ВИЯВЛЕННЯ ЗАГРОЗИ CVE-2020-1472 ЗА ДОПОМОГОЮ IDS/IPS SNORT

Федоров І.А., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

На теперішній час можливості систем виявлення вторгнень є необхідним критерієм щодо інфраструктури захисту інформації в корпоративної мережі компанії.

В роботі побудована модель корпоративної мережі компанії з контролером домену Active Directory та систему активного реагування на інциденти Snort [1].

Об'єктом дослідження є вразливість у протоколі автентифікації Netlogon, який використовується у контролері домену Windows Server.

Служба Netlogon RPC, яка використовується для автентифікації комп'ютера та користувача в Windows, також дозволяє комп'ютеру оновлювати пароль свого комп'ютера в домені. Через низку історичних причин ця служба не використовує стандартні протоколи автентифікації для автентифікації комп'ютера. Уразливість існує в нестандартному методі автентифікації. CVE-2020-1472 - це вразливість підвищення привілеїв із-за небезпечного використання шифрування AES-CFB8 для сеансів Netlogon [2]

Система запобігання вторгненням (IPS) є розширенням рішення IDS. IPS здатна автоматично налаштовувати брандмауер та скидати сеанси на основі загроз у реальному часі. Вона використовується для знаходження аномальної поведінки у мережі та виявлення вторгнень. [2, 3]

В доповіді розповідається робота алгоритму автентифікації Netlogon, як перевірити, чи вразливий ваш домен Active Directory до CVE-2020-1472, проведена робота з аналізу трафіку, який генерується зловмисником та написані правила реагування на цю вразливість.

Список літератури

1. Snort 3 is available! [Електронний ресурс] – Режим доступу: https://www.snort.org/.

2. Netlogon Elevation of Privilege Vulnerability CVE-2020-1472 [Електронний ресурс] – Режим доступу: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472.

3. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень // Системи обробки інформації. – 2014. – №. 6. – С. 122-124.

4. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids.