Ferramentas Maliciosas

Prof. Alexandre Beletti Ferreira

Keyloggers

- Key = tecla, logger = “gravar”.
- Cria logs com todas as teclas digitadas pelo usuário.
- Monitora todos os procedimentos realizados pelo usuário.
- Senha digitadas em sites, comandos executados em um servidor.

Uso de Keylogger

- Descobrir login e senha
- Descobrir procedimentos “metódicos”
- Monitorar as ações de um usuário para determinar o perfil de conhecimento do mesmo

Demonstração de Keylogger

- Será carregado na memória o keylogger
- Serão realizadas algumas operações no sistema operacional
- Será realizada um consulta no log gerado

Network Scanner

- Utilizado para verificar se determinado endereço ou faixa de endereços está com suas portas abertas.
- Caso esteja, alguns scanners permitem fazer uso de brechas comuns para explorar falhas gerais.

Network Scanner

- Tais scanners mostram também as portas abertas de cada endereço da rede, bem como quais são os possíveis serviços que estão rodando nessas portas
- Exemplo:
  - Host: 192.168.0.3
  - Porta Aberta: 80
  - Serviço Padrão: Servidor HTTP

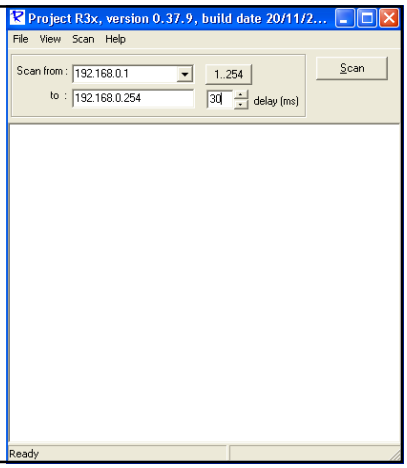
Network Scanner

- Alguns serviços abertos comumente detectados:
- Porta 22: Telnet
- Porta 23: FTP
- Porta 21: Servidor POP
- Porta 110: SMTP
- Porta 443: SSL

7

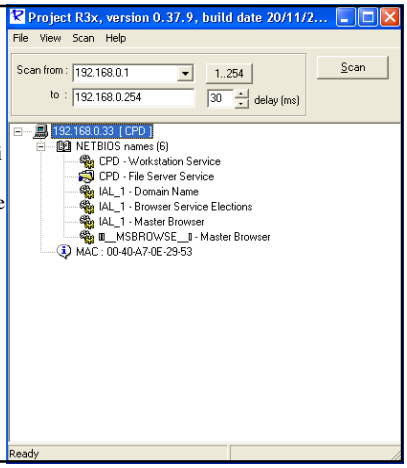
Network Scanner

Exemplo de scanner que tentará localizar “falhas” Em uma rede classe C.
IP inicial: 192.168.0.1
IP final: 192.168.0.254



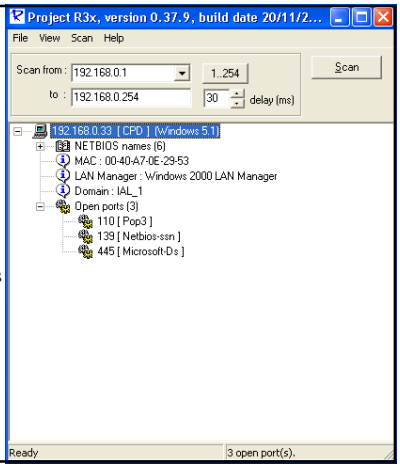
Network Scanner

Apenas uma máquina foi detectada na rede.
Note o MAC da interface bem como outras uma pasta compartilhada de nome CPD.



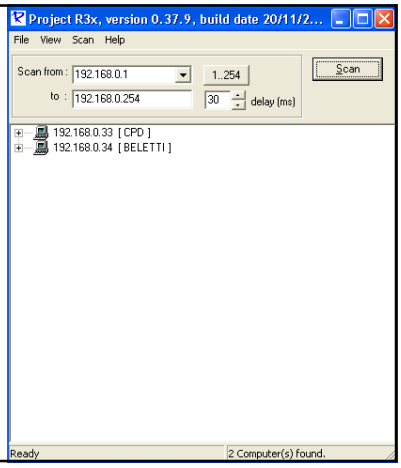
Network Scanner

Pedindo uma intervenção avançada da ferramenta em questão, ela mostra as portas que abertas do host:
110–Envio de Mensagens
139-Netbios
445-Microsoft Ds



Network Scanner

Nesse segundo exemplo, dois hosts foram detectados pela software.



Scanners

- Podem também permitir a quebra de senhas
- Podem utilizar mecanismos de força bruta ou ainda ataque por dicionário

12

Bibliografia

- Softwares de Apoio

13