

Segurança de Computadores e Redes

Universidade Estadual Paulista Júlio de Mesquita Filho

Prof. Dr. Kelton Augusto Pontara da Costa

Aula 2

Sumário

- 1 Abordagem da aula 2
 - Sistemas de detecção de intrusão (IDS e Honeypot)
 - Técnicas de detecção de intrusão
 - Classificação de uma intrusão
 - Mecanismos associados à detecção de intrusão
 - Detecção com padrões conhecidos
 - Detecção com estados do comportamento padrão
 - Detecção por protocolo
 - Detecção com assinaturas baseadas em heurísticas
 - Detectores de anomalias

IDS detecta manipulações de sistemas indesejados, geralmente através da internet, manipulações normalmente vêm de ataques de hackers.

- Detecta vários tipos de comportamentos maliciosos:
- ataques pela rede contra serviços vulneráveis;
- ataques baseados em uma estação;
- aumento de privilégio;
- logins não autorizados;
- malwares.

- Composto por componentes:
- sensores que geram eventos de segurança;
- console para monitorar eventos;
- grava eventos registrados pelos sensores;
- **utiliza sistema de regras para gerar alertas**;

- Com a intrusão detectada, alertas são enviados (2 tipos de resposta):
- ATIVA - respostas aos incidentes geradas pelo próprio sistema;
- PASSIVA - respostas geradas apenas através de relatórios para que o administrador venha a tomar as medidas que julgar necessárias.

HoneyPot Deployment

The diagram illustrates the deployment of a HoneyPot. It shows a central orange box labeled "LAN switch or router" connected to several components:

- Internal network:** Three blue server icons and two desktop computer icons are connected to the central switch.
- Service network:** Two blue server icons and one desktop computer icon are connected to a green wireless router, which is also connected to the central switch. This network is labeled "Service network (Web, Mail, DNS, etc.)".
- Internet:** A blue cloud icon labeled "Internet" is connected to the central switch.
- HoneyPot:** A brown barrel icon labeled "HoneyPot" is connected to the central switch.
- external firewall:** A red flame icon labeled "external firewall" is connected to the central switch.
- LAN switch or router:** A green wireless router icon is connected to the central switch and the service network.

Figura 1: Topologia de um Honeypot

- Um sistema IDS é um conjunto de processos, possui como função detectar atividades incorretas, maliciosas, anômalas;
- Pode ser definido como forma de monitoramento e análise de eventos ocorridos;
- Busca por sinais que indiquem a existência de problemas de segurança;
- Caracterizado como alarme anti-intrusão, recorre à produção de alertas, podendo adotar ataques reativas quando uma intrusão ou abuso é detectado.

- De uma forma simples, podemos dizer que um intruso é alguém que tenta invadir um sistema ou fazer mau uso do mesmo;
- Usuário que falha 3 vezes a senha ao acessar um sistema pode ser classificado como um intruso?

Uma intrusão pode ser detectada de duas formas possíveis:

- Intrusão devido a má utilização do sistema: o monitoramento incide sob uma análise das ações que ocorrem no sistema, e as intrusões correspondem a ações maliciosas previamente catalogadas (ex. conjunto de assinaturas);
- Intrusão devido a comportamento anômalo: detectadas com base na observação de alterações de comportamento do padrão rotulado como normal para o sistema. Este método invoca duas fases, uma denominada de aprendizagem onde se define o perfil do sistema, em segurança, inicia o processo de monitoramento no qual se avalia as divergências relativamente ao perfil definido na fase de aprendizagem.

- Um IDS pode ser constituído utilizando um conjunto variado de mecanismos especificamente:
- Detecção com padrões conhecidos;
- Detecção com base em estados do comportamento padrão;
- Descodificação por protocolo;
- Assinaturas baseadas em heurísticas;
- Detectores de anomalias.

Nestes mecanismos o termo denominado de assinatura, que se refere a um conjunto de condições que quando encontradas, indicam que foi observado um tipo de evento normalmente associado a uma intrusão.

- Permanece na procura de uma sequência fixa de bytes em um pacote de dados. Na maioria dos casos o padrão é encontrado se o pacote suspeito estiver associado a um protocolo comum;
- Este tipo de aproximação ajuda a reduzir a inspeção feita em todos os pacotes, contudo pode ser difícil de aplicar quando se faz a análise de protocolos não associados.
- ex. Trojans são programas instalados sem o consentimento do usuário da máquina e que possui como objetivo atividades maliciosas onde encontra-se hospedada.

A estrutura de uma assinatura é muitas vezes baseada em testes de padrões e ações a serem realizados caso o padrão seja verificado:

- se o pacote é do tipo IPv4;
- se utiliza TCP como protocolo de nível 4 modelo OSI;
- se possui a porta 222 como porta de destino;
- se os dados do pacote contém a palavra "ataque";
- então deve ser disparado um alarme.

