Exploit

Exploit je nástroj nebo technika, kterou útočníci používají k zneužití konkrétní bezpečnostní trhliny (vulnerability). Zatímco zranitelnost je „díra v plotě“, exploit je konkrétní způsob, jak touto dírou prolézt nebo ji zvětšit. Exploity jsou klíčovou součástí malwaru a arzenálu etických i neetických hackerů.

Klasifikace exploitů

Exploity lze dělit podle několika kritérií, nejčastěji podle způsobu útoku a doby existence zranitelnosti:

1. Podle místa útoku

- **Remote Exploit (Vzdálený):** Útočí na systém přes síť (internet). Je nejnebezpečnější, protože nevyžaduje předchozí přístup k cílovému stroji.
- **Local Exploit (Lokální):** Vyžaduje, aby měl útočník již do systému přístup (např. jako běžný uživatel). Cílem je obvykle získat práva administrátora (Root/System).
- **Client-side Exploit:** Útočí na aplikace v počítači uživatele (např. prohlížeč, PDF prohlížeč). K útoku dojde, když uživatel otevře infikovanou stránku nebo soubor.

2. Podle stáří zranitelnosti

- **Zero-day Exploit:** Útok, který využívá chybu, o které vývojáři softwaru zatím nevědí a neexistuje na ni oprava. Jedná se o nejcennější a nejnebezpečnější typ exploitu.
- **Known Exploit (Známý):** Využívá chybu, která je již veřejně známá a na kterou pravděpodobně existuje záplata (patch). Úspěšnost závisí na tom, zda uživatelé systém pravidelně aktualizují.

Anatomie útoku pomocí exploitu

Typický proces zneužití probíhá v následujících krocích:

```
1. **Vulnerability Research:** Vyhledání chyby v kódu (např. pomocí
reverzního inženýrství nebo fuzzingu).
2. **Vytvoření exploitu:** Napsání kódu, který chybu vyvolá (např. způsobí
[[buffer_overflow|přetečení paměti]]).
3. **Payload (Užitečné zatížení):** Samotný škodlivý kód, který exploit
doručí do systému. Může to být šifrovací virus (ransomware), zadní vrátka
```

```
(backdoor) nebo příkazový řádek (shell).
4. **Exekuce:** Po spuštění exploitu přebírá kontrolu payload a vykonává
aktivitu útočníka.
```

Příklady známých exploitů

- **EternalBlue:** Exploit vyvinutý agenturou NSA, který zneužíval chybu v protokolu SMB ve Windows. Byl použit při masivních útocích ransomware WannaCry.
- **Stagefright:** Sada exploitů pro systém Android, které umožňovaly ovládnout telefon pouhým zasláním speciálně upravené MMS zprávy.
- **Log4Shell:** Kritický exploit v knihovně Log4j (Java), který v roce 2021 ohrozil miliony serverů po celém světě díky snadnému vzdálenému spuštění kódu.

Ochrana proti exploitům

Boj proti exploitům je nekončící proces, který zahrnuje:

- **Patch Management:** Pravidelná instalace bezpečnostních aktualizací. To je neúčinnější obrana proti známým exploitům.
- **Zabezpečení na úrovni OS:** Technologie jako ASLR (náhodné rozložení paměti) a DEP (zabránění spuštění dat), které znesnadňují fungování exploitů.
- **Antiexploit moduly:** Moderní antiviry a EDR systémy sledují podezřelé chování aplikací (např. pokus prohlížeče spustit kód v paměti) a blokují jej bez ohledu na to, zda je chyba známá.
- **Bug Bounty programy:** Firmy platí etickým hackerům za nahlášení nalezených chyb, aby je mohly opravit dříve, než budou zneužity.

Související pojmy: Zranitelnost, Malware, Zero-day, Buffer Overflow, Payload, Šifrování, Kybernetická bezpečnost.