SecurityTube Linux Assembly Expert (SLAE^{64})

SecurityTube Linux Assembly Expert

Training: http://www.SecurityTube-Training.com

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

Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{32,64} Course Instructor

Module 2: Introduction to Shellcoding

21. Polymorphism

Vivek Ramachandran
SWSE, SMFE, SPSE, SGDE, SISE, SLAE^{32} Course Instructor

http://SecurityTube-Training.com

Easy Fingerprinting of Basic Shellcode

- AV and IDS can use the shellcode as a pattern to search
- Easy to fingerprint
- Detection simple

Encoding and Encryption

- Original shellcode protected
- Decoder / Decryptor Stub however small, is prone to fingerprinting
- Back to square 1 ☺

Imagine IF

- We could make our shellcode look different every time we create it
- Functionality remains the same
- Semantically equivalent instructions

Detection is now MUCH, MUCH Difficult

Enter Polymorphism

Origins in the Virus World

```
----[ 3.1 - Back in 1992...

In 1992, Dark Avenger invented a revolutionary technique he called
polymorphism. What is it ? It simply consist of ciphering the code of the
virus and generate a decipher routine which is different at each time, so
that the whole virus is different at each time and can't be scanned !

Very good polymorphic engines have appeared : the TridenT Polymorphic
Engine (TPE), Dark Angel Mutation Engine (DAME).

As a consequence, antivirus makers developped new heuristic techniques
such as spectrum analysis, code emulators, ...
```

Source: http://www.phrack.org/issues.html?issue=61&id=9#article

Basic Principle of Create Polymorphic Shellcode

- Replace instructions with equivalent functionality ones
- Add garbage instructions which don't change functionality in any way "NOP Equivalents"

Polymorphic Engines

- ADMutate:
  - http://www.ktwo.ca/readme.html
  - http://www.youtube.com/watch?v=XMt9ExL9I00
- CLET
  - http://www.phrack.org/issues.html?issue=61&id=9#article
- VX Heavens Mirror
  - http://download.adamas.ai/dlbase/Stuff/VX%20Heavens%20Library/static/vdat/mainmenu.htm

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

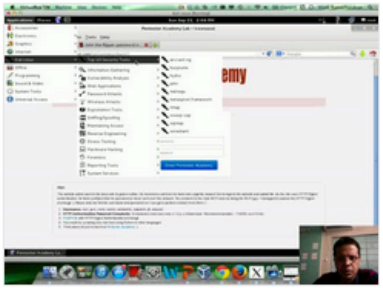
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

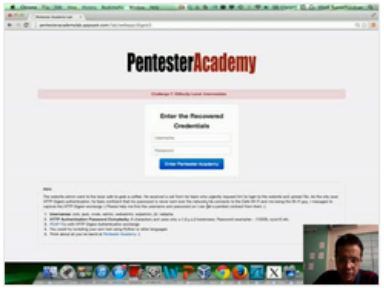
Start Learning Today!

Latest Videos

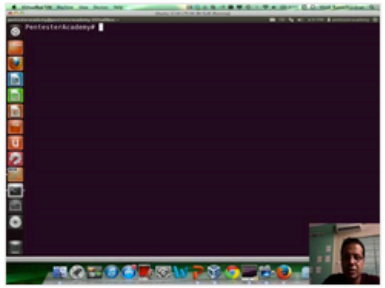
New content added weekly!



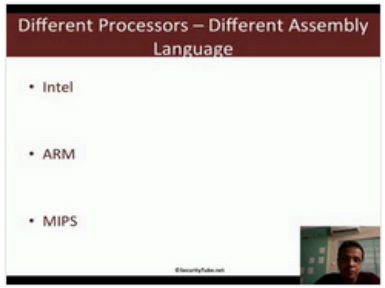
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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