OVERVIEW OF EMET

Agenda

- Previous cycles:
  - Stack-based buffer overflow
  - DEP and ASLR mitigations
  - ROP
  - Stack Canaries
- This cycle:
  - Enhanced Mitigation Experience Toolkit
  - Demonstration

EMET

- Goal: Raise the bar for the attacker!

- Microsoft EMET User Guide:

  “The Enhanced Mitigation Experience Toolkit (EMET) is designed to help prevent attackers from gaining access to computer systems. EMET anticipates the most common techniques attackers might use to exploit vulnerabilities in computer systems, and helps protect by diverting, terminating, blocking, and invalidating those actions and techniques.”

EMET

- Version 4
  - DeMott and others bypassed version 4
- Version 5.2
  - New techniques to disable EMET 5.2 found
- Latest version is 5.5
  - Requires Microsoft .NET Framework 4
  - Released in February 2016
- Easy to install, but lots of configuration options

EMET Mitigations

- DEP
  - Enables DEP, even if it wasn't compiled in
- ASLR
  - Forces randomized addresses, even if it wasn't compiled in
- ROP
  - Several experimental anti-ROP techniques, such as Caller Checks and Stack Pivot Detection
- And Much More! Read the User Guide for details!!

Tool Demonstration

Summary

3 Main Ideas

- EMET makes exploitation more difficult by implementing several mitigations that add additional obstacles for an exploit writer to overcome. EMET raises the bar for the attacker to be successful.
- Weaknesses have been found in previous versions of EMET. The latest version of EMET is version 5.5, which was released in February 2016.
- EMET provides protections such as DEP, ASLR, ROP detection, and many other techniques.
- During DakotaCon, speakers frequently mentioned that enabling EMET is the best way to detect and prevent the red team attacks.

Future Work

- Linux mitigation grsecurity
- Additional attacks and mitigations that EMET addresses:
  - Structured Exception Handling (SEH) attacks
  - Export Address Table (EAT) attacks
  - Heap Sprays
  - Stack Pivoting
  - Certificate Pinning
  - Untrusted Fonts

References

- Alsaheel, A. & Pande, R. (2016, February 23). Using EMET to Disable EMET. Fireeye. Retrieved from https://www.fireeye.com/blog/threat-research/2016/02/using_emet_to_disabl.html.
- DeMott, J. (2014, February 24). Bypassing EMET 4.1. Bromium Labs. Retrieved from https://labs.bromium.com/2014/02/24/bypassing-emet-4-1/.
- Microsoft. (2016). The Enhanced Mitigation Experience Toolkit. Retrieved from https://support.microsoft.com/en-us/kb/2458544.
- Microsoft. (2016). Enhanced Mitigation Experience Toolkit. TechNet. Retrieved from https://technet.microsoft.com/en-us/security/jj653751.

Post Questions and Comments to the Discussion Board