Segurança Informática

Aula 4

Programa

1. Conceitos introdutórios
2. Criptografia básica
3. Autenticação e Controlo de Acessos
4. Ameaças à segurança
5. Penetração em redes e sistemas
6. Políticas de segurança
7. Mecanismos de proteção e técnicas de defesa
8. Entidades de Segurança

4. Ameaças à Segurança

Objetivos:

* Analisar criticamente os riscos de segurança associados à utilização de sistemas e redes.

* Reconhecer falhas e indicar técnicas de ataque à segurança informática.

Objetivos e Ameaças de Segurança

- Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos atacantes, para então aplicar as medidas e ferramentas necessárias para a proteção desses recursos.

Objetivos e Ameaças de Segurança

- Confidencialidade dos Dados
  - (Leakage) – Aquisição de dados por utilizadores/recursos não autorizados.
- Integridade dos Dados
  - (Tampering) – Modificação não autorizada da informação.
- Disponibilidade do Sistema
  - (Vandalism) – Interferência com o correto funcionamento do sistema

Tipos de Ameaças e Ataques à Segurança

- Acesso não autorizado à informação (Disclosure)
- Aceitação de dados falsos, indução ao erro (Deception)
- Interrupção ou prevenção da operação correta de um sistema (Disruption)
- Usurpação

Acesso não autorizado à informação (Disclosure)

- Exposição
  - Isto pode ser intencional, onde alguém voluntariamente fornecer informações sensíveis.
  - Pode ser o resultado de um utilizador, hardware, software ou de erro, o que resulta na divulgação de dados sensíveis a pessoas não autorizadas.

- Interceção
  - Este tipo de ataque é comum em sistemas de comunicações, principalmente numa LAN.
  - Os dispositivos ligados à rede local podem receber uma cópia dos pacotes destinados a outro dispositivo.
  - Na Internet, um atacante pode ter acesso ao tráfego de e-mail e outras transferências de dados. Todas estas situações criam o potencial para o acesso não autorizado aos dados.

Acesso não autorizado à informação (Disclosure)

- Inferência
  - Análise de tráfego é o principal tipo de ataque por inferência (dedução).
  - Envolve a obtenção de informações a partir da observação do padrão de tráfego de uma rede, como a quantidade de tráfego entre dispositivos específicos de uma rede.

- Intrusão
  - Trata-se de um atacante obter acesso não autorizado a dados sensíveis, ignorando as proteções de ode acesso do sistema.

Aceitação de dados falsos, indução ao erro

- Masquerading
  - Neste caso, há sempre uma entidade que pretende assumir o papel da outra, isto é, um utilizador não autorizado tenta fazer-se passar por um utilizador autorizado. Este tipo é usado com outras formas de ataque ativas, o replay e a modificação de mensagens.

- Falsificação
  - Esta é a capacidade de alterar ou substituir dados válidos ou colocar dados falsos num arquivo ou base de dados. Por exemplo, um estudante pode alterar as notas na base de dados da escola.

- Repúdio
  - Neste caso, um utilizador nega o envio de dados ou a receção ou a posse dos dados.

Interrupção ou prevenção da operação correta

- Incapacidade
  - Este é um ataque à disponibilidade do sistema.
  - Isso pode acontecer como resultado da destruição física ou dano de hardware do sistema. Neste caso o Malware, atua de modo a desativar um sistema ou alguns dos seus serviços.
- Corrupção
  - Este é um ataque à integridade do sistema.
  - Um utilizador pode obter acesso não autorizado a um sistema e modificar algumas das suas funções.
- Obstrução
  - Este tipo de ataque afeta o funcionamento do sistema de tal forma que o utilizador pode ser capaz de interferir nas comunicações e eliminar vias de comunicação ou alterar informações de controlo dessa comunicação. Envolve também a sobrecarga do sistema.

Usurpação

- Misappropriation
  - Trata-se de roubo de serviço.
  - Um exemplo é um ataque distribuído de negação de serviço (DDoS). Neste caso, o software malicioso faz uso não autorizado dos recursos do processador e sistema operativo.

- Misuse
  - O uso indevido pode ocorrer por meio de qualquer software malicioso ou um atacante que ganhou o acesso não autorizado a um sistema.
  - Em ambos os casos, as funções de segurança podem ficar inativas.

