BSIDES LAS VEGAS

ACTIVE DIRECTORY SECURITY

8 (very) low hanging fruits and how to smash those attack paths

WAVESTONE

Rémi Escourrou

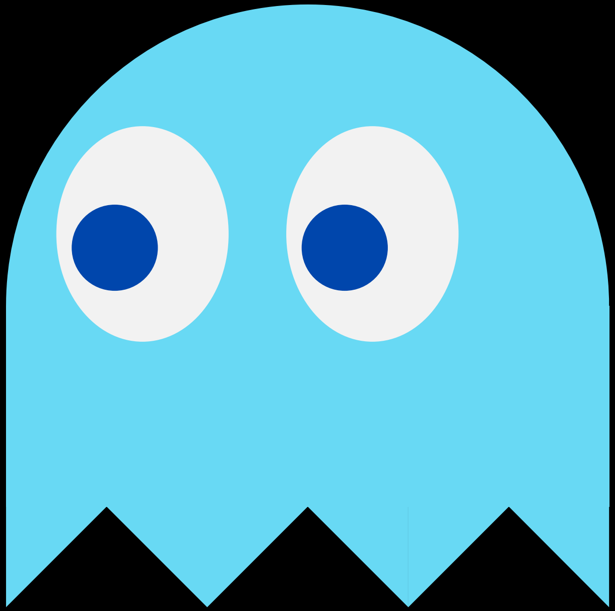
Work at Wavestone as

- Penetration tester
- First responder in the CERT-W

Interests

- Active Directory / Windows stuffs
- Red Wine / Baguette
- Judo

@remiescourrou



Nicolas Daubresse

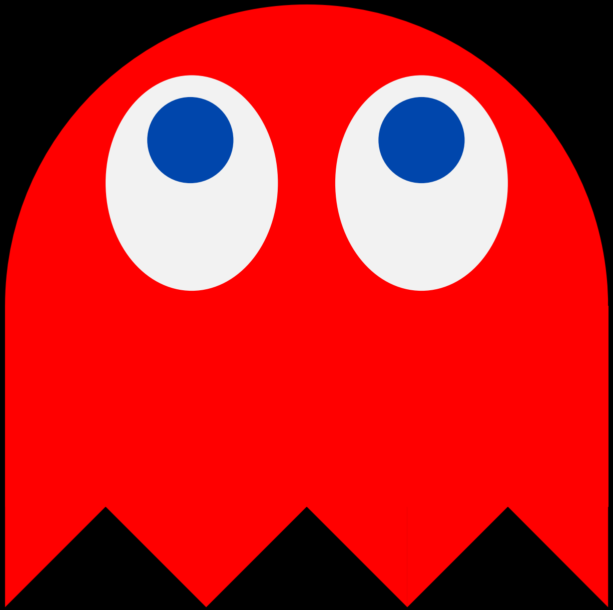
Work at Wavestone as

- Penetration tester
- First responder in the CERT-W

Interests

- Active Directory / Windows stuffs
- Beers
- Board games

@nicolas_dbresse



Welcome inside the pacman firm

Our IS

Microsoft
Active Directory

Groups

Servers

Users

Administrators

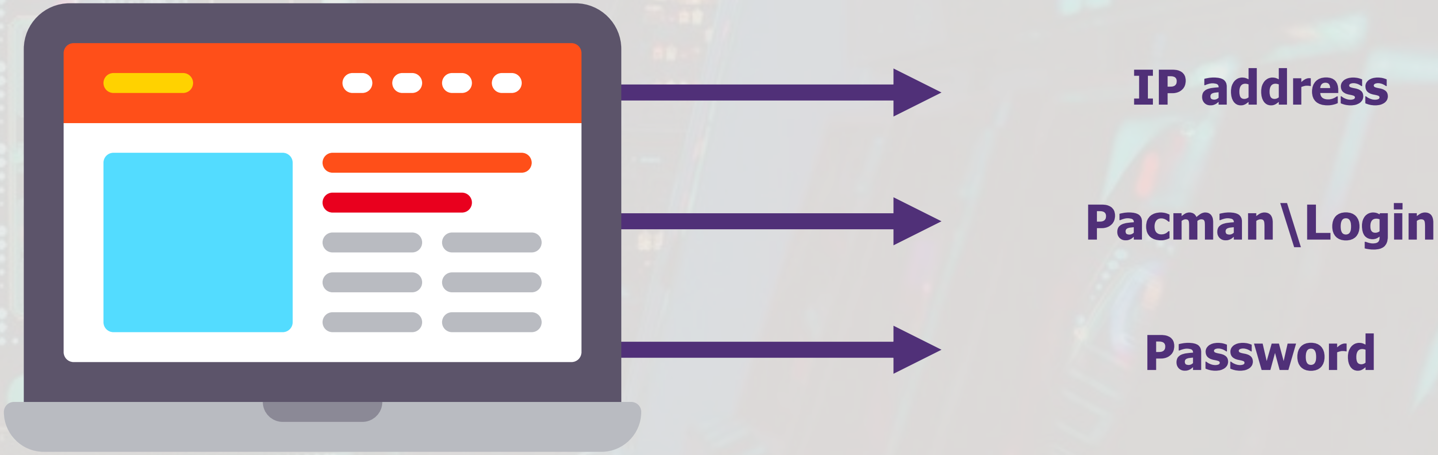
