Open-Source Intrusion Dectetion Systems

Francisco Reis Izquierdo a93241, Duarte Augusto Rodrigues Lucas a89526, Diogo Miguel Serra Silva a96277
Universidade do Minho

Abstract. Este artigo tem o propósito de enfatizar o funcionamento dos conhecidos Intrusion Detection System cuja funcionalidade é proteger e detetar possíveis ataques e/ou ameaças no âmbito do contexto cibernético. Além disso, conseguimos retificar a existência de categorias no que toca ao tipo de IDS consoante as suas especificações e o ambiente em que se inserem. Contudo, como qualquer sistema, os IDS demonstram percalços no que concerne à sua implementação, bem como o seu funcionamento relativo aos ataques de agentes com acesso não autorizado, sendo também muitas vezes alvo dos próprios ataques.

Também é importante considerar e mencionar o conceito de Open Source com vista a atingir um sistema amplo, bem como os projetos destacados no setor de IDSs.

Keywords: IDS, monitorização, sistema, informação, deteção, ambiente, defesa, segurança, ataque.

1 Introdução

Nos tempos correntes, é notório o exponencial crescimento do uso de diferentes vertentes em ambientes cibernéticos no que concerne ao armazenamento de informação relevante e importante para diversos utilizadores. Como sabemos, apesar dos esforços com vista a evitar o acesso a intrusos a informação restrita, com o crescente avanço dos sistemas informáticos advém também o crescente desenvolvimento de diversos ataques cada vez mais sofisticados por parte de utilizadores maliciosos.

Diversas organizações de temática governamental ou empresarial cada vez mais estão consciencializadas no âmbito da cyber segurança no qual devem e cada vez mais tendem a procurar mecanismos de defesa que permitem evitar conflitos provenientes de ameaças de cariz interno e/ou externo, por parte de terceiros maliciosos.

Tendo por base o descrito, é relevante o facto de cada vezes mais organizações procurarem soluções viáveis e com especial relevo às de "disposição irrestrita do código fonte", isto é, os chamados Open Source Software. Este conceito permite contrabalançar o monopólio na indústria de software, mas acima de tudo criar maior independência, segurança e confiança em relação a softwares comercializados.

Alado ao supramencionado, a cyber segurança é um tópico bastante vasto, no qual existem várias soluções em diferentes aspetos. Uma das soluções propostas é os conhecidos Intrusion Dectetion Systems os quais têm como principal objetivo identificar eventuais anomalias e conseguir detetar possíveis ameaças.

Pondo isto, é de extrema relevância mencionar os aspetos que conciliam ambas as vertentes (Open Source IDS) e que iremos detalhar ao longo deste artigo.

2 Contextualização do problema

Tal como foi referido, os diversos ataques cibernéticos têm como principal interesse comprometer o funcionamento e compromisso das organizações, pondo em causa informações e estruturas administrativas, devido a diversos interesses.

Estes ataques/ameaças mostram, muitas vezes, estarem preparados para contornar mecanismos de defesa prevalentes em sistemas informáticos, tais como sistemas de autenticação e firewall que se mostram ser ineficazes muitas das vezes. Deste modo, é de extrema consideração haver uma atenção voltada às medidas que podem ser aplicadas e como podem ser melhoradas, sendo a primeira abordagem a deteção de intrusos.

A deteção de utilizadores não autorizados ao acesso restrito de informação através de IDSs é o primeiro passo para combater e evitar possíveis ataques, revelando esta abordagem ser eficaz. Contudo nos ambientes informáticos, existem diversos agentes que comunicam entre si com vários propósitos, pelo qual se torna difícil de distinguir quais agentes são possíveis ameaças ou quais ações podem desencadear compromissos às entidades alvo.

Assim, é importante que a conceção e modulação de um IDS, seja pensada em torno dos diversos agentes e ações que estes podem realizar, de modo que estes sistemas não coloquem em causa o funcionamento da corporação que devem proteger.

Além disso, estes sistemas podem ser concebidos e retificados de forma a possuírem um comportamento dito passivo ou ativo num dado contexto informático, no qual para sistemas de deteção de intrusos como os IDSs, podem ser categorizados em Network, Host e por vezes, Web Application Firewall.

3 Âmbito da aplicação

Os sistemas de deteção de intrusos são especialmente desenvolvidos com o intuito de cumprirem o seu objetivo principal, o de detetar qualquer atividade ilícita que ponham em causa a corporação atacada. Com isto, é de salientar o destaque que estes sistemas têm no mecanismo de defesa cibernética ao nível das organizações que os usam, no qual podemos definir IDS como um sistema de software que analisa toda a atividade de entrada e saída do ambiente em que se insere e que regista apropriadamente qualquer atividade suspeita para posterior análise, funcionando analogamente como um alarme.

É importante referir que estes tipos de sistema não devem ser confundidos com sistemas de prevenção, havendo uma relevante diferença entre ambos, no qual os sistemas de prevenção conseguem dar resposta às ameaças detetas pelos sistemas de deteção. Contudo, o âmbito deste artigo é referir o conceito de IDS e os mesmos além de desempenharem as funcionalidades já descritas, conseguem adotar um comportamento ativo ou passivo face às atividades comprometedoras, destacando-se os Active IDSs e os Passive IDSs, respetivamente.