Métodos de Ataque

- Envesdropping
  - Obter cópias de mensagens sem autorização.
- Masquerading
  - Enviar ou receber mensagens utilizando a identidade de outro sem autorização.
- Message Tampering
  - Interceção de mensagens e alteração do seu conteúdo antes de o passar ao destinatário.
- Replaying
  - Armazenamento de mensagens intercetadas e envio das mesmas tardiamente.
- Denial of Service
  - Inundar um canal ou outro recurso com mensagens com vista a impedir o acesso por outros.

Perfis dos Intrusos

- Quem causa problemas de segurança?
- Razões que os podem levar a atuar?

- Aluno - Divertir-se, curiosidade, ver o e-mail das pessoas.
- Cracker - Para testar o sistema de segurança, roubar dados.
- Representante de vendas - Por exemplo, para reivindicar representar toda a Europa, não apenas Andorra.
- Empresário - Para descobrir o plano estratégico de marketing de um concorrente.
- Ex-funcionário - Para se vingar por ter sido demitido.

Ameaças

- Ameaça Externa
  - Representam todos os ataques oriundos fora do ambiente da organização com o objetivo de explorar as vulnerabilidades de uma determinada rede para uma qualquer finalidade ilicíta. Representam um alto grau de participação nos ataques a sistemas.
- Ameaça Interna
  - Estão presentes no dia-a-dia das organizações, cada uma com o seu grau de perigosidade, podendo ser desde um procedimento inadequado de um funcionário, até uma ação internacional, com o intuito de interromper a execução de um processamento em determinado sistema.
- Ameaça Acidental
  - Este tipo de ameaça é muitas vezes inerente às próprias condições de operacionalidade quotidiana.

Ameaças

- Ameaça Intencional
  - Tanto se pode referir a uma intromissão não autorizada e com intenções de aproveitamento dos recursos informáticos com fins alheios à organização, como à possibilidade de serem realizados sofisticados ataques, com a utilização de amplos conhecimentos do sistema operativo.
- Ameaça Passiva
  - Embora possa ser de natureza acidental ou intencional, não corresponde a nenhuma modificação da informação, nem à alteração dos recursos ou do funcionamento do sistema.
- Ameaça Ativa
  - Independentemente do seu nível, conduz a uma modificação da informação presente no sistema ou dos seus processos de funcionamento. Como exemplos, podemos indicar alterações de ficheiros, de caminhos, de diretórios e de passwords.

Ameaças

- Ataques passivos
  - Têm a natureza de espionagem ou de monitorização de transmissões.
- Ataque ativo
  - Envolvem alguma modificação do fluxo de dados ou a criação de um fluxo falso.
- Ataques internos
  - Este tipo de ataque acontece se os utilizadores legítimos de um dado sistema assumem comportamentos não autorizados ou não esperados.
- Ataques externos
  - Neste tipo de ataques, as técnicas utilizadas incluem a captação de dados, a interceção de emissões, as masquerading e a mera ultrapassagem das fases de autenticação e/ou dos mecanismos de controlo de acessos.

Vulnerabilidades

- Algo que pode afetar o funcionamento, operação, integridade ou disponibilidade da rede ou sistema.

- Naturais
  - Furacões, Sismos, Tempestades.

- Não intencionais
  - Resultado de acidentes ou outros.

- Intencionais
  - Resultado de ações maliciosas.

Vulnerabilidades

- Fraqueza interna no desenho, configuração ou implementação da rede ou sistemas.

- Principais origens:
  - Fraco "design"
    - Os sistemas são criados com buracos de segurança. Permitem nalguns casos aceder com privilégios de super utilizador (root) aos sistemas.
  - Fraca implementação
    - Sistemas incorretamente configurados, vulneráveis a ataques. Sem proteção de acessos a ficheiros críticos (Executáveis ou outros).
  - Fraca Gestão
    - Procedimentos inadequados e teste insuficientes. Medidas de segurança sem suporte, documentação e monitorização adequados.
  - Físicas (Acesso), HWe SW,Meios físicos, Transmissão, Humanas.
    - Exemplos:
      - Instalação física: má protecção física de equipamentos
      - Hardware e Software: situações não previstas, limites, bugs no projecto
      - Humana: desleixo, preguiça, ganância, revolta, etc.