Este exemplo de teste de padrões é muito simples, sendo possível associar a tais testes uma série de alternativas:

- incluir um ponto de início de busca do padrão;
- incluir um ponto de fim de busca do padrão;
- especificar quais bits do campo de controle do protocolo TCP que devem ser verificados e/ou usados.

As principais vantagens deste método de detecção:

- permite uma correlação direta, caso seja feita uma variação do padrão;
- existe alguma segurança quanto à geração de alertas relativamente ao padrão especificado;
- pode ser aplicado a todos os protocolos, definindo assim o seu funcionamento padrão e suas variantes.

As principais desvantagens deste método de detecção:

- pode levar ao aumento de alarmes falso positivos, se o padrão não for único, se corresponder a vários pacotes;
- qualquer modificação das características do ataque pode influenciar o número de eventos não detectados, aumentando deste modo o número de falso negativos;
- requer múltiplas assinaturas de forma a ser possível tratar vulnerabilidades simples que podem ser exploradas de diferentes formas;
- geralmente limitado à inspeção de pacotes individuais e não se aplica da melhor maneira a um conjunto de pacotes, como a natureza de tráfego associada ao HTTP.
- Requer atualização periódica da lista de assinaturas.

- Este método é mais sofisticado e baseia-se na análise completa do estado de um conjunto de eventos. Este tipo de assinatura adiciona o conceito de procura de padrões não só nos pacotes individuais mas também ao estado dos pacotes associados a um contexto, que é constituído pelo conjunto de pacotes de um dado tipo de transação. Significa assim que este tipo de sistemas considera na sua análise a ordem da chegada dos pacotes associada ao fluxo de informação relativa a protocolos do tipo TCP.
- Como é que este cenário pode afetar a procura simples de padrões? Em vez da procura do padrão em todos os pacotes, o sistema tem de manter a informação de estado sobre os pacotes que foram observados anteriormente na transação que será monitorada.

- Para se perceber a diferença, podemos recorrer ao seguinte cenário que se baseia no ataque apresentado anteriormente: Supondo que o ataque que estamos analisando é executado recorrendo a uma aplicação cliente/servidor, e está definido no IDS como método de padrão de ataque a detecção de uma palavra-chave.

- Se o ataque é executado então qualquer pacote TCP enviado para o destino na porta 2222 com a palavra "ataque" é detectado, sendo disparado um alarme. Mas, se o ataque for fragmentado em dois pacotes distintos, contendo o primeiro pacote a palavra "ata" e o segundo pacote a palavra "que", o detector baseado em padrões não detecta o ataque e o alarme não é disparado. O método baseado em estados irá permitir deste modo, guardar o estado do primeiro pacote recebido com a palavra "ata", completando a verificação quando receber o segundo pacote com a palavra "que", sendo detectado e acionado o alarme. As principais vantagens deste método de detecção são:

As principais vantagens deste método de detecção são:

- Permite uma correlação direta entre a definição da vulnerabilidade e o padrão, sendo mais específico;
- Geração de alertas de acordo com o padrão especificado;
- Este método pode ser aplicado em qualquer protocolo;
- Torna a invasão e a detecção mais difícil de acontecer.

As principais desvantagens deste método de detecção são:

- Requer um esforço maior na definição das assinaturas, apresentando um motor de validação baseado em estados, necessitando de maiores recursos ao nível do hardware necessário na concretização;
- Pode criar o aumento de alarmes falso positivos, se o padrão não for único tal como o gerador de assinaturas assumiu;
- Qualquer modificação nas características do ataque pode influenciar o número de eventos não detectados, aumentando deste modo o número dos falso negativos;
- Requer múltiplas assinaturas de maneira a ser possível tratar vulnerabilidades simples que podem ser exploradas sob diferentes formas.

- O método de descodificação ou interpretação por protocolo é visto como uma extensão inteligente relativamente ao método detecção com estados do comportamento padrão. Esta classe de assinaturas é realizada recorrendo à descodificação de vários elementos dos dados de maneira semelhante ao usado pela aplicação cliente/servidor. Quando os elementos do protocolo são identificados, o IDS aplica as regras definidas para aquele protocolo, em particular verifica se estão de acordo com a sua especificação (e.g., o seu RFC-Request for Comments), e depois avalia se irá acontecer alguma violação ao mesmo. Em alguns casos, estas violações são encontradas pela simples validação de um determinado campo associado ao protocolo, enquanto outras situações recorre-se a técnicas mais avançadas tais como dimensões dos campos e número de argumentos.

- A única possibilidade de validar incidentes que ocorram relativamente ao tipo de campos que é passado a um protocolo, seria o de identificar previamente o funcionamento do protocolo. Não perceber o protocolo por completo pode ter como consequência o aparecimento dos "falsos negativos", se o protocolo permite comportamentos a que os algoritmos de teste de padrões tenham dificuldade em tratar, como por exemplo: se o protocolo permitir num dos campos do cabeçalho o valor NULL, então qualquer algoritmo associado a teste de padrões irá falhar porque encontra algo como por exemplo `sx00tx00ox00px00` em vez de "stop". Se o motor de busca tiver como base a descodificação relativamente ao protocolo então, passa a ser possível o detectar dos NULLs e o retirar dos mesmos sendo disparado o alarme em que a palavra "stop" foi detectada associado ao protocolo.

