Fooling The Hound
Deceiving Domain Admin Hunters
- Tom Sela -

Follow Me!
TOM SELA
Security Researcher
tom@illusivenetworks.com
@4x6hw

> ls -l

Head Of Security Research at “illusive networks”
- Malware Research Team Leader in “Trusteer” (IBM Security)
- Telekom Innovation Labs - Ben-Gurion University
Acknowledge The Forefathers

@wald0
@CptJesus
@harmj0y
Not This Hound
Agenda

1. Crash Course in Lateral Movement & Graphs

2. Deceptions
   - Real world examples
   - Deception techniques (x4) + Demos

3. Fooling the Hound
   - Planting deceptions in the Lateral Movement Graph

4. Wrap Up \ Conclusions
- Goal -

Detect Attackers
Hunting Domain Admin Credentials
Plant and Monitor
Deceptive Users and Computers
Attack Kill Chain

Credit: Microsoft ATA
From Breach to Complete Domain Control in 6 steps

1. “Reception-PC” HasSession User “Liz”
2. User “Liz” MemberOf Group “GNA”
3. Group “GNA” AdminTo “Room2-PC”
4. “Room2-PC” HasSession Domain Admin “Helpdesk”
5. Domain Admin “Helpdesk” AdminTo “CFO-PC”
6. “CFO-PC” HasSession User “Clark”
Building a Lateral Movement Graph

**Nodes**
- Computer
- Group
- User

**Edges**
- HasSession: Who is logged in where?
- AdminTo: Who has admin rights where?
- MemberOf: Which users, groups and computers belong to which groups?

**Connections**
- MemberOf: Group to Group
- AdminTo: Computer to User
- HasSession: User to Computer

* No administrative privileges required

Credit: *Six Degrees of Domain Admin* - DEF CON 24
Deception

“The act of causing someone to accept as true or valid what is false or invalid”

- Merriam-Webster’s Dictionary
Deceptions in Warfare

- Medieval Times-
  Trip Stairs

- WW2 -
  Fake Tanks
Take Control of the Attacker’s Path With Deceptions

Bloodhound can produce a precise path to any target.

Using the same methods, defenders can predict where to look for attackers.

Even better, using deceptions, defenders can make attackers go where defenders want them to go.
Without deceptions

Credit: BloodHound
With deceptions

Credit: BloodHound
Where to Plant Deceptions?

Existing Machines

Detection: Monitor failed logins attempts

Trap Servers

Detection: Monitor interaction with the server
How to Create Deceptive User Sessions?
From Breach to Complete Domain Control in 6 Steps

1. "Reception-PC" HasSession User "Liz"
2. User "Liz" MemberOf Group "GNA"
3. Group "GNA" AdminTo "Room2-PC"
4. "Room2-PC" HasSession Domain Admin "Helpdesk"
5. Domain Admin "Helpdesk" AdminTo "CFO-PC"
6. "CFO-PC" HasSession User "Clark"
From Breach to Being Caught in 4 Steps

1. "Reception-PC" HasSession User "Liz"
2. User "Liz" MemberOf Group "GNA"
3. Group "GNA" AdminTo "Room2-PC"
4. Domain Admin "Superman" HasSession "CFO-PC"
5. "CFO-PC" AdminTo User "Clark"
6. Domain Admin "Helpdesk" HasSession Domain Admin "Helpdesk"
Where to Plant Deceptions?

Existing Machines

Detection: Monitor failed logins attempts
How to Create Deceptive User Sessions?

Method 1: HKU Registry SIDs
Method 1: Extracting Registry SIDs

**Win API:** RegEnumKey

**Tools:** Get-LoggedOnLocal, PsLoggedon.exe, PVEFindADUser.exe

**Location:** Registry HKU

**Deception Planting:** “reg load HKU\<SID> dummy.dat”
Extracting Registry SIDs - cont.

- HKU Registry Hive holds read permission to “Everyone” by default
- Any Domain User can query the SIDs under HKU of any domain machine
- Converting the SID to username, provides a list of logged-in users.

**Fun Fact:** Enumerating the HKU can give lots of additional information on the target machine: Wifi connections, Geolocation, installed programs etc...
Extracting Registry SIDs - cont.

1. `RegEnumKey HKU`
2. Returns a list of SIDs under HKU
3. Convert SIDs to usernames

Adding registry key to deceive attackers

```
S-1-5-21-1758464992-2458465632-765033826-1104
S-1-5-21-1758464992-2458465632-765033826-1104 Clases
```
How to Create Deceptive User Sessions?

Method 2: Logon-Sessions’ Information
From Breach to Being Caught in **4** Steps

1. "Reception-PC" has a session with User "Liz".
2. User "Liz" is a member of Group "GNA".
3. "GNA" is managed by AdminTo "Room2-PC".
4. "Room2-PC" has a session with Domain Admin "Superman".
5. "CFO-PC" is managed by AdminTo User "Clark".
6. Domain Admin "Helpdesk" has a session with "CFO-PC".
Method 2: Extracting Logon-Sessions’ Information

**Win API:** NetWkstaUserEnum

**Tools:** Get-LoggedOn, PsLoggedon.exe, NetView.exe, Mimikatz, WCE

**How To Access:** Wkssvc named pipe

**Deception Planting:** “runas /netonly /noprofile /user:<Domain>\<User> <process>”

**Open Source Tool:** “Dcept” by secureworks [https://github.com/secureworks/dcept](https://github.com/secureworks/dcept)
Extracting Logon-Sessions’ Information - cont.