Ataques

- Técnicas específicas para explorar uma vulnerabilidade.
- Passivos - Muito difíceis de detectar
  - Captura de pacotes, Análise de Tráfego, Monitorização e registo de informação a utilizar mais tarde em ataques.
- Ativos - Ações mais abertas na rede ou sistemas.
  - Worm
  - Vírus

Evolução das necessidades de segurança

	1965 - 1975	1975 - 1989	1990 - 1999	1999 - atual
Plataformas	Utilização de computadores em Time Sharing	Sistemas distribuídos baseados em Redes Locais	Serviços globais Internet	Internet, Dispositivos Móveis, Web Services
Recursos Partilhados	Memória, Ficheiros	Serviços locais (NFS), Redes Locais	Emai, Sites, Comércio eletrónico	Objetos distribuídos, código móvel
Requisitos de Segurança	Identificação e autenticação de utilizadores	Proteção de serviços	Forte segurança para transações comerciais	Controlo de acessos a objetos individuais, código de segurança móvel
Gestão do ambiente de segurança	Única autoridade, Única base de dados de autorização (/etc/passwd)	Única autoridade, Delegação, Bases de dadoa de autorizações replicadas (NIS)	Muitas autoridades. Nenhuma autoridade global da rede	Autoridades por atividades. Grupos com responsabilidades partilhadas

Auditoria Informática

- Da mesma forma que um controlo deve ser feito para evitar o acesso não autorizado a um sistema, deve ser feito também o controlo das ações dos utilizadores autorizados.
- Controlos de auditoria devem permitir a criação de históricos de acessos válidos para, uma eventual verificação de atividades irregulares executadas por utilizadores devidamente autorizados.
- A correta aplicação desses princípios, pode trazer benefícios para a segurança informática:
  - Aumentar a produtividade dos utilizadores através de um ambiente mais organizado
  - Maior controlo sobre os recursos informáticos
  - Garantir a funcionalidade das aplicações críticas da organização.

Auditoria Informática

- Numa operação de auditoria são realizadas as seguintes atividades:
  - Análise de risco
  - Avaliação do desempenho de um sistema
  - Análise de danos causados por um ataque, falha ou simplesmente um desastre

Auditoria Informática - Análise de risco

- A análise de risco consiste num processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no ambiente da organização, possibilitando uma visão do impacto negativo causado à mesma.

- Através da aplicação desse processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela organização (linhas de orientação).

- O processo de análise de risco deve, no mínimo, proporcionar as seguintes informações:
  - Pontos vulneráveis do ambiente
  - Incidentes de segurança causado pela ação de cada ameaça

- Medidas de proteção adequadas para impedir ou diminuir o impacto de cada incidente.

Auditoria Informática - Avaliação do desempenho

- Esta atividade faz parte de uma auditoria para medir a capacidade dos recursos de uma organização e avaliar a capacidade efetiva utilizada.
- Pode, propor mecanismos para otimizar a capacidade para atingir os objetivos que a organização estabeleceu.
- Monitorização e avaliação da implementação de regras e procedimentos.
- Em qualquer organização, deve haver um manual de procedimentos que define a operação do negócio/organização e nesse manual o aspeto da segurança (segurança informática) não deve ser deixado de fora.

Auditoria Informática - Análise de danos causados

- Esta atividade é geralmente realizada após o início de um ataque ou desastre.
- Provavelmente já existe perda de informação dentro de uma organização.
- Pretende avaliar os danos e impactos.
- Propor um plano de recuperação.

Auditoria Informática – A norma TCSEC

- TCSEC – Trusted Computer System Evaluation Criteria (DoD, 85), também conhecido como Orange Book, para a avaliação de segurança de dispositivos de segurança (criptografia, firewalls, etc.).

- Em relação aos programas informáticos, a norma TCSEC define os requisitos de segurança necessários para a garantia da confidencialidade das informações.

- Em 1991, uma comissão europeia conjunta da Alemanha, França, Holanda e Reino Unido publicou uma norma europeia para certificação de segurança intitulada ITSEC (Information Technologie Security Evaluation Criteria), baseada no TCSEC, tornando-se depois um padrão europeu voltado tanto para a avaliação de produtos como de sistemas.