Application

Workstations

LAB PREREQUISITE

VMs are available through **Remote Desktop Protocol**

Wifi : ActiveDirectory

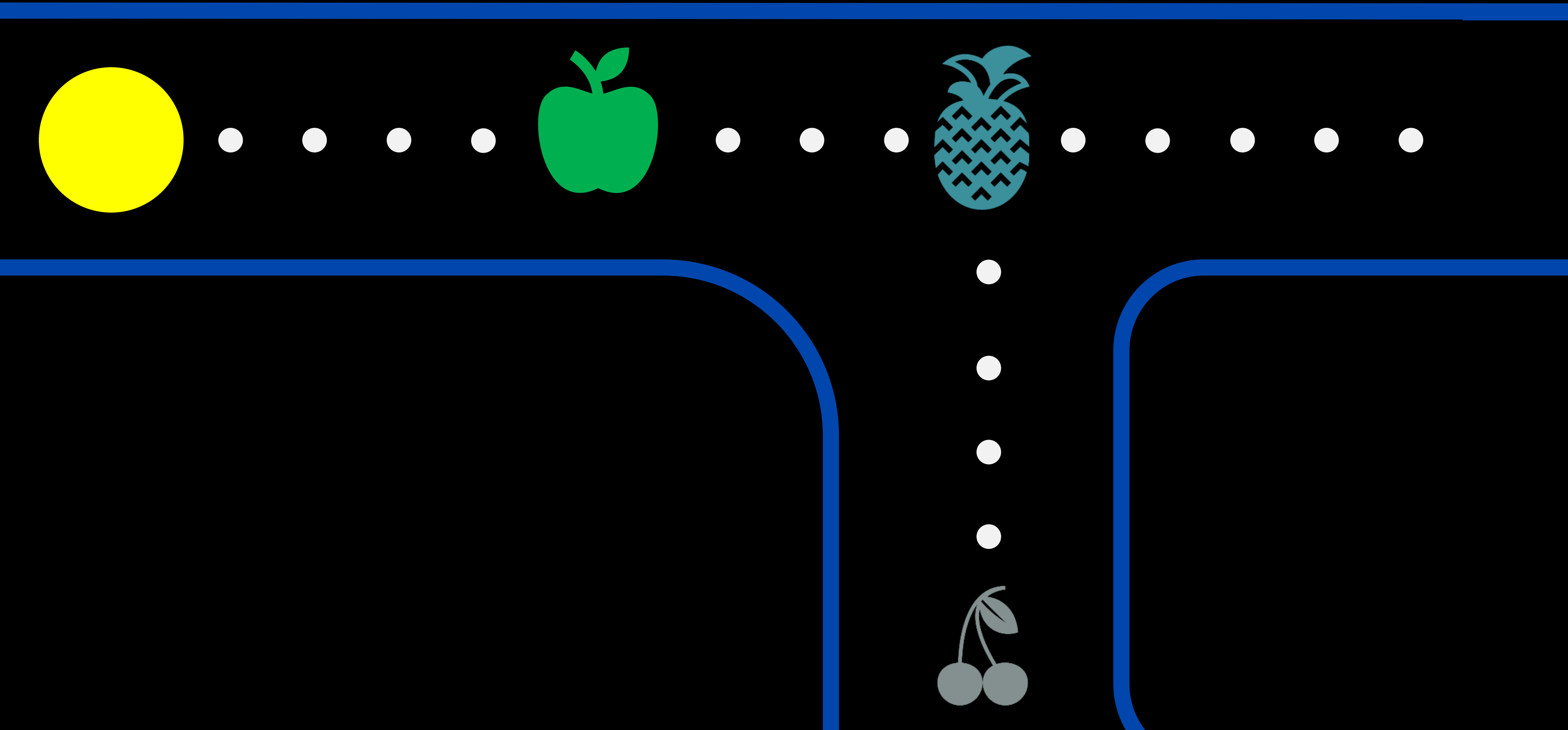


IP address

Pacman\Login

Password

READY ?

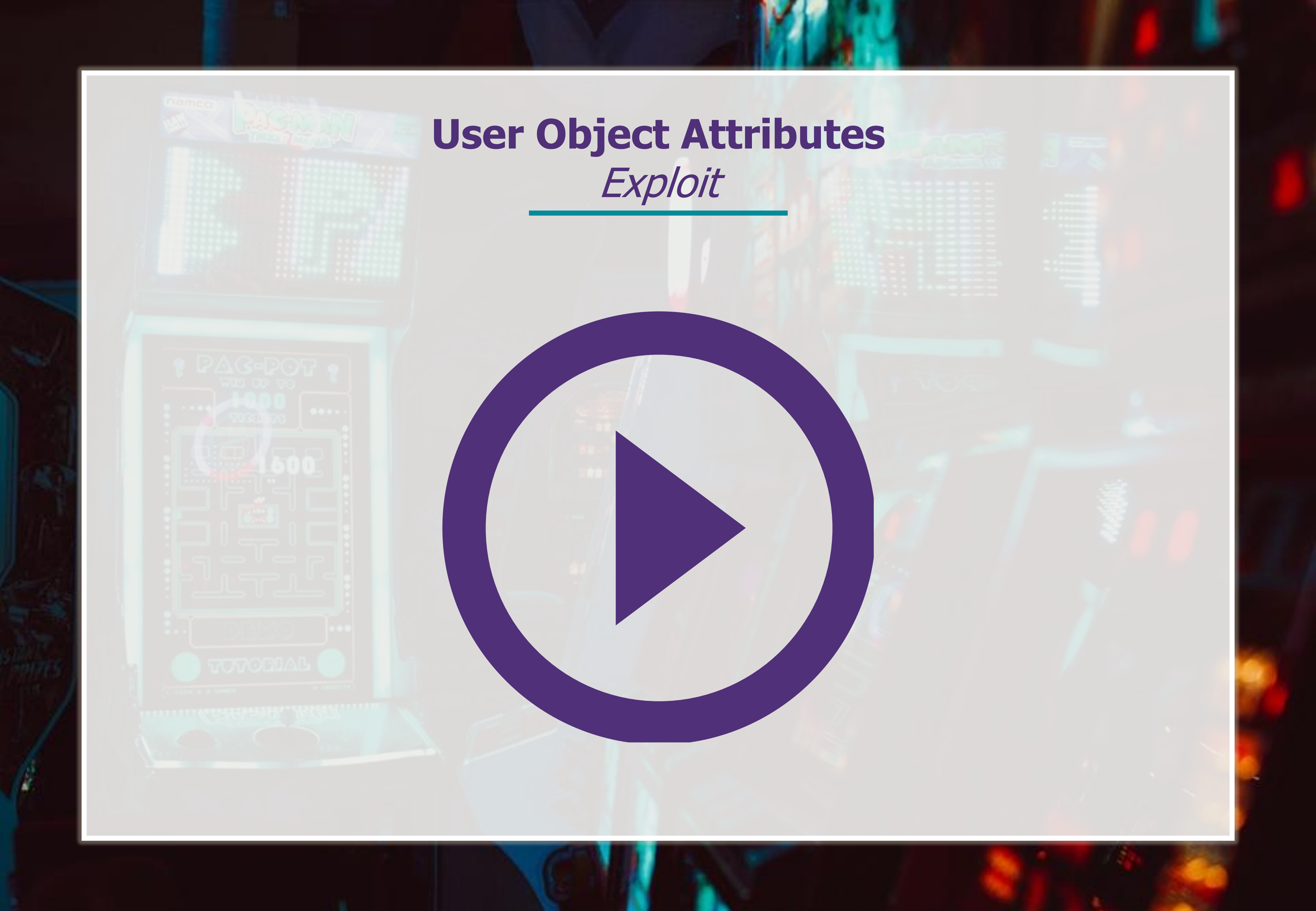


User Object Attributes

- **samAccountName :** user logon name
- **MemberOf :** groups which this user belongs
- **adminCount :** set to 1, if the account was a member of one of the administrative groups
- **pwdLastSet :** date and time that the password for this account was last changed
- **badPwdCount :** number of times the user tried to log on to the account using an incorrect password
- […]
- **description : free field !!!!**

