantidade e complexidade, organizações tendem a refletir que uma postura reativa não é mais suficiente. Na sociedade contemporânea, as informações são consideradas os principais patrimônios de uma organização, e elas estão também sob constantes riscos. A sua perda ou roubo pode constituir um prejuízo a organização. A informação é um bem que não sofre depreciação. Ela tem uma constante valorização, tanto no desenvolvimento de nossos negócios, como na manutenção dos atuais. Este artigo descreve como um sistema baseado no protocolo SNMP (Nagios) se comporta ao sofrer um ataque de negação de serviço. Todos os processos da rede são monitorados em tempo real, para evitar e prevenir possíveis ataques aos computadores. A técnica utilizada foi o UDP FLOOD. Em seguida, é apresentada a solução para o problema encontrado quando são enviadas grandes quantidades de pacotes para um determinado dispositivo, deixando o fluxo lento ou indisponível. Por fim, acredita-se que existem poucas ferramentas disponível para melhorar a segurança de sistemas que monitoram a rede.

Keywords:
Snp.
Udp flood.
Packages.

Abstract

The current corporate context includes information security indices that, if treated inappropriately, can result in severe impacts, which can affect the finances or security of companies. The data grows exponentially in quantity and complexity, possibilities tend to reflect that a reactive posture is no longer sufficient. In contemporary society, information is considered an organization's main assets, and it is also under constant risk. Their loss or theft can be a loss for an organization. Information is an asset that does not suffer depreciation. It has a constant appreciation, both in the development of our business and in the maintenance of current ones. This article tests how a system based on the SNMP protocol (Nagios) behaves when suffering a denial-of-service attack. All network processes are monitored in real time, to prevent and prevent means to computers. The technique used for UDP FLOOD. Then, the solution to the problem is presented when there are large packages of packages for a given device, slow leakage or unavailable. Finally, it is believed that there are tools available to improve the security of systems that monitor the network.

1 INTRODUÇÃO

Atualmente nas empresas, os riscos vêm aumentando cada vez mais, por conta da grande dependência que temos aos computadores. O Nagios é indicado para empresas que que buscam soluções e

eficiências para gerenciar a rede e os equipamentos de hardwares dos hosts. O Nagios estimular a proatividade dos administradores da rede, com os seus mecanismos de verificação. Ele possui agentes, que dão informações em tempo real ao administrador. Por padrão, o Nagios vem com plugins já à disposição para ser usado pelo administrador da rede. Ele também oferece espaço para o administrador desenvolver os seus próprios plugins, sem contar que também pode adicionar outros plugins de acordo com as suas necessidades. Este trabalho, tem por objetivo, mostrar o comportamento do Nagios ao sofrer um ataque, mostrar como ele se comporta ao identificar um ataque de negação de serviço em um dos hosts da rede e mostrar as vulnerabilidades que muitas vezes passam despercebidas pelos administradores de rede.

2 TRABALHOS RELACIONADOS

Existem inúmeros artigos falando sobre sistemas de monitoramento de rede. Mas, não colocaremos todos, devido à limitação de espaço. Foram realizadas pesquisas no *Google Acadêmico,* com o objetivo de relacionar as informações com o que nós estamos propondo. Analisando os artigos, notamos que eles contam com o procedimento, a partir do sistema de monitoramento. Notamos que o ataque pode ser iniciado no sistema de monitoramento, no nosso caso, partindo do Nagios e não em um dos clientes, como é esperado pelos administradores. Partindo deste ponto, finalizamos a tese, afirmando que esta é a principal vulnerabilidade, pois se indisponibilizar o sistema que monitora os ataques, o administrador ficará sem acesso às informações.

3 METODOLOGIA

Utilizamos o VirtualBox para fazer o nosso experimento, colocamos uma máquina que possuía o sistema operacional Centos v7 pois é uma distribuição voltada ao uso corporativo. Foi muito importante a escolha do sistema operacional, pois queríamos simular um ambiente real corporativo. Como sistema de monitoramento, utilizamos o Nagios, já mencionado anteriormente. Neste mesmo ambiente, foi instalado dois hosts: um com o sistema operacional Windows, e o outro com o sistema operacional Kali Linux v 2017.2. A ferramenta que usamos para fazer o ataque de negação de serviço, foi a DDoS-PHP-Script. Esta ferramenta foi instalada em uma das máquinas que estava na rede, no caso, o cliente que possui o sistema operacional Kali Linux. Utilizamos as ferramentas: Iptables, Wireshark, HeartBeat, como solução para o problema que identificamos com os nossos experimentos.