Monitorização

- Os sistemas informáticos têm um papel cada vez mais importante numa instituição. A sua complexidade requer uma monitorização constante de equipamentos, software e comunicações, de forma a garantir um sistema fiável e produtivo.

- Os resultados dessa monitorização são informação imprescindível para qualquer responsável pela administração de sistemas.

- A monitorização de um sistema, pode ser dividida em três grandes áreas:
- Monitorização do sistema
  - Localizado no "centro" do sistema, que irá fornecer informações sobre o uso do CPU, memória.

- Monitorização da rede
  - Consiste em diagnosticar a disponibilidade do equipamento ligado a uma rede. As tecnologias utilizadas para este tipo de supervisão são bastante simples. O nível de informações retornadas é limitado.

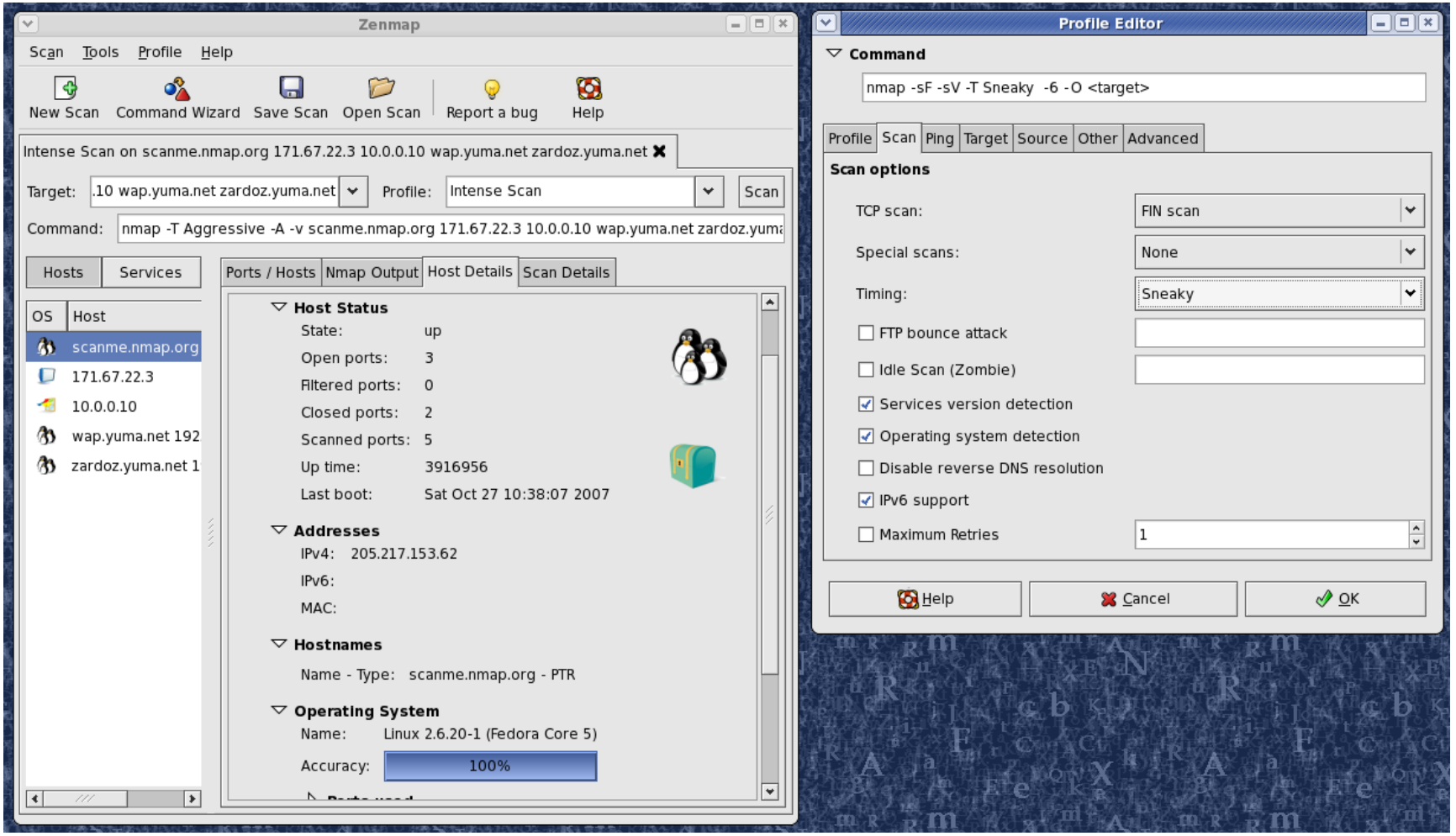
- Monitorização de aplicações
  - Através deste acompanhamento, não teremos em consideração apenas os equipamentos, mas também as aplicações que são executadas e as informações que eles retornam.