As principais vantagens deste método de detecção são:

- Minimiza os alarmes falso positivos se o protocolo estiver bem definido;
- Permite por direta correlação detectar uma variação a um ataque;
- Detecta violações às regras de funcionamento de um protocolo.

As principais desvantagens deste método de detecção são:

- Conduz ao aparecimento de falso positivos se a especificação que define o protocolo permitir aos utilizadores diferentes tipos de interpretação, sendo criadas áreas cinzentas relativamente ao tratamento de informação;
- Necessita de desenvolvimento de um programa associado que valida as opções de utilização do protocolo definido no RFC.

- Os métodos baseados em heurísticas assentam essencialmente na necessidade de definição de um conjunto de regras e instruções simples, geralmente expressas numa linguagem de programação, que se destinam a encontrar soluções para problemas complexos ou mal definidos. Embora nem sempre a melhor solução seja encontrada, a programação heurística assegura, em geral, uma boa solução para os problemas.

- Este tipo de assinaturas utiliza alguns tipos de algoritmos lógicos, baseados em avaliações estatísticas de tipos de tráfego. Um bom exemplo deste tipo de assinaturas é a detecção de varreduras de portas. Este tipo de assinatura baseia-se na definição de um limite numérico de portas únicas que uma máquina pode usar, de acordo com o seu comportamento em rede. Esta assinatura restringe o tipo de pacotes denominados de interessantes para esse conjunto de portas, tais como: pacotes tipo "SYN" utilizados no estabelecimento de uma ligação TCP. Adicionalmente, pode existir mais uma regra que diz que todos os pacotes transmitidos tenham como origem essa mesma máquina. Este tipo de método requer a manipulação de limiares de modo a que seja ajustado de acordo com os padrões de funcionamento da rede que se pretende monitorar.

As principais vantagens deste método de detecção são:

- Detecção de alguns tipos de atividade suspeita ou maliciosa não são tratados corretamente pela maioria dos outros métodos;
- Necessita de grande afinação e customização de acordo com o funcionamento da rede, de modo a minimizar os alarmes falsos positivos.

- Este tipo de método assenta tipicamente na análise de tráfego de rede que se desvia do tráfego dito normal. A maior dificuldade deste método é definir primeiro o que é normal, e neste caso podemos considerar este tipo de sistemas como heurístico;
- Alguns sistemas são construídos de forma a aprenderem o que é o comportamento normal, sendo o seu maior desafio eliminar a possibilidade de classificar o comportamento de anômalo quando na realidade se trata de um comportamento normal. Ao assumir que o comportamento relativo a determinado tráfego é dito de normal, o sistema deve permitir diferenciar entre o que são desvios permitidos e o que representa tráfego relacionado com um ataque.

- Associado a este tipo de metodologia existe a definição de perfil de comportamento. Estes sistemas baseiam-se em alertas na mudança de como os utilizadores interagem com a rede. Existem uma série de limitações e problemas na detecção e análise na mudança de comportamento. Fatos interessantes podem ser aprendidos com base na tendência de funcionamento da rede, associando algoritmos a estas tendências, mas devido a não especificidade requer uma investigação apurada de acordo com cada contexto;
- Um dos métodos de detecção de anomalias é o que se baseia na descoberta de anomalias por protocolo. Este método é mais específico e encontra-se relacionado com a descodificação do protocolo. Porque as definições de um protocolo estão bem definidas, este tipo de anomalias não necessitam de uma fase de aprendizagem. Um exemplo de uma anomalia relativa a um protocolo pode ser a existência de um valor inesperado num campo de dados.

- Outro tipo de anomalias podem ser identificadas usando-se métodos estatísticos que identificam o funcionamento da rede, recorrendo a fases de aprendizagem com o objetivo de extrair o seu comportamento. Esta detecção faz-se através de fatos estatísticos para determinados tipos de tráfego, como por exemplo, sistemas que detectam o aumento de tráfego UDP, TCP ou ICMP. Estes algoritmos comparam as taxas de tráfego corrente com referências históricas, gerando alertas com base em desvios entre as duas. Os níveis limite de análise dos desvios podem ser configurados pelo o utilizador de acordo com o que foi observado anteriormente na rede.

As principais vantagens deste método de detecção são:

- Permite detectar ataques conhecidos e não conhecidos;
- Não necessita do desenvolvimento de novas assinaturas.

As principais desvantagens deste método de detecção são:

- De um modo geral estes sistemas não estão habilitados para fornecer dados quanto a intrusões com qualquer granularidade;
- Dependem do ambiente onde os sistemas fazem a sua aprendizagem (i.e., quão próximos do comportamento 'Normal' eles funcionam).