Commando VM — альтернатива Kali Linux для Windows

habr.com/ru/articles/446152

Александр

AlexRed 31 мар 2019 в 18:27

3 мин

26K

Информационная безопасность*

Буквально на днях компания FireEye презентовала систему **Commando VM**, предназначенную для пентестеров и Red Team, работающую под управлением операционных систем семейства Microsoft Windows.

FireEye позиционирует Commando VM как «первый в своем роде» дистрибутив для пентестеров под Windows, однако они явно лукавят, т.к. на ум сразу приходит как минимум проект Pentest Box, который также заточен под Windows.

В тоже время, сама система Commando VM довольно интересна и заслуживает внимания…

Краткое описание

Commando VM основана на популярной виртуальной машине Flare VM, которая создана для целей реверс-инжиниринга и анализа вредоносных программ.

По факту, Commando VM является не образом виртуальной машины, а скорее скриптом автоматической установки, который превращает операционную систему Windows, работающую на виртуальной машине, в инструмент для проведения пентестов.

Commando VM использует пакеты Boxstarter, Chocolatey и MyGet для установки всего программного обеспечения и предоставляет множество инструментов и утилит для поддержки проведения пентеста.

Перечень утилит

Active Directory Tools
— Remote Server Administration Tools (RSAT)
— SQL Server Command Line Utilities
— Sysinternals

Command & Control
— Covenant
— PoshC2
— WMImplant
— WMIOps

Developer Tools
— Dep
— Git
— Go
— Java
— Python 2
— Python 3 (default)
— Visual Studio 2017 Build Tools (Windows 10)
— Visual Studio Code

Evasion
— CheckPlease
— Demiguise
— DotNetToJScript
— Invoke-CradleCrafter

— Invoke-DOSfuscation
— Invoke-Obfuscation
— Invoke-Phant0m
— Not PowerShell (nps)
— PS>Attack
— PSAmsi
— Pafishmacro
— PowerLessShell
— PowerShdll
— StarFighters

Exploitation
— ADAPE-Script
— API Monitor
— CrackMapExec
— CrackMapExecWin
— DAMP
— Exchange-AD-Privesc
— FuzzySec's PowerShell-Suite
— FuzzySec's Sharp-Suite
— Generate-Macro
— GhostPack
— Rubeus
— SafetyKatz
— Seatbelt
— SharpDPAPI
— SharpDump
— SharpRoast
— SharpUp
— SharpWMI
— GoFetch
— Impacket
— Invoke-ACLPwn
— Invoke-DCOM
— Invoke-PSImage
— Invoke-PowerThIEf
— Kali Binaries for Windows
— LuckyStrike
— MetaTwin
— Metasploit
— Mr. Unikod3r's RedTeamPowershellScripts
— NetshHelperBeacon
— Nishang
— Orca
— PSReflect

— PowerLurk
— PowerPriv
— PowerSploit
— PowerUpSQL
— PrivExchange
— Ruler
— SharpExchangePriv
— SpoolSample
— UACME
— impacket-examples-windows
— vssown

Information Gathering
— ADACLScanner
— ADExplorer
— ADOffline
— ADRecon
— BloodHound
— Get-ReconInfo
— GoWitness
— Nmap
— PowerView
— Dev branch included
— SharpHound
— SharpView
— SpoolerScanner

Networking Tools
— Citrix Receiver
— OpenVPN
— Proxycap
— PuTTY
— Telnet
— VMWare Horizon Client
— VMWare vSphere Client
— VNC-Viewer
— WinSCP
— Windump
— Wireshark

Password Attacks
— ASREPRoast
— CredNinja
— DSInternals
— Get-LAPSPasswords

— Hashcat
— Internal-Monologue
— Inveigh
— Invoke-TheHash
— KeeFarce
— KeeThief
— LAPSToolkit
— MailSniper
— Mimikatz
— Mimikittenz
— RiskySPN
— SessionGopher

Reverse Engineering
— DNSpy
— Flare-Floss
— ILSpy
— PEview
— Windbg
— x64dbg

Utilities
— 7zip
— Adobe Reader
— AutoIT
— Cmder
— CyberChef
— Gimp
— Greenshot
— Hashcheck
— Hexchat
— HxD
— Keepass
— MobaXterm
— Mozilla Thunderbird
— Neo4j Community Edition
— Pidgin
— Process Hacker 2
— SQLite DB Browser
— Screentogif
— Shellcode Launcher
— Sublime Text 3
— TortoiseSVN

— VLC Media Player
— Winrar
— yEd Graph Tool

Vulnerability Analysis
— Egress-Assess
— Grouper2
— zBang

Web Applications
— Burp Suite
— Fiddler
— Firefox
— OWASP Zap

Wordlists
— FuzzDB
— PayloadsAllTheThings
— SecLists

Установка

Разработчики советуют использовать Commando VM только в качестве виртуальной машины!