Mapeamento de recursos

- Antes dos ataques, há sempre uma atividade prévia de reconhecimento dos serviços estão disponíveis na rede.
- Utilização de ping para determinar os endereços disponíveis na rede.
- Exploração de portos acessíveis (port-scanning): tentativa de estabelecer conexões TCP com séries de portos em sequência para ver quem responde.
- Exploração de recursos na rede.
- Utilização da aplicação nmap
  - Network Exploration and Security Auditing http://nmap.org/

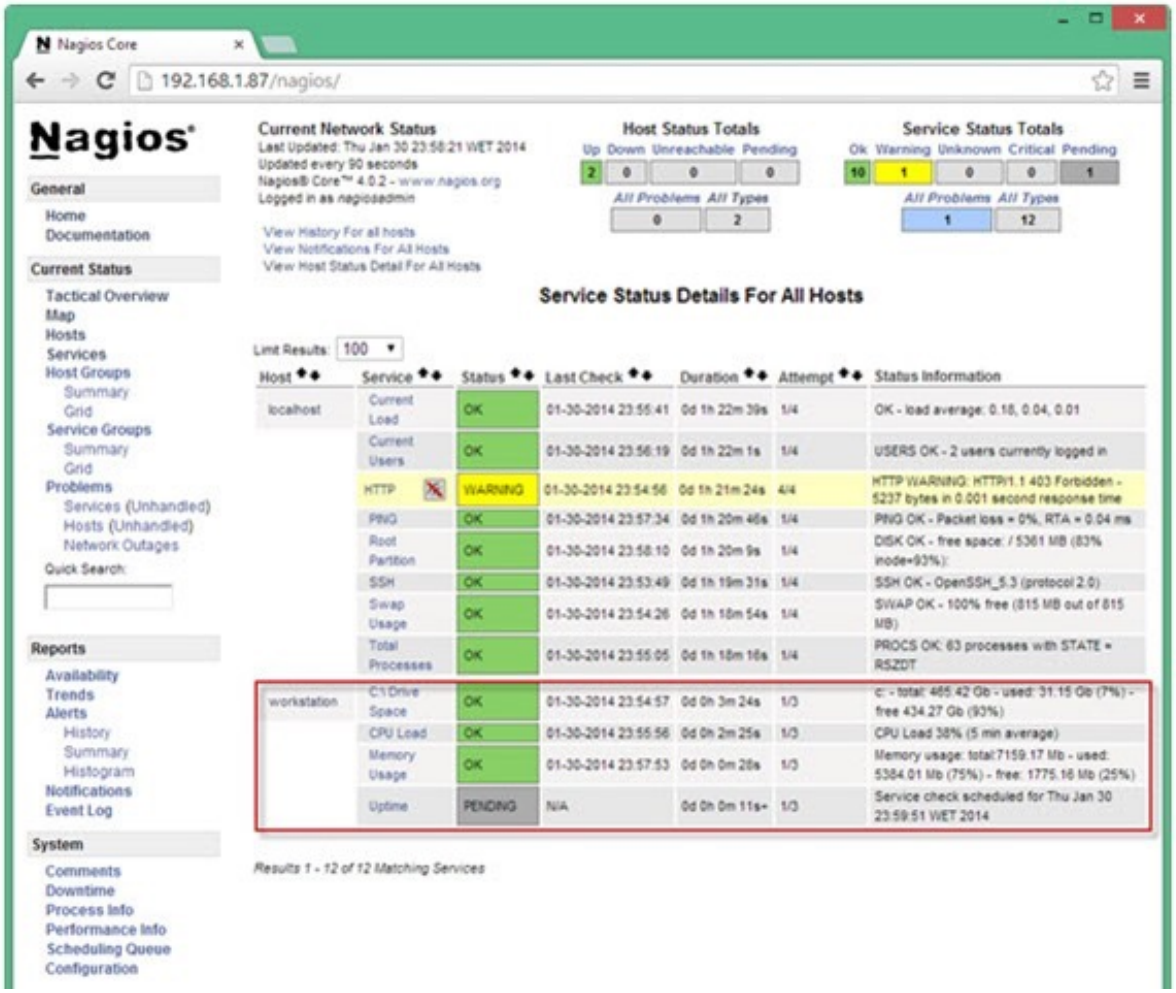
Network Exploration and Security Auditing

