**Analisis Common Vulnerabilities and Exposures (CVE) dari FreeBSD**

**(Tugas Mata Kuliah Keamanan Jaringan Komputer)**

****

**Nama: Azwar Hidayat**

**NIM: 09011281520126**

**Jurusan Sistem Komputer**

**Fakultas lmu Komputer**

**Universitas Sriwijaya**

**2018**

Langkah 1 : mengecek versi FreeBSD terbaru



Langkah 2 : Cek CVE pada web : <https://cve.mitre.org/cve/search_cve_list.html>



CVE pada web : <https://www.cvedetails.com/vulnerability-list/vendor_id-6/product_id-7/version_id-225726/Freebsd-Freebsd-11.1.html>



Langkah 3 : Analisis CVE sebagai celah untuk melakukan serangan



Langkah 4 : Temukan cara attack dari vulnerabillity tersebut (Source : <https://www.secureworks.com/blog/attacking-windows-smb-zero-day-vulnerability>)

Attack Scenario :

1. The attacker runs the PoC on a system they control (see Figure 1). The attacker-controlled system in this example is running the PoC (Win10.py) and listening on TCP port 445.



Figure 1. Running the SMB zero-day exploit on an attacker-controlled system. (Source: SecureWorks)

1. The attacker sets up and runs a web server on another system.
2. The attacker places the "redirect-smb.php" PHP file listed in Figure 2 in the public directory. This PHP file uses the Redirect to SMB attack.



Figure 2. PHP file placed in web server's public directory. (Source: SecureWorks)

1. Using Internet Explorer on a victim's Windows 10 system to access the attacker's web server, the victim clicks the link corresponding to the "redirect-smb.php" file (see Figure 3).



Figure 3. Victim clicks link to malicious PHP file. (Source: SecureWorks)

1. Clicking this link redirects the victim's system to the attacker's SMB server and initiates the DoS attack (see Figure 4).



Figure 4. Sending the SMB DoS exploit to the victim's system. (Source: SecureWorks)

1. A few seconds later, the victim's Windows 10 system crashes, displaying a Blue Screen of Death (BSOD) (see Figure 5), and is automatically restarted.



Figure 5. BSOD displayed on victim's system after exploiting the SMB DoS vulnerability. (Source: SecureWorks)