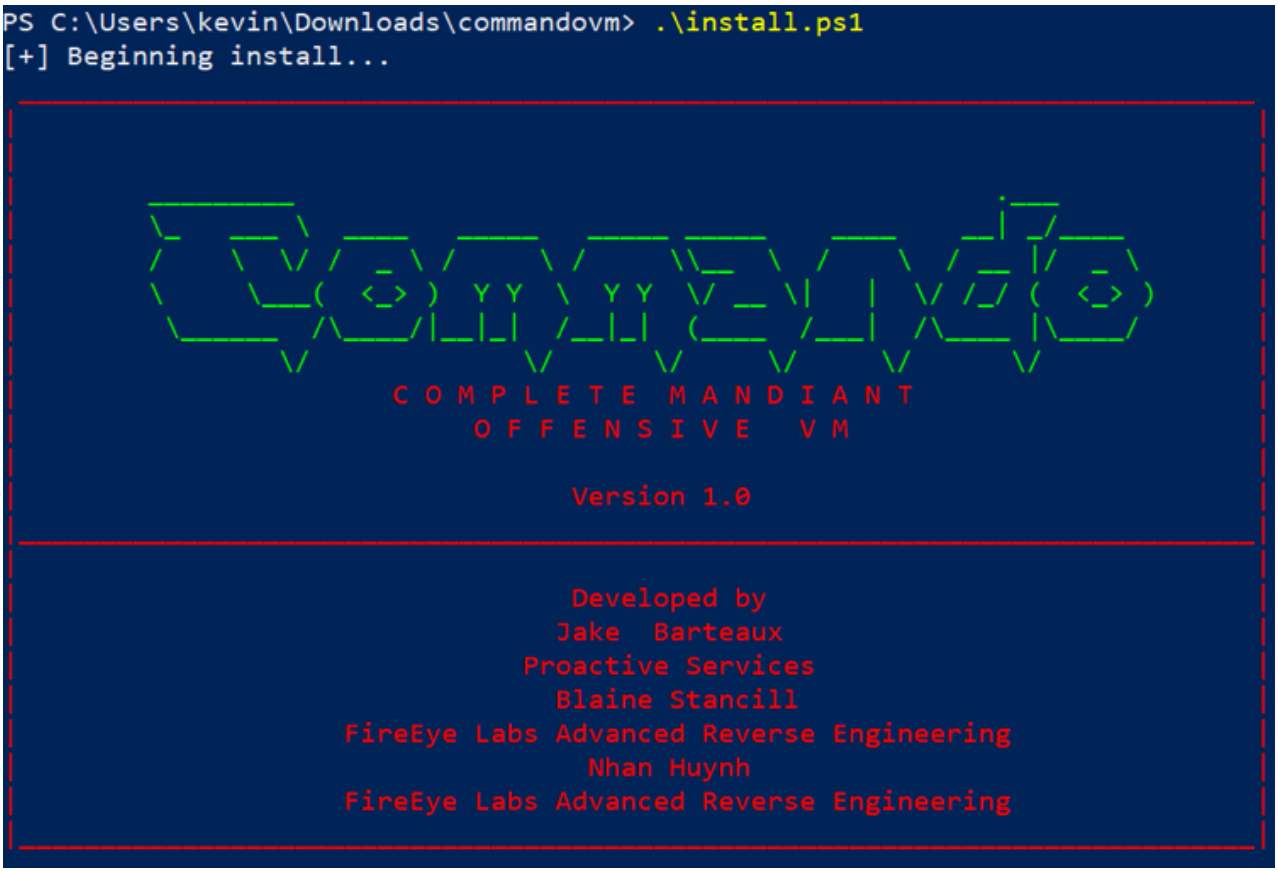
Требования по железу:
— 60 Гб свободного места на диске.
— 2 Гб оперативной памяти.