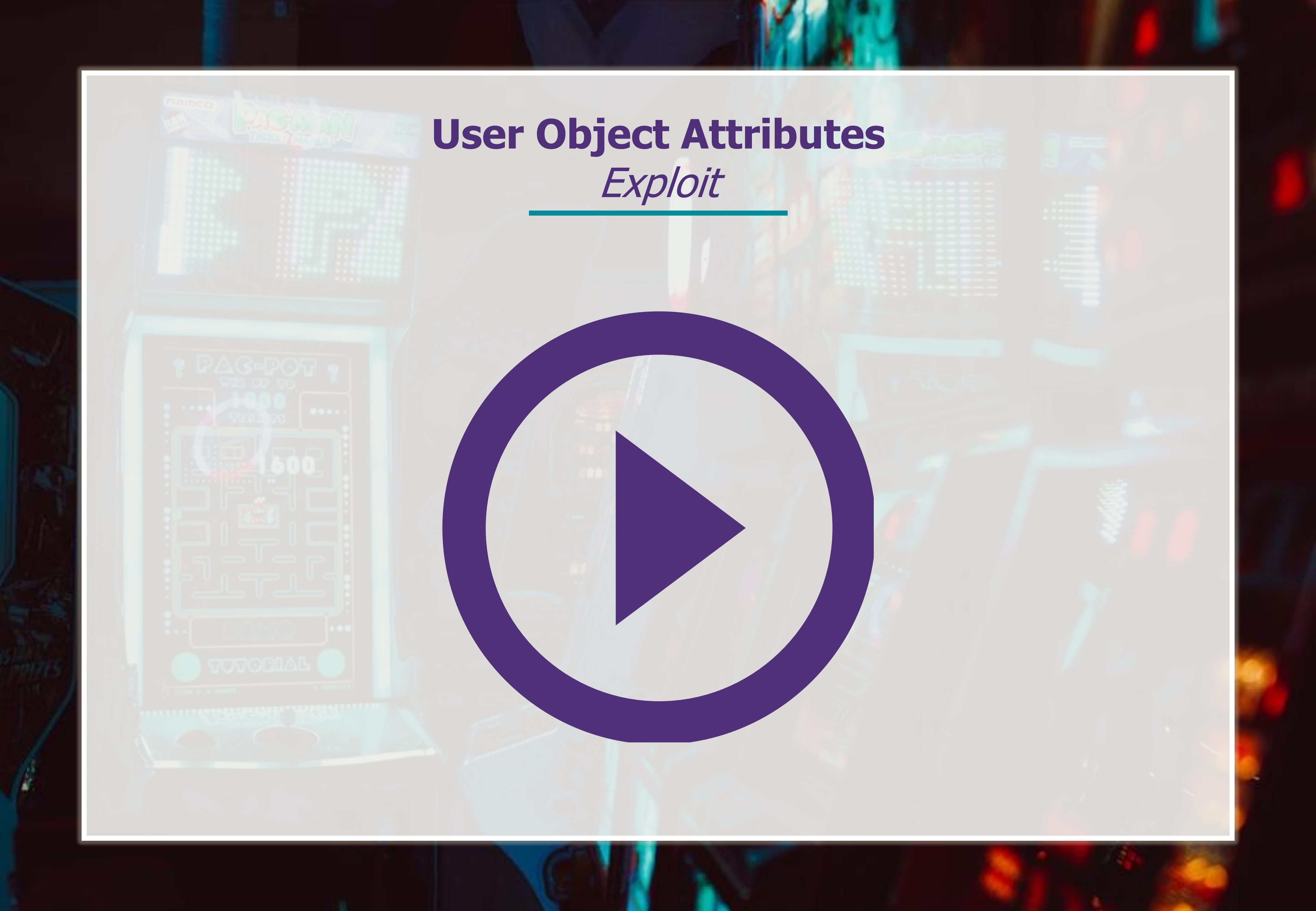
User Object Attributes

Exploit



User Object Attributes

Exploit



User Object Attributes

Feedback

PENTEST FAIL

Find a password inside a DA user's description **after 2 days**…

STATISTICS

50 % of the time we found at least one password inside description attribute

User Object Attributes

Harden & Trap

Review user description manually

1/ Extract all user description and review them once

2/ Perform differential analysis each month

Set a user honeypot

1/ Create a decoy user with a password inside the description

2/ Detect NTLM and Kerberos authentication on this account
Events ID 4625 and 4771

User Object Attributes

Harden & Trap

Set a user honeypot

1/ Create a decoy user with a password inside the description

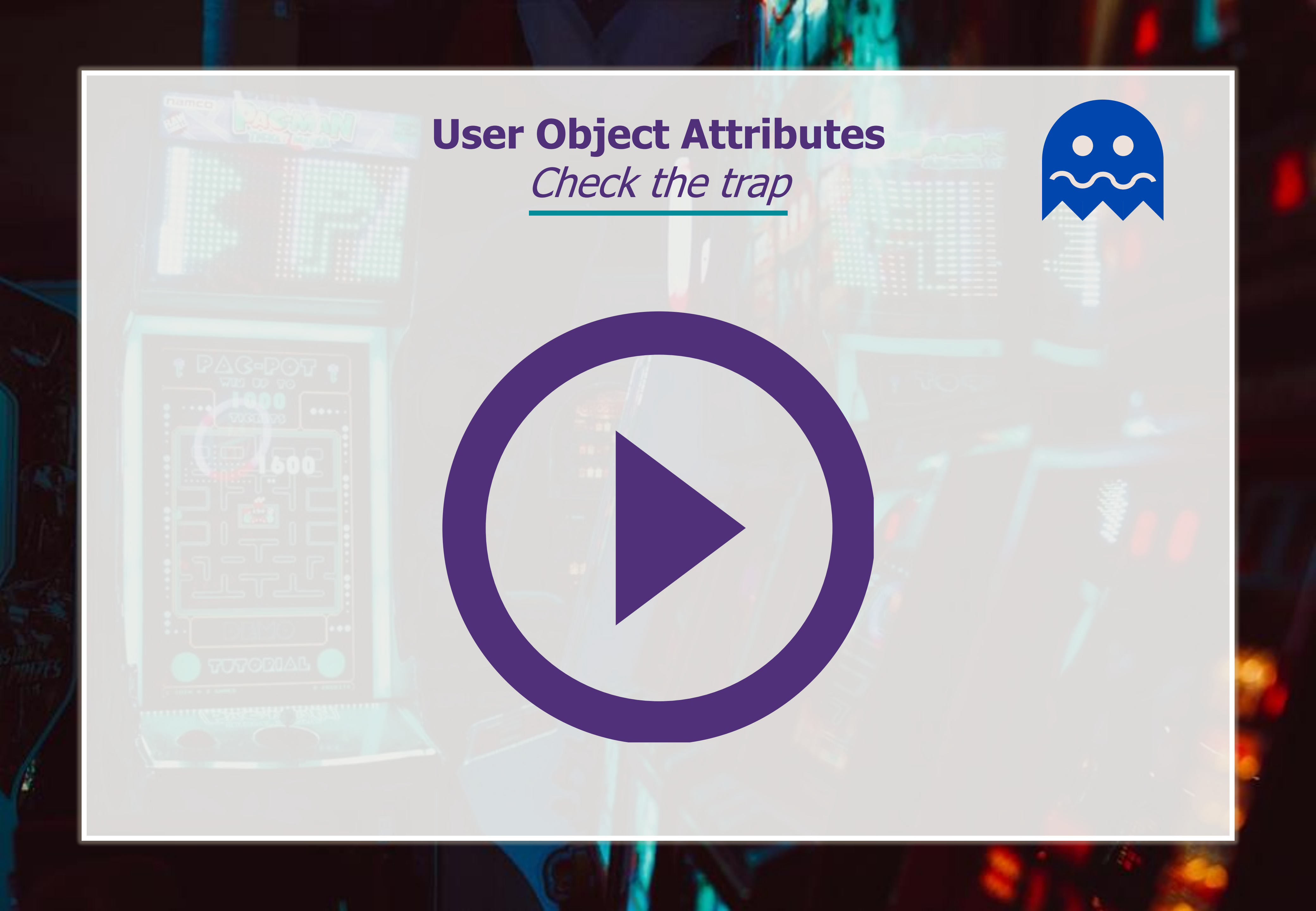
2/ Detect NTLM and Kerberos authentication on this account
Events ID 4625 and 4771