NMAP.org



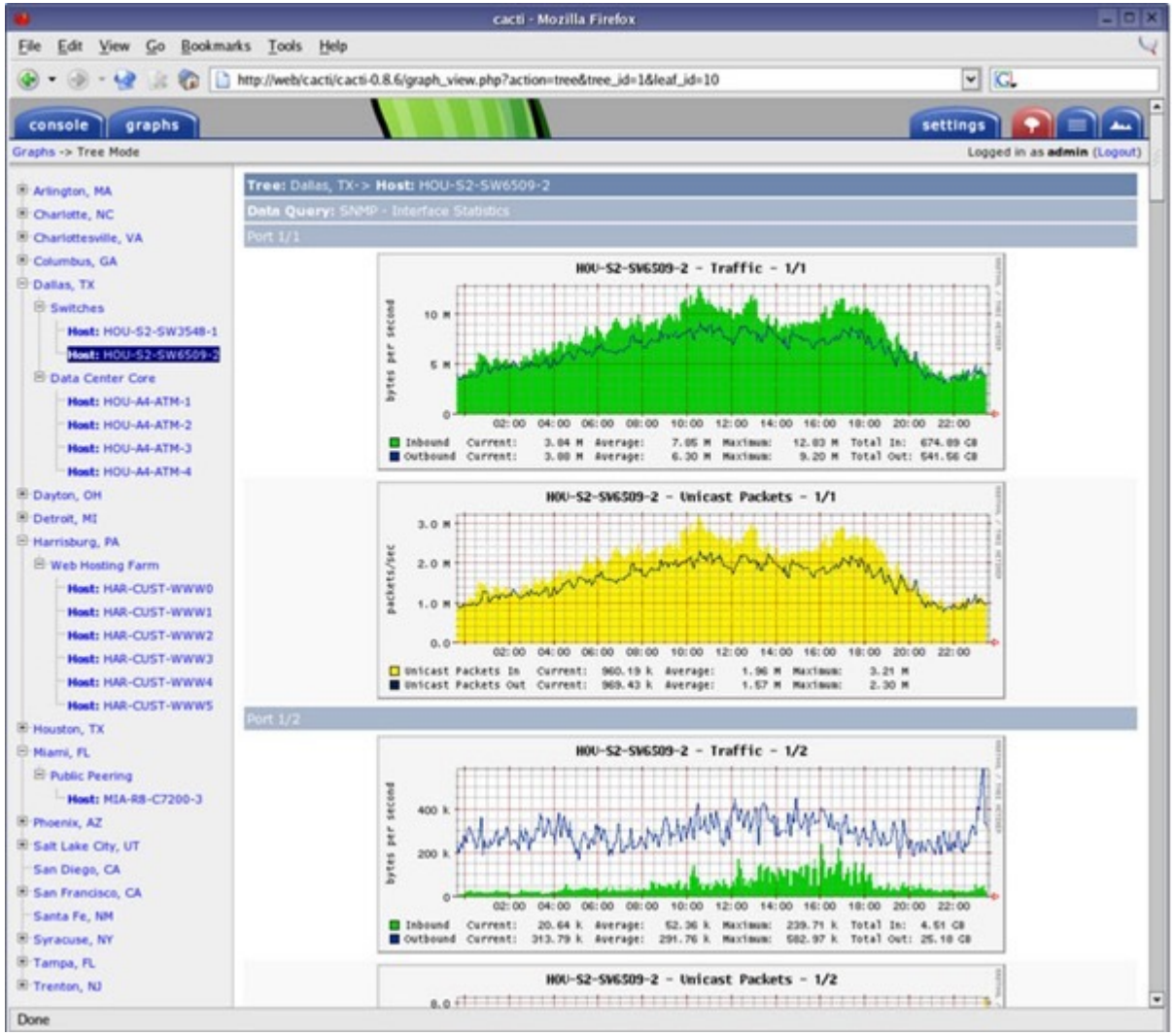
The Nagios IT Management Software Suite

Nagios.com



Cacti the complete rrdtool-based graphing solution

Cacti.net



Mapeamento de Recursos - Precauções

- Registar o tráfego à entrada da rede
- Fechar acessos de portos não utilizados
- Detectar actividade suspeita
  - Endereços IP de origem duvidosa
  - Varrimento sequencial de portos
- Utilizar ferramentas de port-scanning no próprio sistema
  - Técnica comum a hackers para reconhecimento
  - Programa que escuta os números de portas bem conhecidos para detectar informações e serviços em execução no sistema
- Exemplos de portas comuns padrão da Internet:
  - 20 FTP dados (transferência de arquivos)
  - 21 FTP controlo
  - 23 Telnet (terminal)
  - 25 SMTP (envio de e-mail)
  - 80 HTTP (WWW)
  - 110 POP3 (recepção de e-mail)

Ataques - Análise de Pacotes

Ataques:

- Possível em todas as redes com broadcast (LANs).
- Interfaces de rede em modo promíscuo recebem todo o tráfego que passa que pode ser capturado por analisador.
- Podem ler todos os dados não encriptados (usernames, passwords, etc…).

Precauções:

- Instalar software
- Encriptar dados sensíveis na Intranet

Ataques - IP Spoofing

Ataque:

- Podem-se gerar pacotes IP diretamente de uma aplicação, inserindo qualquer valor de IP no campo do endereço de origem.

- O destinatário não pode saber que o IP é forjado.

Precauções:

- Os routers não devem encaminhar pacotes com endereços de origem inválidos, ou seja, cujo endereço não pertença à gama do router.

Ataques - Denial of Service (DoS)

- Ação que interrompe um serviço ou impede totalmente o seu uso por utilizadores legítimos.