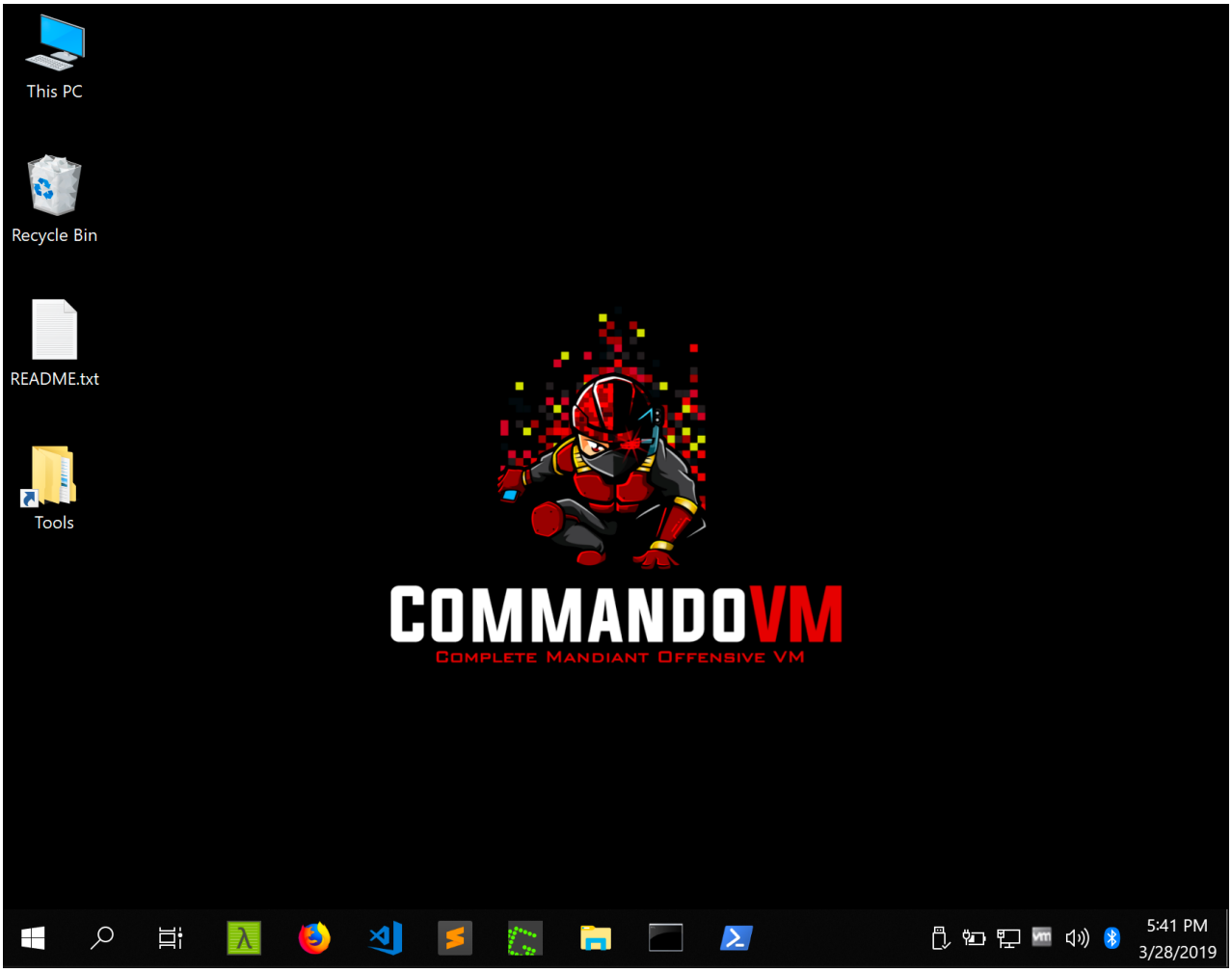
Требования по ОС:
— Windows 7 SP1
— Windows 10 (приоритетнее)