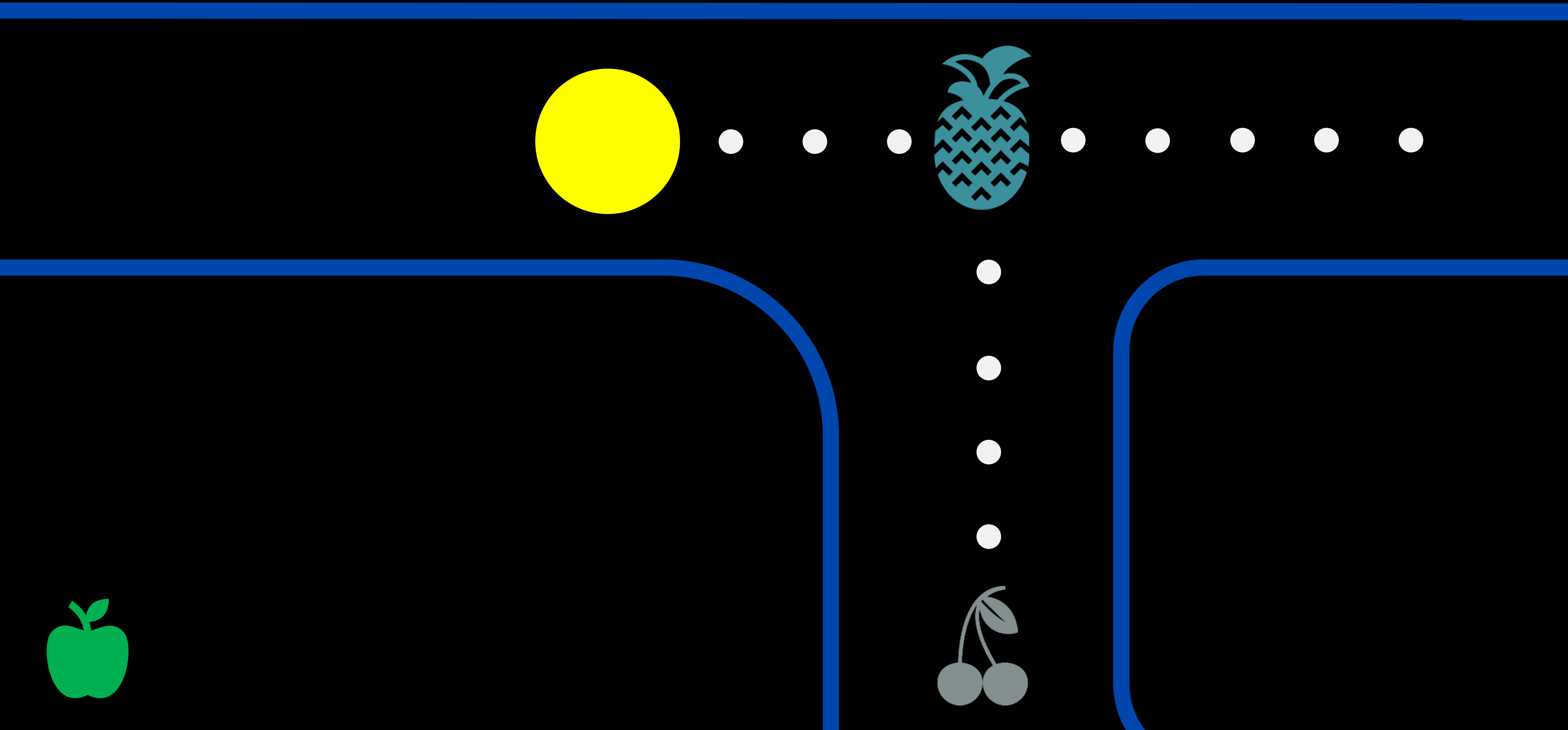
Event ID for NTLM and Kerberos authentication are different

"Fun with LDAP, Kerberos (and MSRPC) in AD Environments" @ropnop

User Object Attributes

Check the trap





Network share

- Time saving > IT Production > security

- Classic keywords in share:

.ps1 : ConvertTo-SecureString, SqlConnection, LdapConnection, NetworkCredential

.vbs : strDomain, strPassword

.sql : Trusted_Connection, Integrated Security, Connect

.txt : pwd, pass

Network share

Exploit

Network share

Exploit

Network share

Feedback

BEST SHOT

More than **5 000 passwords** in a single text file

IT FAIL

Require IT to use **Keepass** but let them put the **password in .txt** inside the **same directory**

