Honeypots

Atraindo e Isolando Hackers

Honeypots

- Em vez de tentar bloquear um hacker com um firewall ou encontrar um hacker com um sistema de detecção de intrusão, alguns administradores preferem o método do *honeypot*.

Honeypots

- Normalmente rodam em um único computador.
- Emula a atividade de uma rede, e os detalhes de um sistema operacional, tal como, Linux, Windows, Solaris.
- Ele parece uma rede real.
- Oferece falhas facilmente exploráveis para encorajar hackers a desperdiçarem seu tempo explorando essa rede fictícia.

Honeypots

- Um *honeypot* pode servir para dois propósitos:

  - atrair um hacker para uma área longe dos dados importantes e isolá-los;

  - estudar os métodos e técnicas de um hacker, para se poder defender deles.

Para aprender sobre Honeypots

- Honeynet Project:
  http://project.honeynet.org
- Distributed Honeypot Project:
  http://www.lucid.net
- Lista de Honeypots disponíveis:
  http://www.networkintrusion.co.uk
- Science Applications International Corporation
  http://www.saic.com (wireless honeypot)

Para aprender sobre Honeypots

- Tiny Honeypot
  http://www.alpinista.org/thp
- NetFacade
  http://www22.verizon.com/fns/netsec/fns_netsecurity_netfacade.html
- Symantec ManTrap
  http://www.symantec.com
- The Deception Toolkit
  http://www.all.net/dtk/download.html

Distribuição

- Muitos honeypots são freeware, e incluem o código-fonte para que você possa estudar como eles funcionam e mesmo contribuir com idéias.

Configuração e Experimentação

- Demandam tempo para serem configurados e mantidos.

- Experimentar um honeypot do tipo Cavalo de Tróia: se alguém tentar acessar seu computador com um Cavalo de Tróia de acesso remoto, seu honeypot poderá enganar o hacker, ...

Experimentação

- ... ... fazendo-o pensar que ele tem acesso secreto, quando na verdade, ele está isolado dos seus dados e você está observando suas atividades a cada investida.

Honeypots de Cavalos de Tróia

- NetBuster
  http://surf.to/netbuster
- FakeBO
  http://cvs.linux.hr/fakebo
- Tambu Dummy Server
  http://www.xploiter.com
- The Saint
  http://www.megasecurity.org

Rastreando um Hacker

- Os hackers podem atacar qualquer computador no mundo da Internet.
- Alguém pode estar sondando seu computador e procurando suas vulnerabilidades.
- Pode-se pegar um hacker, mas assim que ele se desconecta ele desaparece do mapa.

Rastreando um Hacker

- Uma vez que os hackers podem aparecer e desaparecer ...
- Para eliminar os refúgios dos hackers no anonimato a Sharp Technology desenvolveu o Hacker Tracer: http://www.sharptechnology.com/bh-cons.htm que pode rastrear o caminho de um hacker ... ...

Rastreando um Hacker

- ... ... de volta ao provedor de acesso Internet dele, e possivelmente descobrir o endereço IP do hacker.
- Saber o endereço IP pode identificar a localização ... ...

Rastreando um Hacker

- ... ... ou pode não lhe dar pista nenhuma sobre onde o hacker está.

- Se seu firewall ou sistema de detecção de intrusão identificar um IP, coloque-o no McAfee Visual Trace que é parte do McAfee Personal Firewall

  http://mcafee.com

Rastreando um Hacker

- ... ... ou o VisualRoute
  http://www.www.visualware.com

  para ver a localização aproximada do hacker em um mapa-múndi.

Rastreando um Hacker

- Para rastrear mais as atividades de hackers visite o site myNetWatchman http://www.mynet-watchman.com e compartilhe as tentativas de ataques ao seu computador com pessoas do mundo todo.

Defendendo-se ... ...

- Com um bom Firewall, um sistema de detecção de intrusão, um sistema operacional com segurança reforçada e até mesmo um honeypot, você pode proteger seu computador e possivelmente virar o jogo para cima do hacker rastreando-o e revelando a localização dele.