- Objetivo principal é indisponibilizar um serviço, apenas para causar o transtorno/prejuízo da interrupção ou para eliminar uma proteção que assim permita atingir outras formas de acesso não autorizado.
- Tipos de ataques DoS:
  - Consumo de banda de rede, sobrecarga.
  - Consumo de recursos de sistema: criar situações de abuso ou sobrecarga que ultrapassem o limite do recurso (buffer, HD...).
  - Atingir falhas que levam à interrupção.
  - Adulteração de DNS: ao invés de desativar um serviço, impede o acesso ao serviço legítimo.

Ataques - Denial of Service (DoS)

Ataque:

- Fluxos de pacotes gerados maliciosamente podem por o servidor em baixo.
- Distributed DOS (DDOS): múltiplos fluxos provenientes de origens coordenadas.
  - Por exemplo, um host remoto lança um ataque.

Precauções:

- Filtrar pacotes antes de atingirem o host.
- Identificar a origem dos ataques, na maior parte dos casos hosts inocentes que foram alvo de ataques e comprometidos.

Ataques – Denial of Service (DoS) - Exemplos

- Ping da Morte (Ping of Death)
  - De aplicação simples, baseado em vulnerabilidade.
  - Vulnerabilidade: sistemas que não tratam adequadamente pacotes ICMP (pacote de controle a nível de IP) maiores do que o normal.
  - Ataque: enviar sequência de ping com campo ICMP de tamanho máximo (maior que o comum).
  - http://www.youtube.com/watch?v=FzuFYdDUjsQ
- Smurf
  - Atacante envia um ECHO_REQUEST ICMP geral fazendo spoof do endereço origem como o endereço IP da máquina alvo = solicita uma resposta (eco) ICMP a todas as máquinas de uma rede, fingindo ser a máquina alvo.
  - Todas as máquinas da rede respondem para a máquina alvo real, sobrecarregando a rede e o sistema alvo.

QUESTÕES

?