STATISTICS

99,99 % of the time we found at least one password inside “Domain Users” shares

Network share

Detect and Trap

Monitor traffic

1/ Identify large amount of SMB connection in small amount of time

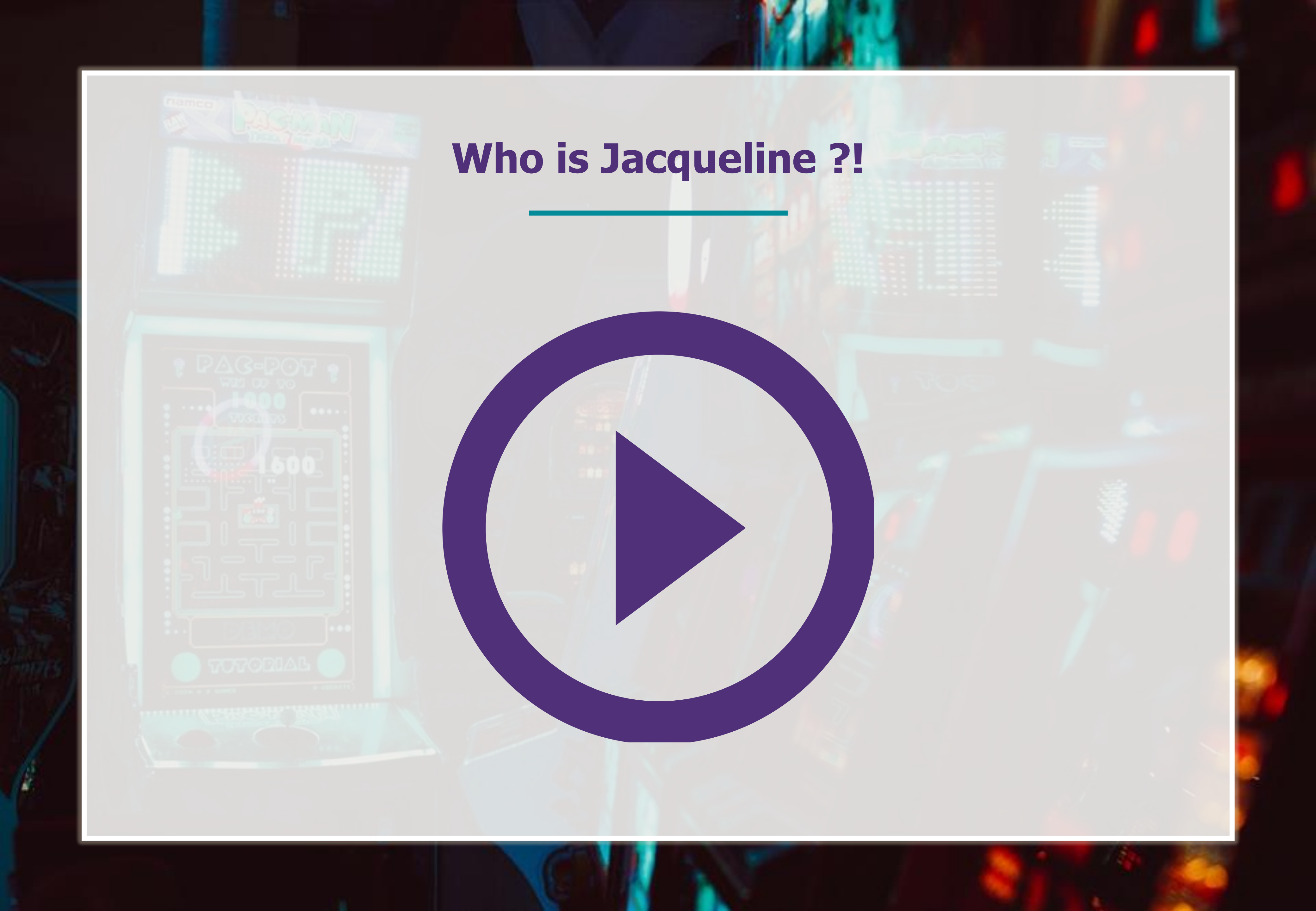
2/ Identify large amount of file opening

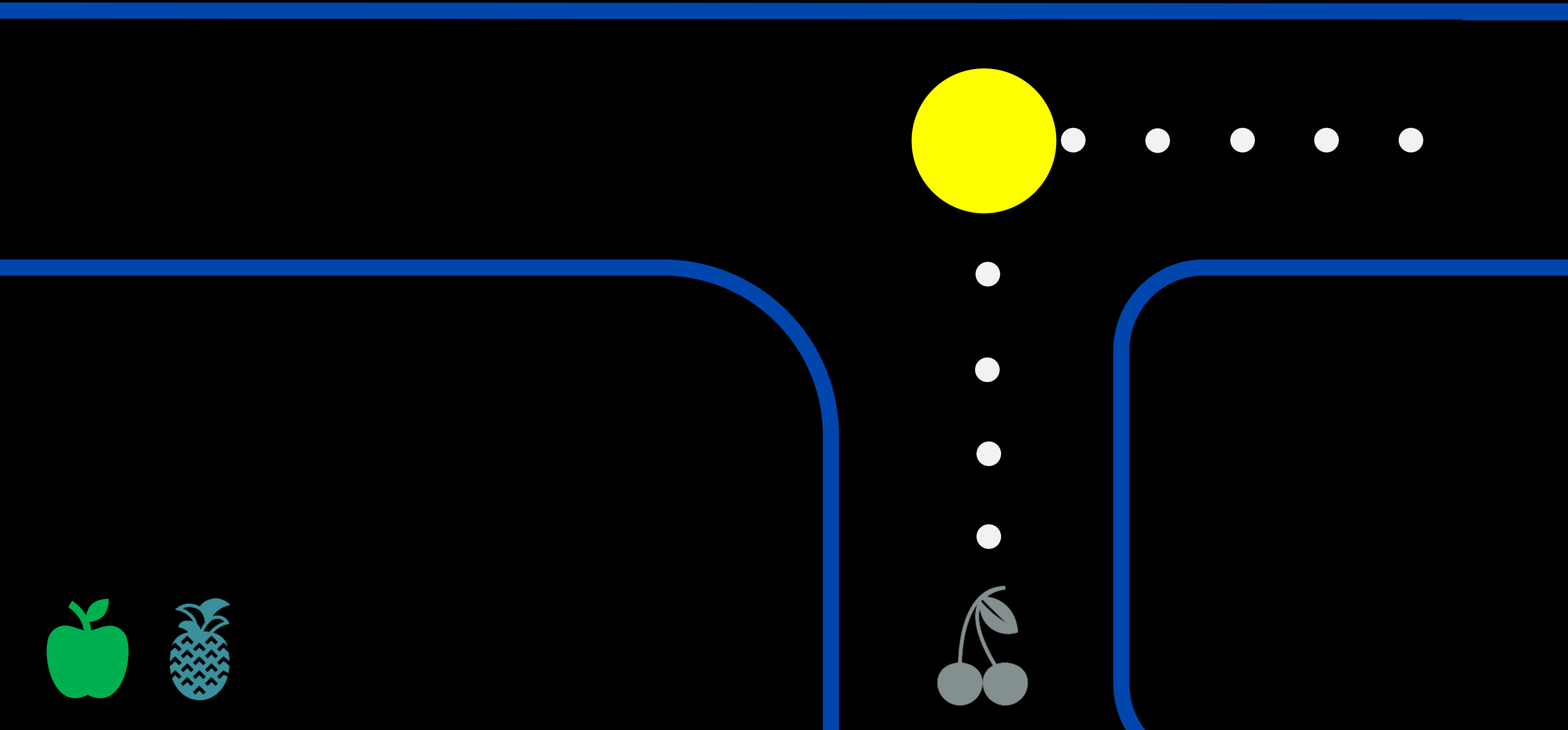
Set a user honeypot

1/ Create a decoy user with a password inside the directory "\\DOMAIN\NETLOGON"

2/ Detect NTLM and Kerberos authentication on this account
Events ID 4625 and 4771

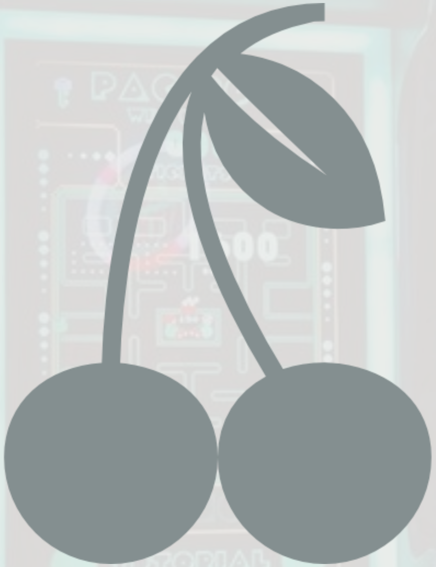
Who is Jacqueline ?!