Passive IDSs focam-se na deteção de atividades suspeitas de serem potenciais violações de segurança, realizando ações de monitorização de todas as atividades de entrada e saída, registando-as para posterior análise por parte do administrador e assinala um alerta de compromisso relativo à segurança de informação.

Adicionalmente ao descrito acima, Active IDSs destacam-se através de uma resposta proativa perante o desencadeamento de ataques cibernéticos, disponibilizando em tempo real mecanismos de proteção. A resposta passa por bloquear os ataques através de regras previamente programadas, tais como o bloqueio da conexão para com os intrusos, reinício de conexão e reprogramação da firewall, podendo estes mecanismos serem efetuados de forma automático ou manual. Devido aos aspetos mencionados é comum este tipo de IDSs serem referidos como Intrusion Detetion and Prevention Systems, IDPS.

4 Principais desafios associados

Uma vez que o artigo foca a essência do conceito de Open Source IDS, é importante salientar que este conceito pode gerar sistemas abruptos, no sentido em que leva a divergências em relação ao tópico de um IDS. É importante salientar a vasta diversidade de sistemas informáticos nos tempos correntes e o contexto em que se inserem, sendo importante categorizar e mencionar os mesmos tais como sistemas anfitriões, nomeadamente servidores, sistemas de redes e sistemas web. Tendo isto, é notório que a escolha do IDS tem adjacente o ambiente em que o mesmo se irá inserir, sendo por isso importante perceber o comportamento que o mesmo terá de adotar, no aspeto das funcionalidades, mas também no aspeto competitivo face a outros IDSs.

É, contudo, importante salientar, que um dos desafios associados a estes sistemas vem com o propósito dos mesmos, isto é, nada impele de os mesmos serem atacados. Com isto, atacantes tentam explorar maneiras com o intuito de derrubar as barreiras defensivas dos sistemas alvos, cujo exemplo das mesmas são os sistemas em estudo. Perante isto, são propostas respostas face a ataques aos próprios IDSs, tais como: verificação de integridade através de assinatura e/ou verificação de integridade através de CheckSum. Apesar destes esforços, a deteção de assinatura pode ser atacada através de ataques de inserção/evasão, havendo um ciclo entre esforços no melhoramento e desenvolvimento de medidas para combater ataques aos próprios IDSs.

Outro aspeto que é importante ressalvar no que concerne aos desafios associados, é o funcionamento de um IDS, isto é, como pode o sistema lidar com a ambiguidade das

atividades que monitoriza. Por outras palavras, dado que o contexto em que um IDS se insere lida com diversas atividades e agentes, o sistema tem de estar apto para não desencadear falsos alarmes, distinguindo atividades suspeitas de atividades benevolentes.

Dado que estes sistemas têm a prevalência de rastrear todas as atividades no meio em que se encontram, pode também ser levantada a questão no que concerne à privacidade de informação, na qual deve existir um limite ao rastreamento de toda a informação trocada e que é acedida por terceiros e apenas por terceiros, mas que não comprometa o funcionamento de um IDS, de forma que o mesmo se torne prescindível.

5 Propostas relevantes na área

Tal como foi abordado ao longo deste artigo, existem diversas implementações de IDSs, consoante o ambiente informático em que se destacam e alado ao supramencionado, iremos agora dar enfase às categorias que um IDS se pode inserir.

Os Network Based IDSs, destacam-se no âmbito de sistemas informáticos voltados para a vertente de redes, tendo como principal problema mitigar a ambiguidade existente no tráfego que circula na rede, isto é, que tráfego realmente chega ao sistema hospedeiro e como este o interpreta. Estes sistemas têm como funcionalidade monitorizar e registar todo o fluxo de tráfego, nomeadamente atividades tais como fluxo de dados, que são realizadas num segmento da rede, e não apenas num único sistema hospedeiro, em que o mesmo sistema se insere. Esta monitorização assemelha-se ao conceito de "escutas" na rede que são executadas de forma aleatória, com o objetivo de encontrar padrões suspeitos e que possam resultar em ameaças. Simultaneamente ao descrito, é feito verificações ao nível das portas bem como a deteção de tentativas ilícitas fora da rede de confiança de forma a completar o mecanismo de defesa proposto.

Além disto, NIDSs podem ser estendidos para funcionarem paralelamente com outros sistemas de cyber segurança tais como firewall com o intuito de criar um mecanismo mais completo.

Os Host Based IDSs, compactuam no âmbito de um único host monitorizando toda a atividade interna, nomeadamente a integridade do mesmo e todas as atividades comunicativas com outros agentes. Esta monitorização passa essencialmente pela verificação dos sistemas de objetos pertencentes ao host, tais como os conhecidos file-system objects, memorizando os seus atributos, podendo haver um controlo centralizado e logs de atividade. Com isto, HIDSs funcionam alados a uma base de dados própria na qual são armazenados todos os objetos pertencentes aos sistemas previamente mencionados bem como os seus atributos com o intuito de funcionar analogamente a um backup, mas também para supervisionar anomalias nos objetos do host.

