Network Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

Pentester Academy: http://www.PentesterAcademy.com

©SecurityTube.net

Pentesting Windows Endpoints: AV Evasion using Python

©SecurityTube.net

AV Bypass

- No Silver Bullet
- Need to improvise methods always
- Custom techniques / code more difficult to beat

©SecurityTube.net

Python to EXE

- Pyinstaller

http://www.pyinstaller.org/

©SecurityTube.net

Python Script to Launch Shellcode

- Pyinstaller Win32 Shellcode Runner

http://pastebin.com/rrhcGeHh

©SecurityTube.net

Convert to EXE

```
c:\code samples\pyinstaller-2.0\pyinstaller-2.0>pyinstaller.py -w -a -F ..\..\av
-evasion.py
39 INFO: wrote c:\code samples\pyinstaller-2.0\pyinstaller-2.0\av-evasion.spec
59 INFO: Testing for ability to set icons, version resources...
59 INFO: ... resource update available
69 INFO: UPX is not available.
1276 INFO: checking Analysis
1276 INFO: building Analysis because out00-Analysis.toc non existent
1276 INFO: running Analysis out00-Analysis.toc
1276 INFO: Adding Microsoft.VC90.CRT to dependent assemblies of final executable

1424 INFO: Searching for assembly x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.21
022.8_none ...
1424 INFO: Found manifest C:\Windows\WinSxS\Manifests\x86_microsoft.vc90.crt_1fc
8b3b9a1e18e3b_9.0.21022.8_none_bcb86ed6ac711f91.manifest
1424 INFO: Searching for file msvcr90.dll
1424 INFO: Found file C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_
9.0.21022.8_none_bcb86ed6ac711f91\msvcr90.dll
1424 INFO: Searching for file msvcp90.dll
1424 INFO: Found file C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_
9.0.21022.8_none_bcb86ed6ac711f91\msvcp90.dll
1424 INFO: Searching for file msvcm90.dll
1424 INFO: Found file C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_
9.0.21022.8_none_bcb86ed6ac711f91\msvcm90.dll
1551 INFO: Analyzing C:\code samples\pyinstaller-2.0\pyinstaller-2.0\support\_py
i_bootstrap.py
2808 INFO: Analyzing C:\code samples\pyinstaller-2.0\pyinstaller-2.0\PyInstaller
\loader\archive.py
2955 INFO: Analyzing C:\code samples\pyinstaller-2.0\pyinstaller-2.0\PyInstaller
\loader\carchive.py
3111 INFO: Analyzing C:\code samples\pyinstaller-2.0\pyinstaller-2.0\PyInstaller
\loader\iu.py
3161 INFO: Analyzing ..\..\av-evasion.py
3308 INFO: Looking for run-time hooks
3308 INFO: Analyzing rthook C:\code samples\pyinstaller-2.0\pyinstaller-2.0\supp
ort/rthooks/pyi_rth_encodings.py
3653 INFO: Warnings written to c:\code samples\pyinstaller-2.0\pyinstaller-2.0\b
uild\pyi.win32\av-evasion\warnav-evasion.txt
3663 INFO: checking PYZ
3663 INFO: rebuilding out00-PYZ.toc because out00-PYZ.pyz is missing
3663 INFO: building PYZ out00-PYZ.toc
4657 INFO: checking PKG
4667 INFO: rebuilding out00-PKG.toc because out00-PKG.pkg is missing
4667 INFO: building PKG out00-PKG.pkg
6222 INFO: checking EXE
6222 INFO: rebuilding out00-EXE.toc because av-evasion.exe missing
6222 INFO: building EXE from out00-EXE.toc
6222 INFO: Appending archive to EXE c:\code samples\pyinstaller-2.0\pyinstaller-
2.0\dist\av-evasion.exe

c:\code samples\pyinstaller-2.0\pyinstaller-2.0>_
```

©SecurityTube.net

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

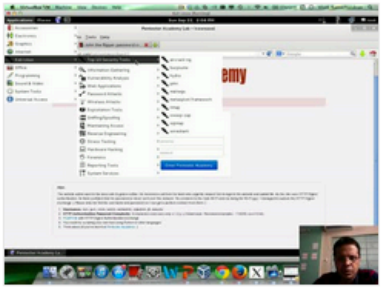
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

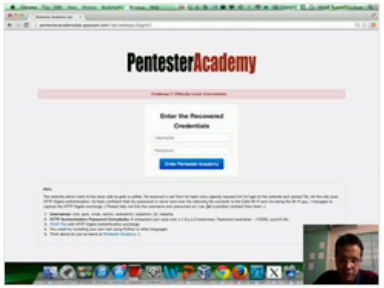
Start Learning Today!

Latest Videos

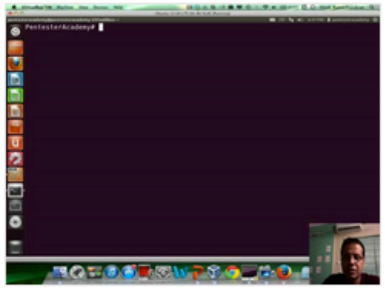
New content added weekly!



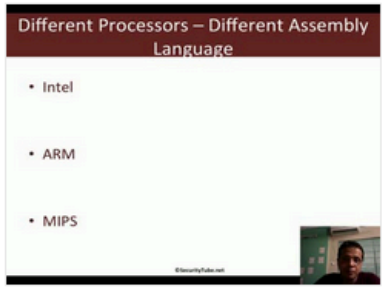
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux

©SecurityTube.net