Password Spraying

- **One user has one password**
- **But one password could be used by several users**

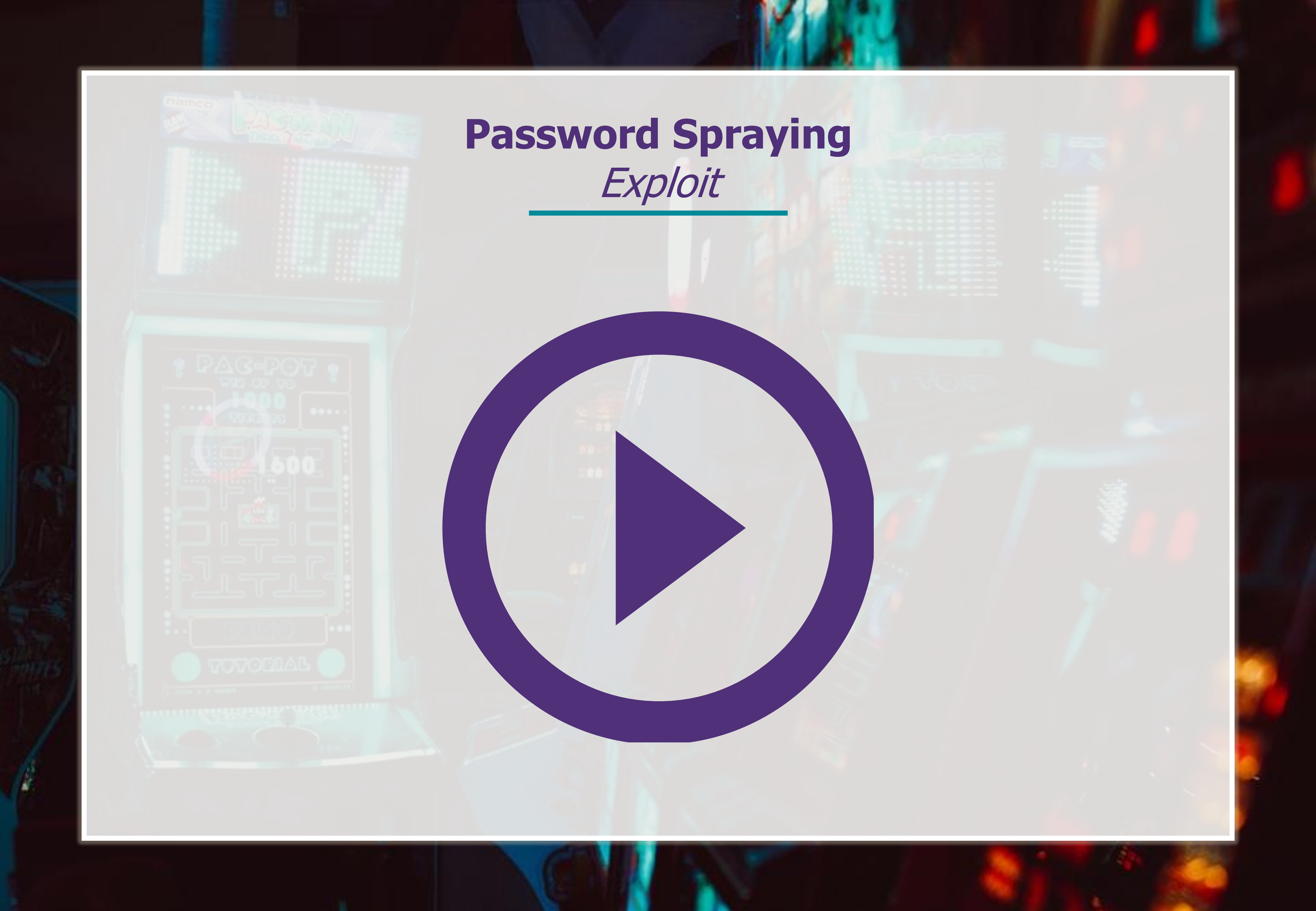


- With badPwdCount attributes, you will never block any accounts
- Best targets : FIRM2018! or FIRM2018*

⚠ **badPwdCount is not replicated between DC but centralized on PdC**

Password Spraying

Exploit



Password Spraying

Feedback

BEST SHOT

The **same password** was always used when creating accounts… Good news, a DA account was created on the first day of our assessment

STATISTICS

100 % of the time we found a valid password pattern

Password Spraying

Detect

Monitor NTLM and Kerberos authentication

1/ Create a correlation rules that state if x number of events occur within y time frame that password spraying is happening.

-> Configure alerts for >50 events **4625** (NTLM) within 1 minute

-> Configure alerts for >50 events **4771** (Kerberos) with failure code=0x18 within 1 minute

-> Configure alerts for >100 events **4648** (runas) on workstations within 1 minute.

https://www.trimarcsecurity.com/single-post/2018/05/06/Trimarc-Research-Detecting-Password-Spraying-with-Security-Event-Auditing

Password Spraying

Harden

Ban passwords using common local words

1/ Code and **deploy a custom password filter DLL** in order to ban common passwords

But… Are you enough confident to inject a custom DDL in all your DC that intercepts password change requests ?