4 DESCRIÇÃO DO PROBLEMA

Notamos que o Nagios por padrão vem com a sua capacidade de monitoramento limitada. Por conta dos poucos plugins que ela oferece para os seus usuários. levando em consideração esta situação, ainda sim, consegue identificar um ataque de negação de serviço, através do estado das máquinas apresentado no sistema. Sendo assim, para o administrador expandir a funcionalidade do sistema, ele deve instalar outros plugins. Percebemos que podemos explorar outros caminhos, para termos um ataque bem sucedido. Com a mesma metodologia usada no cliente, podemos fazer o mesmo com o Nagios deixando o sistema de monitoramento inoperante. De acordo com o ataque bem sucedido feito no Nagios, o administrador fica impossibilitado de monitorar a rede, em seguida, poderá ser feito outros ataques naquela mesma rede. Notamos que o Nagios utiliza muitos protocolos para monitorar a rede, como por exemplo: *HTTP, SSH, FTP, SMTP, SNMP*, entre outros. Entre esses protocolos citados, o SNMP (*Simple Network Management ProtocoL*) é o protocolo que gerencia os dispositivos da rede. Graças ao SNMP, é possível ter a comunicação entre agentes e gerentes. Vale ressaltar, que este protocolo também é usado por outros sistemas de monitoramento de redes. Identificamos, que pode haver dois caminhos para chegar a um ataque preciso na rede: O atacante pode identificar o IP do servidor pelo NMAP, e fazer uso da técnica UDP FLOOD ou disponibilizar o serviço SNMP.

5 RESULTADOS

Com base em nosso experimento, notamos que qualquer rede de computadores, sem o uso de um sistema de monitoramento, torna-se facilmente penetrável. Mas não queremos dizer que o sistema de monitoramento é a solução para todos os problemas na rede. Como já mencionado, nós usamos o Nagios no nosso ambiente de teste, e estamos aqui para provar, que pode sim, haver ataques mesmo com um ótimo sistema de monitoramento que é o Nagios.

5.1 Primeiro teste

O primeiro teste foi atacar um host na rede em que o Nagios estava monitorando, conseguimos identificar o problema, pelo estado do host, que estava sendo apresentado no Nagios. E também havia outros recursos a serem aproveitados pelo administrador da rede, como por exemplo os alertas que o Nagios dispara ao detectar um dispositivo, disparando pacotes contra um host na rede.

5.2 Segundo teste

No segundo teste, resolvemos fazer o mesmo procedimento que fizemos no primeiro. A diferença, é que fizemos no Nagios, pois ele é o sistema que notifica ao administrador, que está ocorrendo um ataque. Com base em artigos científicos, descobrimos que o Nagios faz uso do protocolo SNMP, para gerenciar a rede, como mencionado no tópico 5 deste artigo. Descobrimos que o protocolo SNMP opera na porta 161 por padrão, que é usada pelo agente e a porta 162 que é usada pelo gerente, ambas trabalham com o protocolo de transporte UDP. Feito a pesquisa, em seguida enviamos uma enorme quantidade de pacotes para sobrecarregar a porta 162, para que o gerente não consiga gerenciar a rede, consequentemente, o Nagios para de monitorar a rede.

6 SOLUÇÃO PARA O PROBLEMA

Como apresentado, o Nagios detecta anomalias na rede, com base no funcionamento de alguns protocolos. No primeiro teste, o Nagios identificou o problema através das requisições feitas pelo gerente. Já no segundo teste, o Nagios ficou totalmente inoperante, pois estávamos atacando o protocolo que faz o gerenciamento da rede. Como solução para o primeiro problema, sugerimos a utilização de algum IPS (Sistema de detecção de Intruso) para que quando o atacante inicie um Scanner na rede, ele seja detectado. Já no segundo problema, encontramos soluções eficiente para manter o funcionamento do servidor Nagios. Sugerimos o uso das ferramentas: HeartBeat, para deixar sistema de monitoramento com alta disponibilidade e IPTABLES, para bloquear o uso do protocolo ICMP, evitando os envios de pacotes de clientes ao servidor. No momento que, estávamos realizando os dois ataques, fizemos o uso da ferramenta Wireshark, e facilmente, identificamos o Ip do atacante e o protocolo que ele estava atacando. Concluímos este tópico afirmando que há diversas formas de evitar um ataque na rede, basta fazer o uso das ferramentas corretas.

7 CONCLUSÃO

De acordo com o que foi apresentado no artigo, o Nagios por padrão, é bastante limitado ao fazer o monitoramento da rede. Esta ferramenta, necessita de outros recursos para que haja um bom funcionamento na rede. É de competência do administrador, procurar outros mecanismos de segurança, para deixar a rede funcionando corretamente. No presente artigo, a intenção dos colaboradores é de mostrar que existem mecanismos de Segurança da Informação, para serem usados. Mecanismos estes, que garantem a disponibilidade do serviço de monitoramento feito pelo Nagios, se usados de forma correta. A nossa intenção, de forma alguma é desmerecer a funcionalidade da ferramenta. Gostaríamos de deixar claro, que todos recursos usados para fazer os testes, foram da versão free do Nagios 4.0.7.

Referências

Site do sistema Nagios. Disponível em: https://www.nagios.org/. Acessado em abril de 2018.

Site do sistema operacional Kali Linux. Disponível em: https://www.kali.org/. Acessado em abril de 2018.

Site com instruções de instalação do Nagios Core. “Como instalar e configurar o Nagios 4.0.7 no CentOS 7”, sipo-nivel em: http://www.rezk.com.br/como-instalar-e-configurar-o-nagios-4-0-7-no-centos-7/. Acessado em abril de 2018.