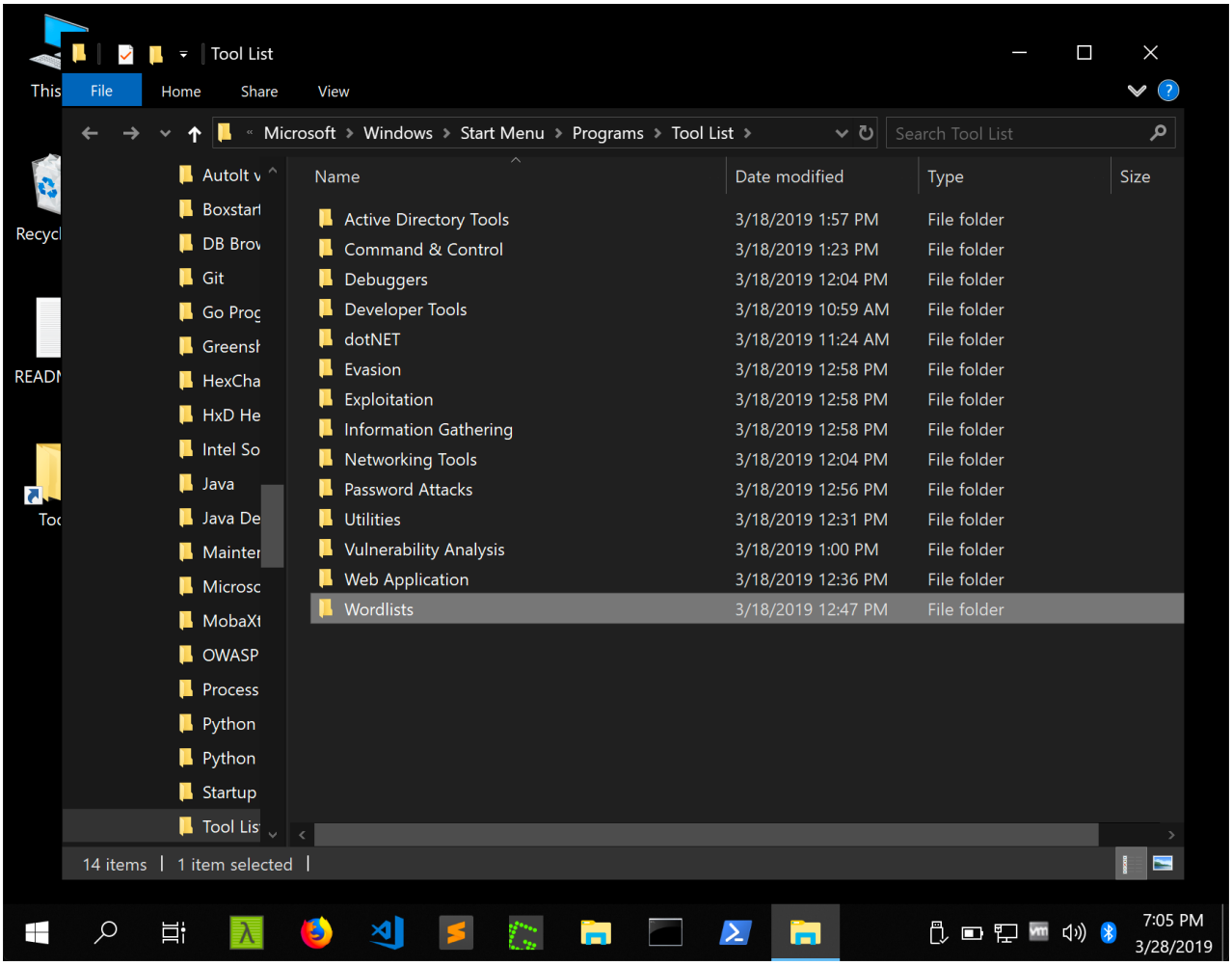
Установка производится путем запуска скрипта установки в PowerShell, скачать который можно из репозитория Commando VM

Видеогайд установки

Скриншоты


PS C:\Users\kevin\Downloads\commandovm> .\install.ps1
[+] Beginning install...
COMPLETE MANDIANT
OFFENSIVE VM
Version 1.0
Developed by
Jake Barteaux
Proactive Services
Blaine Stancill
FireEye Labs Advanced Reverse Engineering
Nhan Huynh
FireEye Labs Advanced Reverse Engineering


This PC
Recycle Bin
README.txt
Tools
COMMANDOVM
COMPLETE MANDIANT OFFENSIVE VM
5:41 PM
3/28/2019


Tool List
File
Home
Share
View
Microsoft › Windows › Start Menu › Programs › Tool List ›
Search Tool List
Name
Date modified
Type
Size
Active Directory Tools 3/18/2019 1:57 PM File folder
Command & Control 3/18/2019 1:23 PM File folder
Debuggers 3/18/2019 12:04 PM File folder
Developer Tools 3/18/2019 10:59 AM File folder
dotNET 3/18/2019 11:24 AM File folder
Evasion 3/18/2019 12:58 PM File folder
Exploitation 3/18/2019 12:58 PM File folder
Information Gathering 3/18/2019 12:58 PM File folder
Networking Tools 3/18/2019 12:04 PM File folder
Password Attacks 3/18/2019 12:56 PM File folder
Utilities 3/18/2019 12:31 PM File folder
Vulnerability Analysis 3/18/2019 1:00 PM File folder
Web Application 3/18/2019 12:36 PM File folder
Wordlists 3/18/2019 12:47 PM File folder
14 items | 1 item selected |
7:05 PM
3/28/2019