Many people give much more attention to **0-Day** vulnerabilities, but what they did not know is that security solution vendors have a short time response to deliver a protection to these **0-Day** attacks – within hours or within couple days. As soon as a **0-Day** reaches the Internet, as soon as some security solution vendors have coverage to protect systems, and people no longer need this patch... And as soon as a **0-Day** reaches the Internet and security solution vendors cover it, as soon as people do not patch the vulnerability trusting this security model. There are other groups of people that do not even know about the **0-Day** vulnerability or, sometimes, do not even care about it. And, sometimes, people just cannot deploy the patch on a legacy environment! That said we can conclude that **0-Day** only has the value of being ***UNKNOWN***, right? But: "*what if a **KNOWN** vulnerability, which is not detectable by security solutions, could be possible?*"

Another aspect is that since the early ages of security, security solutions use a so claimed technology: **Pattern Matching**. **Pattern Matching** technology is as need today as it was in the past, but the security solution cannot be based only on this. To address this well-known "weakness" the **Exploit Next Generation® Methodology** was first designed in 2004, applied in 2005, published in 2008, and became a methodology in 2009. Its main goal is showing everyone that: "*a single vulnerability does not mean a single way to exploit this vulnerability*".

While some excellent researches have been done addressing OS based protection (such as: **Data Execution Prevention** and **Address Space Layout Randomization**), the **Exploit Next Generation® Methodology** (***ENG***$^{++}$) addresses the security designed solutions, and gets a powerful approach when combined with other techniques. ***ENG***$^{++}$ (pronounced /ĕn'jĭn/ incremented) is a methodology intended to change the behavior of exploit developers, and it provides a specific set of procedures for offering set based mutation of key aspects of an exploit to prevent simple **Pattern Matching** and ineffective **Stateful Packet Inspection** or **Deep Packet Inspection** by **Intrusion Detection System** (***IDS***) and **Intrusion Prevention System** (***IPS***) solutions.

ENG^{++} works by deep analysis of a vulnerability and using all the acquired knowledge of this analysis to offer a variety of decision points targeting the actual triggering of the vulnerability (i.e., brand-new variants), rather than the shellcode that executes after the vulnerability. For ***ENG***$^{++}$ to be effective, it requires exploit developers to determine additional paths to execution beyond those that are available in a standard PoC or even in a standard Automated Penetration Testing Tool's exploitation module.

For ***ENG***$^{++}$ to be effectively stopped, it requires that **IDS** and **IPS** vendors understand the traits of the vulnerability equally well, and can detect multiple paths of execution. In essence, it shows the frailty of signature based **IDS** and **IPS** solutions. If they are simply **Pattern Matching**, they will not match the pattern after mutation. If they are skipping paths to execution, their sigs will fail on the mutations. Only **IDS** and **IPS** solutions that are robust will catch all of the permutations. That is the very first definition of "**Z-Day Attacks**" concept: "*any new attack exploitation variant, which cannot be detected by regular **IDS** and **IPS** solutions*".

Basically:

- ***ENG***$^{++}$ uses randomness to provide unpredictable payloads and unpredictable vulnerabilities' triggers.
- ***ENG***$^{++}$ requires deeper vulnerability knowledge, from the developers' perspective, in the exploit creation process.
- ***ENG***$^{++}$ helps creating new exploit variants, maintaining the reliability, and can be applied to: Penetration Testing; Exploit Development; ***IDS*** and ***IPS*** Evasion Testing; ***IDS*** and ***IPS*** Quality Assurance; etc...
- ***ENG***$^{++}$ helps proofing whether an ***IDS*** and ***IPS*** solution is susceptible to evasion or not.
- ***ENG***$^{++}$ can be applied with/to any exploit development framework, such as: **Metasploit Framework**; **CORE Impact Pro**; **Immunity CANVAS Professional**; or any other Automated Penetration Testing Tool.
- ***ENG***$^{++}$ Methodology applied results in brad-new attack variants, such as: **MS02-039**; **MS02-056**; **MS08-078**; and **MS09-002**.

There are no similarities between **Exploit Next Generation®** (***ENG***$^{++}$) and **Advanced Evasion Techniques** (***AET***), let me get this clear:

- ***ENG***$^{++}$ has a totally different approach and has no similarity, despite the fact that both of them can be used to bypass ***IDS*** and ***IPS*** technology, with ***AET***.
- ***ENG***$^{++}$ is much broader than ***AET*** and, basically, it does not lie on building a custom TCP/IP stack, being much easier to be applied to usual threats by attackers.
- ***ENG***$^{++}$ is definitely a computer's ecosystem independent methodology, and can be applied, virtually, to almost all both old vulnerabilities and new vulnerabilities.

In a few words: **Exploit Next Generation® Methodology** is not the same thing as **Advanced Evasion Techniques** (***ENG***$^{++}$ ***!= AET***).