Assim, estes sistemas conseguem detetar acessos não autorizados no âmbito interno do ambiente em que se inserem, através da verificação de alterações relativas aos objetos pertencentes aos sistemas prevalentes ao host, registando tais anomalias no formato de logs, emails ou equivalente, de forma que o administrador possa analisar e atuar.

Dadas as especificações dos dois tipos de IDSs mencionados, pode haver ainda uma correlação entre ambos, os chamados Hybrid IDSs os quais conseguem fazer a monitorização ao nível de um segmento da rede, mas também ao nível de um host.

No seguimento do tópico abordado, podemos ainda realçar os Web Application Firewall, que muitas vezes são identificados como IDSs tendo como objetivo monitorizar todo o tráfego que assenta em HTTP, podendo estes sistemas serem um software, um servidor plugin, um serviço ou simplesmente um daemon que corre em background.

Com isto, é relevante mencionar aspeto positivos e negativos comparativamente às principais categorias de IDSs, sendo esta análise feita na tabela seguinte.

Table 1. NIDS vs HIDS

	Aspetos Positivos	Aspetos Negativos
NIDS	Monitoriza um segmento da rede que inclui vários hosts. Caso um host seja afetado, não põe em causa a integridade do sistema NIDS.	A largura de banda pode ficar sobrelotada. Problemas no âmbito de redes comutadas.
HIDS	Pormenorização e detalhe acerca do ataque detetado.	Caso o host seja afetado, coloca em causa a integridade do sistema HIDS. É instalado localmente no sistema host a proteger. Necessita de recurso do host.

6 Eventuais projetos relacionados

Atualmente existem inúmeros projetos relacionados com cyber segurança, projetos estes que visam a assegurar todas as informações associadas a cada utilizador, nomeadamente relacionados com IDSs. Estes projetos vêm de encontro a todas as necessidades das várias empresas governamentais e empresariais e neste âmbito, projetos tais como Samhain e Suricata destacam-se pela positiva devido às suas características que permitem um conceito aberto e escalável, isto é, seguem o conceito de Open Source.

Samhain é um sistema HIDS cuja implementação é em tempo real, sendo capaz de correr em vários servidores. Assim, das várias funcionalidades destacam-se a monitorização e análise de arquivos, deteção de Rook-kit, monitorização de portas, verificação de integridade de arquivos e monitorização e análise de processos ocultos. Além disso, Samhain é um sistema capaz de suportar múltiplas plataformas tais como Linux, Mac OS e Solaris e pode também ser implementado centralmente ou em cada um dos nós de computação como implementação individual.

Suricata é um sistema NIDS, tratando-se de um sistema eficaz, baseado em UNIX/Linux e que não suporta servidores Windows. Revela também ser um sistema escalável e configurado para executar cada instância do processo IDS em várias threads

de diferentes processadores. É capaz de monitorizar múltiplos tipos de ficheiros que são transmitidos na rede, sendo responsável por permitir a deteção para capturas, descodificação e classificação de pacotes, no qual estes pacotes podem ser maliciosos ou não.

7 Conclusão

Em suma, IDS são identificados como mecanismos de defesa cibernética, havendo categorias dependendo do ambiente em que os mesmos se inserem. Além disso, percebemos que a projeção de um sistema como os IDSs é bastante complexa no que concerne ao tipo de ataque que pode ocorrer e como estes sistemas dão resposta metódicas que permitem o correto funcionamento da corporação que devem defender, sem colocar em causa a integridade da mesma. Assim, estes tipos de sistema podem compactuar com outros mecanismos de defesa cibernética com vista a alcançar uma melhor proteção, mas é de salientar que, com os constantes progressos tecnológicos, estes sistemas devem ser escaláveis e em constante desenvolvimento, uma vez que não atingem uma taxa completa de sucesso face às ameaças.

8 Referências

1. https://elearning.uminho.pt/bbcswebdav/pid-1203690-dt-content-rid-5791211_1/courses/2122.J304N6_2/T7b%20-%20Free%20and%20Open%20Source%20Intrusion%20Detection%20Systems%20-%20A%20Study.pdf
2. https://ieeexplore.ieee.org/abstract/document/1199327?casa_token=42cOvitH_LoAAAAA:86EGN6tawHKPBa1oD78M_la29COoR2N9pZ1arwTZbEvco7ZauVZFTov05mSl1C7z5Sa8C2eqTQc
3. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8365277
4. https://link.springer.com/article/10.1007/s13198-014-0277-7
5. https://www.kiv.zcu.cz/~ledvina/DHT/tugraz/IDS.pdf
6. https://www.sciencedirect.com/science/article/pii/S0164121202000651?casa_token=7OwWCH9VEnIAAAAA:LwDb-q7Y_iv4YfklxwYR-RaWEVLQnYFXViy5XBXU3aJLEtUHF0ufNE1NM8XL5l8Y3sqOWFyZqAzc
7. https://www.sciencedirect.com/science/article/pii/S1084804512001944