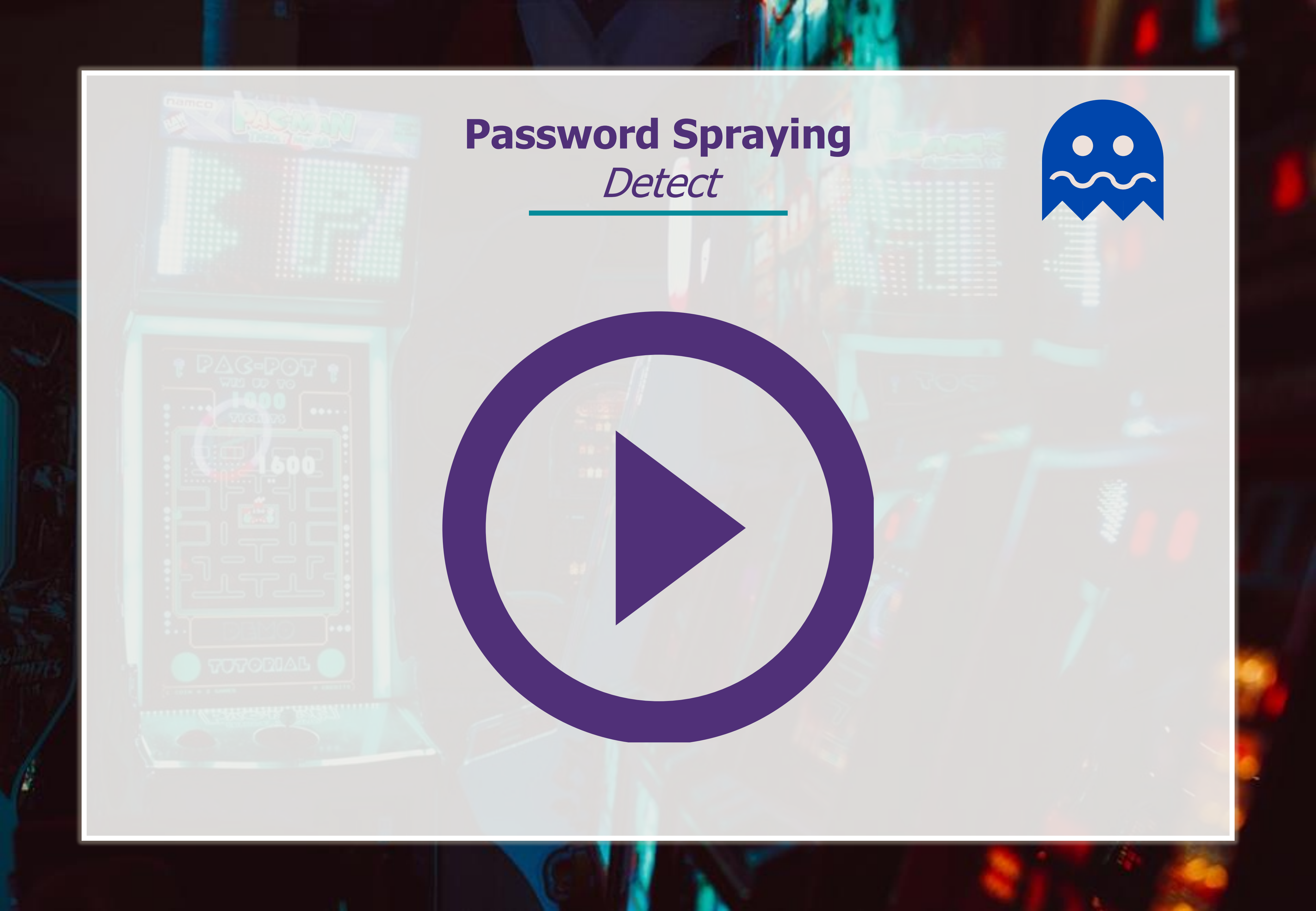
2/ **Enforce Azure AD password protection** if you are using Azure AD Premium P1 or P2

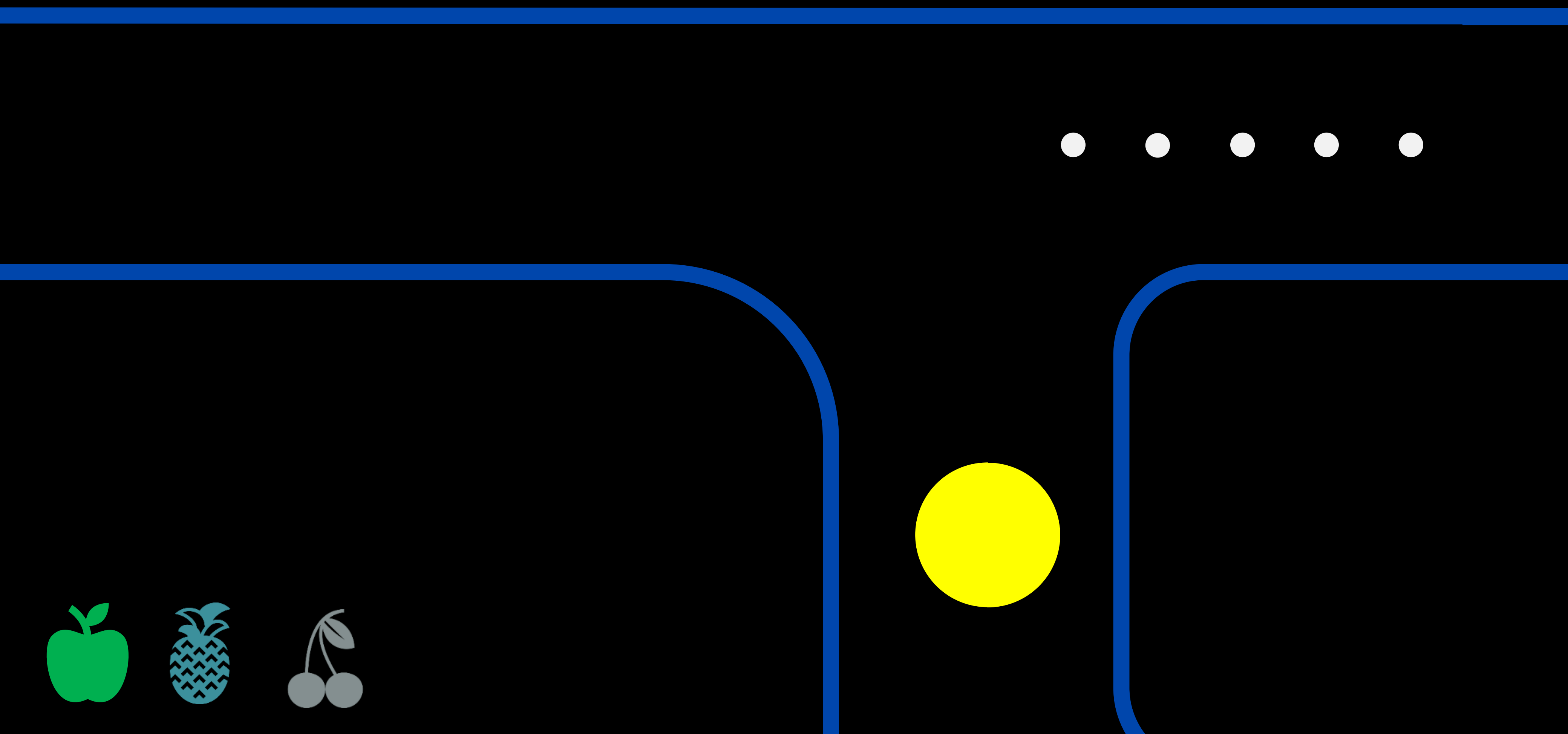
In this case, the DLL was written by MS!