• For every successful login, Windows creates a logon session and returns a user token.

• `NetWkstaUserEnum` returns the information of all existing tokens.

• No successful authentication -> no token.

• Except for… “RunAs /netonly”
Extracting Logon-Sessions’ Information - cont.

3. Extract the usernames from **WKSTA_USER_INFO_1**

**Syntax**

```c++
typedef struct WKSTA_USER_INFO_1 {
    LMSTR wku1_username;
    LMSTR wku1_logon_domain;
    LMSTR wku1_oth_domains;
    LMSTR wku1_logon_server;
} WKSTA_USER_INFO_1,
*PKWSTA_USER_INFO_1,
*LPWKSTA_USER_INFO_1;
```

1. **NetWkstaEnumUsers Request**

2. **NetWkstaEnumUsers Response**

*The API requires administrative privileges on the target*
PS C:\> Import-Module "C:\Dev\Tools\Bloodhound\Bloodhound.ps1"
PS C:\>
How to Create Deceptive User Sessions?

Method 3: SMB Sessions
From Breach to Being Caught in 4 Steps

1. "Reception-PC" HasSession User "Liz"
2. User "Liz" MemberOf Group "GNA"
3. Group "GNA" AdminTo "Room2-PC"
4. Domain Admin "Superman" HasSession "Room2-PC"
5. Domain Admin "Superman" AdminTo "CFO-PC"
6. User "Helpdesk" HasSession "CFO-PC"
Where to Plant Deceptions?

Detection: Monitor interaction with the server
Method 3: Extracting SMB Sessions

**Win API:** NetSessionEnum

**Tools:** Get-NetSession, Netsess.exe, NetView.exe

**How To Access:** Srvsvc named pipe

**Deception Planting:** Deceptive server response to NetsessionEnum
Extracting SMB Sessions - cont.

- The “Lanman SMB server” is installed by default on any windows machine
- SMB session information contains the source host and username
- Remote access of session information does not require admin privileges
Extracting SMB Sessions - cont.

1. User: “Clark”  
   Computer: “Room2-PC”

2. NetSession Request
   File Server
   SMB Session

3. NetSession Response
   User: “Clark”  
   Computer: “Room2-PC”

4. “Clark” user is logged on to Computer “Room2-PC”
Extracting SMB Sessions - cont.

1. NetSession Request

2. NetSession Response
   User: “Superman”
   Computer: “Room2-PC”

3. “Superman” is logged on to “Room2-PC”
PS C:\> Import-Module "C:\Dev\Tools\Bloodhound\Bloodhound.ps1"
PS C:\>
How to Create Deceptive Local Admins?
From Breach to Being Caught in 3 Steps

1. "Reception-PC" HasSession User "Liz"
2. "Room3-PC" HasSession Domain Admin "Superman"
3. AdminTo "GNA" Group "GNA"
4. HasSession "Room2-PC"
5. AdminTo "CFO-PC" Domain Admin "Helpdesk"
6. "CFO-PC" HasSession User "Clark"
How to Create Deceptive Local Admins?

Method 1: Administrator’s Group Members
Method 1: Extracting Local Admins

**Win API:** NetLocalGroupGetMembers

**Tools:** Get-NetLocalGroup

**Location:** SAM database

**Deception Planting:** Deceptive server response to NetLocalGroupGetMembers
• “NetLocalGroupGetMembers” API remotely retrieves members of a particular local group

• Remote access of group membership does not require admin privileges
Extracting Local Admins – cont.

1. NetLocalGroupGetMembers Request

2. NetLocalGroupGetMembers Response
   ‘Administrators’ group member: “Liz”

3. “Liz” is an administrator of “Room3-PC”

Trap Server “Room3-PC”
SHOW ME HOW TO FOOL
Planting Deceptions in The Lateral Movement Graph

**Goal:** Make every ‘shortest path’ contain at least one deception

**Method:**
1. Add deceptive sessions to every 1st degree computer
2. Add deceptive computers to the top 1st degree groups
3. Add non-connected computers to the graph
Add deceptive sessions to every 1st degree computer
Add deceptive computers to the top 1st degree groups
Add deceptive session to every 1st degree computer
Add deceptive computer to the top 1st degree groups
Add non-connected computers to the graph
We Covered

1. Lateral movement and graphs
2. 4 methods to plant deceptions
3. How to control the path of an attacker
4. How to plant deceptions in every ‘shortest path’ to domain admin

Conclusions

1. Deceptions bring doubt and uncertainty to the operations of attackers
2. As a security strategy, walls are good, but we have to assume that walls will be breached
3. Using deceptions, we could make attackers fear what awaits them behind the walls
Using Deceptions, We Could Make Attackers...
Questions?

tom@illusivenetworks.com

@4x6hw
Thank You

tom@illusivenetworks.com

@4x6hw

Follow Me!