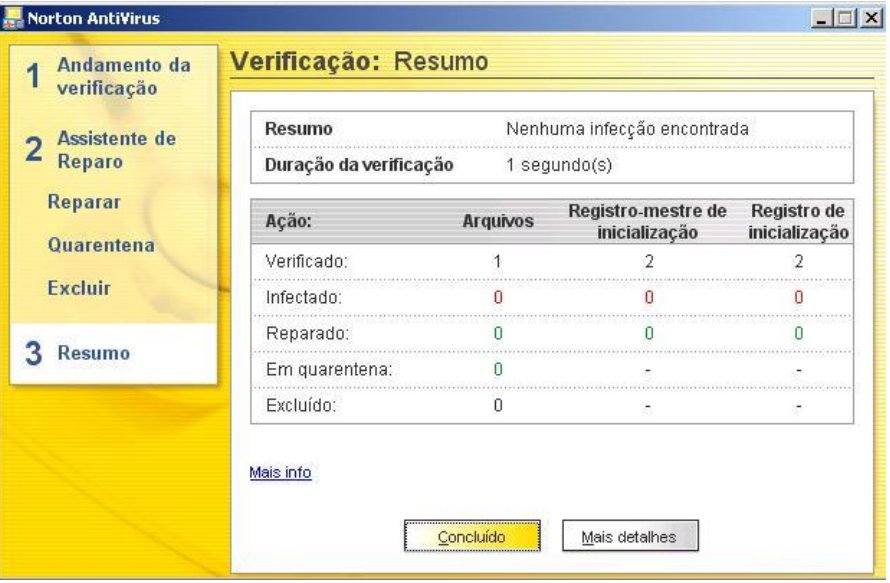
Engenharia Social

Marcos Flávio Araújo Assunção

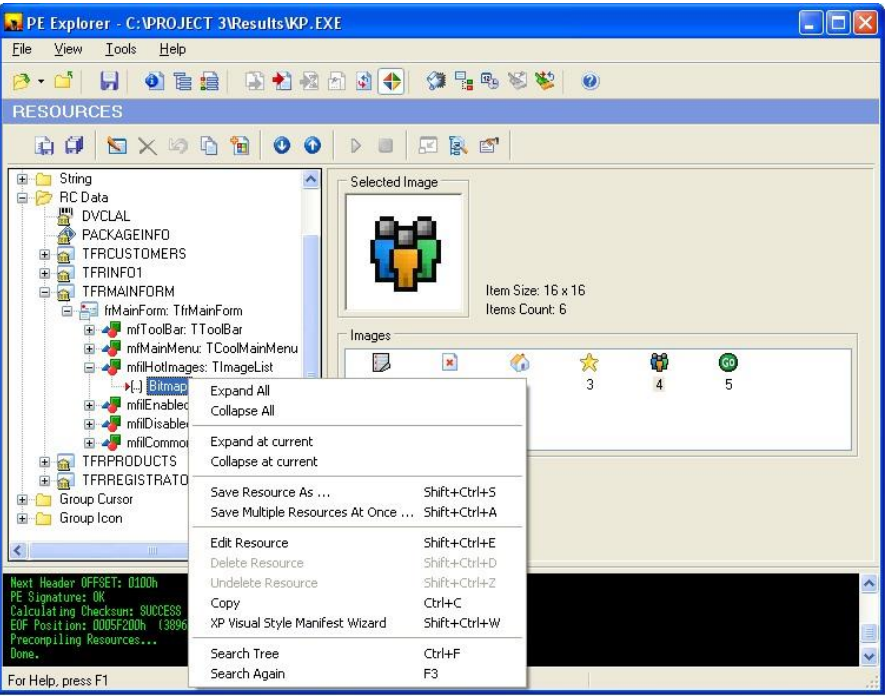
Fundamentos de Ethical Hacking

Ocultamento do Antivirus



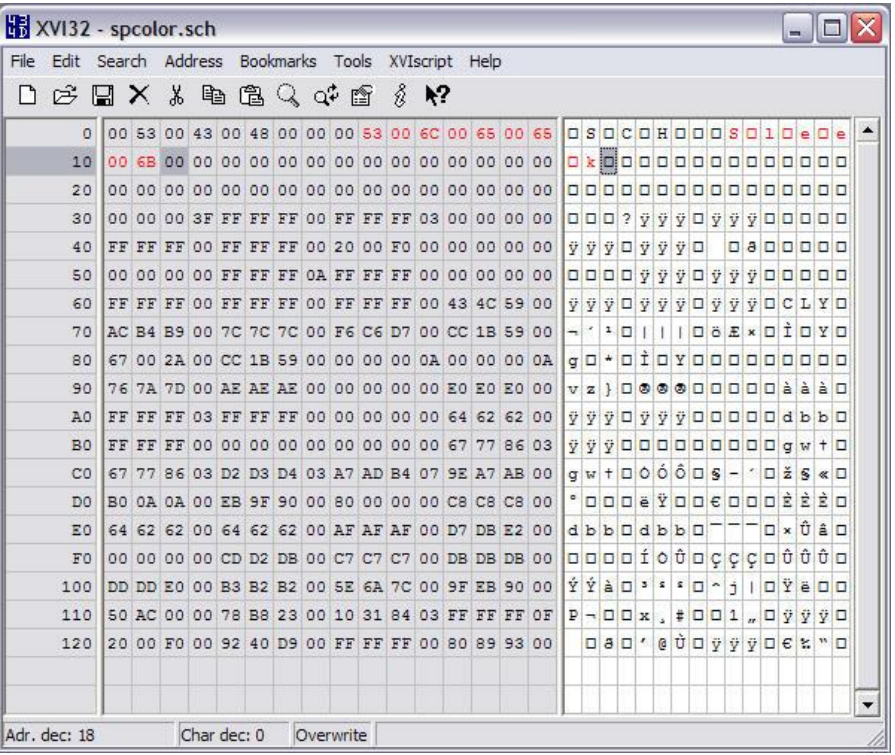
- Assinatura
- Edição de recursos
- Criptografia do executável
- Polimorfismo de código

Edição/remoção de recursos binários



- Permite “mudar” a estrutura binária de um malware, dificultando detecção por AVs

Edição hexadecimal



- Permite “mudar” certas strings em um software, tentando com isto dificultar a detecção por AVs

Veil-Evasion

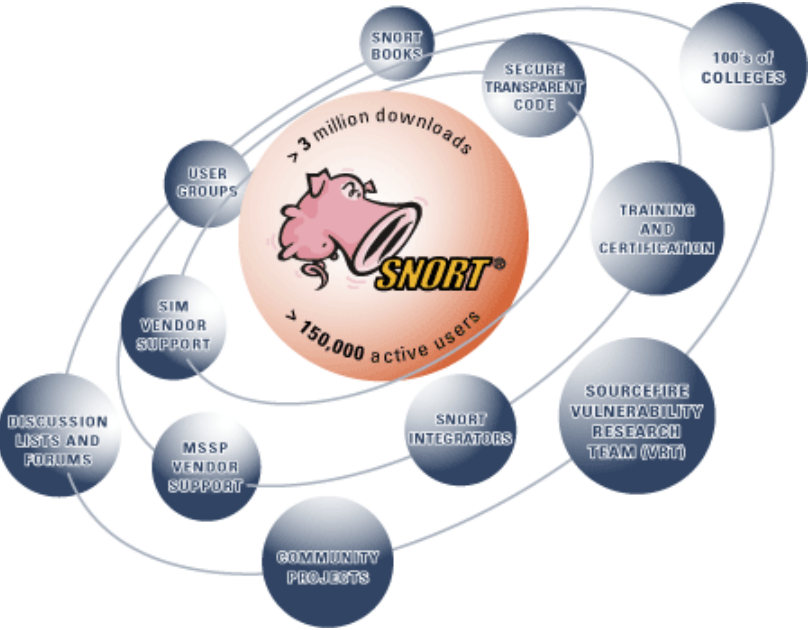
```
root@kali: ~
================================================================================
 Veil-Evasion | [Version]: 2.4.3
================================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 Main Menu

        24 payloads loaded

 Available commands:

        use             use a specific payload
        info            information on a specific payload
        list            list available payloads
        update          update Veil to the latest version
        clean           clean out payload folders
        checkvt         check payload hashes vs. VirusTotal
        exit            exit Veil

 [>] Please enter a command:
```

- Software que permite gerar um payload criptografado em diversos tipos de linguagens e formatos
- Uma das soluções mais utilizadas no ocultamento do AV

Veil-Evasion

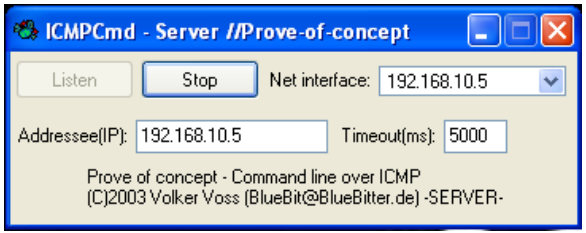
- Proteção “cara-crachá”
- Filtro de pacotes
  - Spoofing
  - Porta de origem
  - Conexão reversa
- Sandbox
  - DLL injection
- Personal Firewall killing (processo)
- Tunneling
  - HTTP (proxy)
  - ICMP (ping)
  - DNS

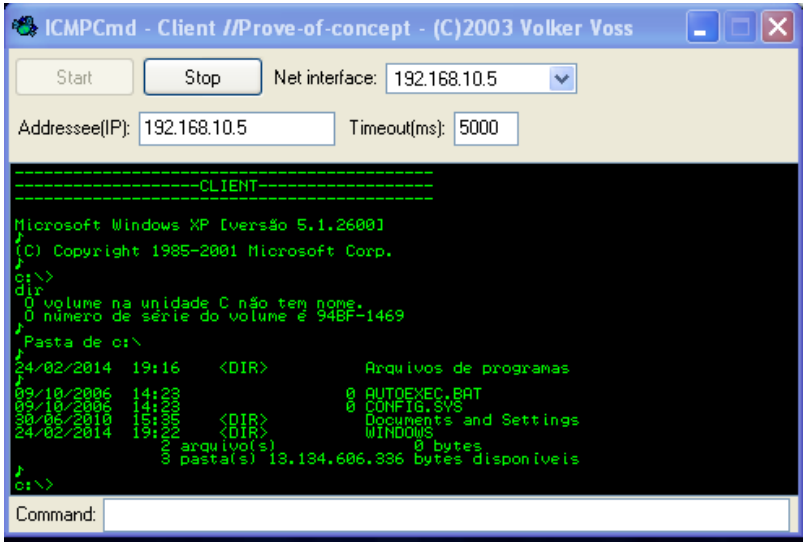
Ocultamento do IDS



- Assinatura
- Comportamento
- Fragmentação
- Tunelamento
- Criptografia

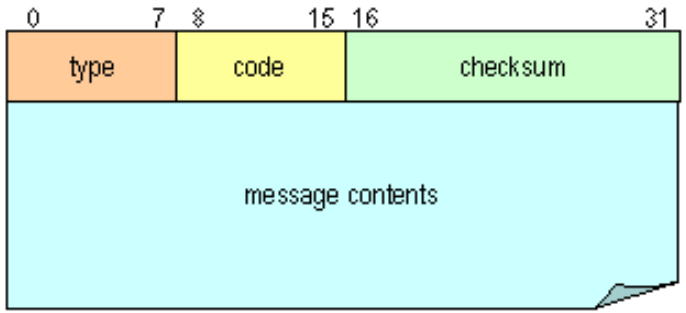
Tunelamento ICMP - ICMPCMD





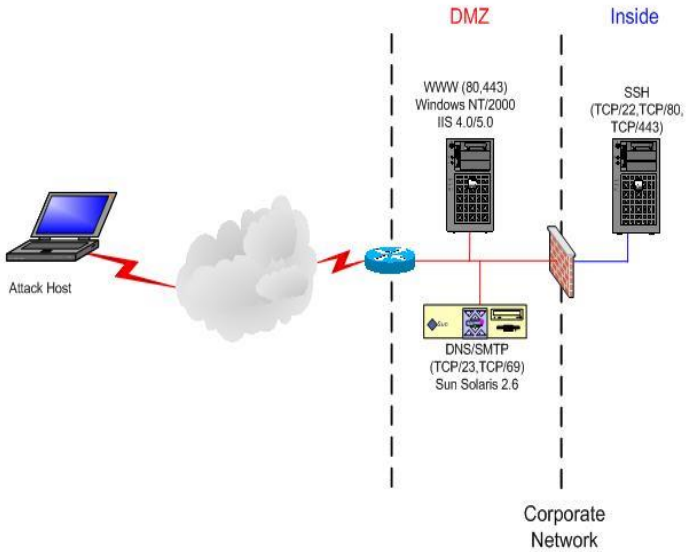
- Exemplo simples de tunelamento
- Usa apenas o “ping” para se comunicar

Tunelamento ICMP - Loki



- Tunelamento ICMP
- ICMP_ECHO
- ICMP_ECHOREPLY
- Loki
- Lokid

Reverse HTTPS Meterpreter payload



- meterpreter/reverse_https
- Tunelamento
- Porta 8443 -> 443
- Com ou sem Proxy (reverse_https_proxy)