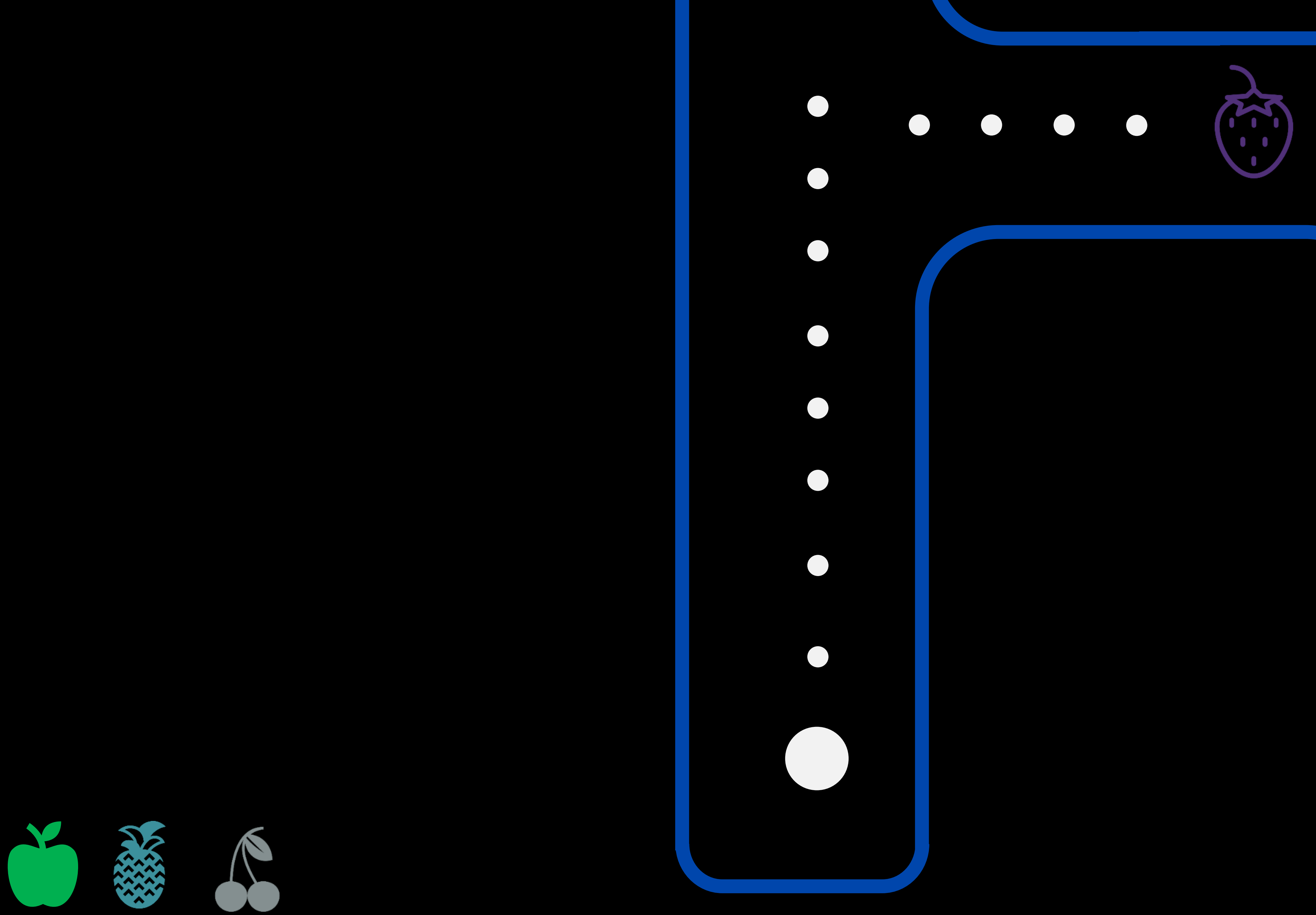
https://github.com/jephthai/OpenPasswordFilter
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Password Spraying

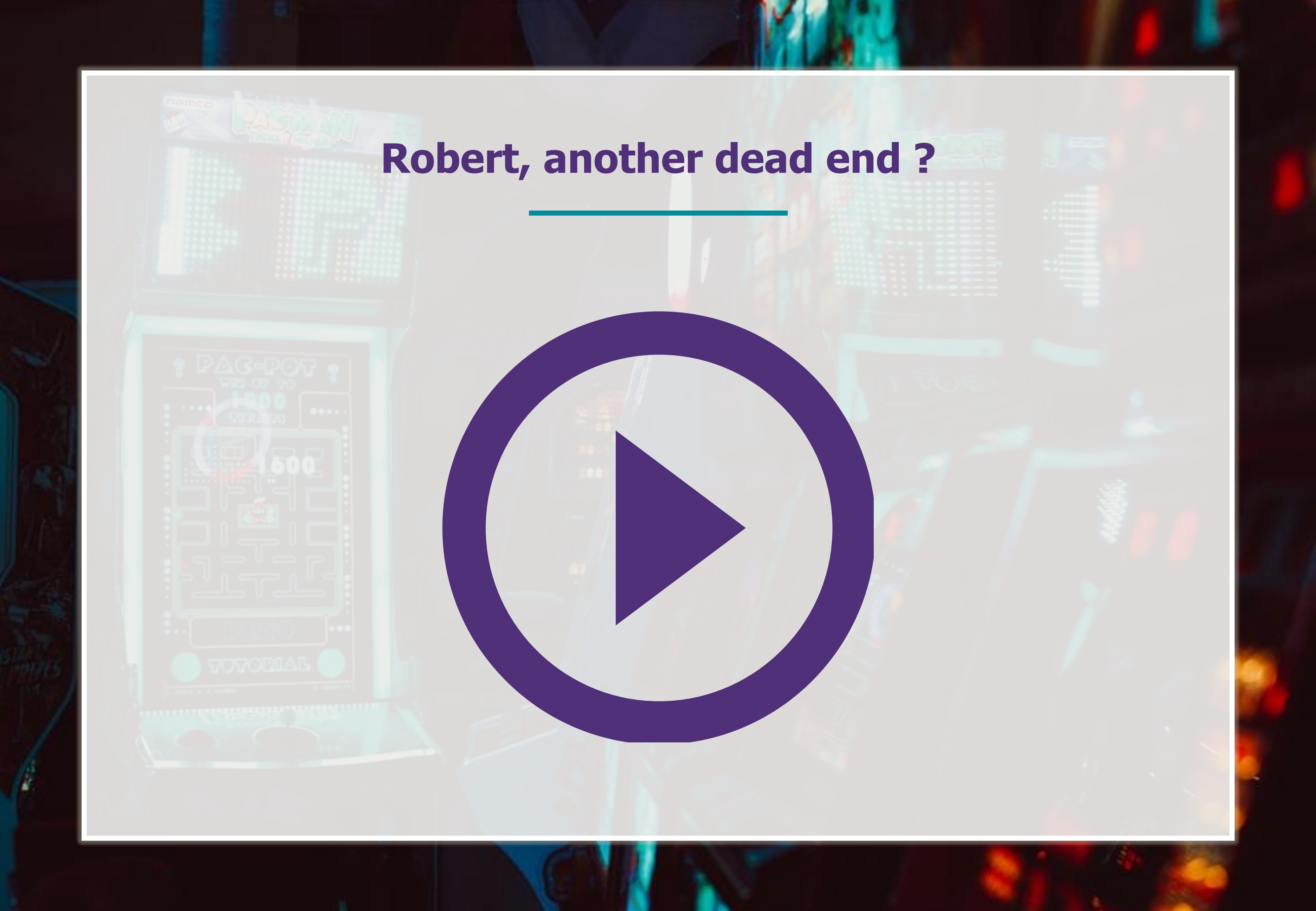
Detect

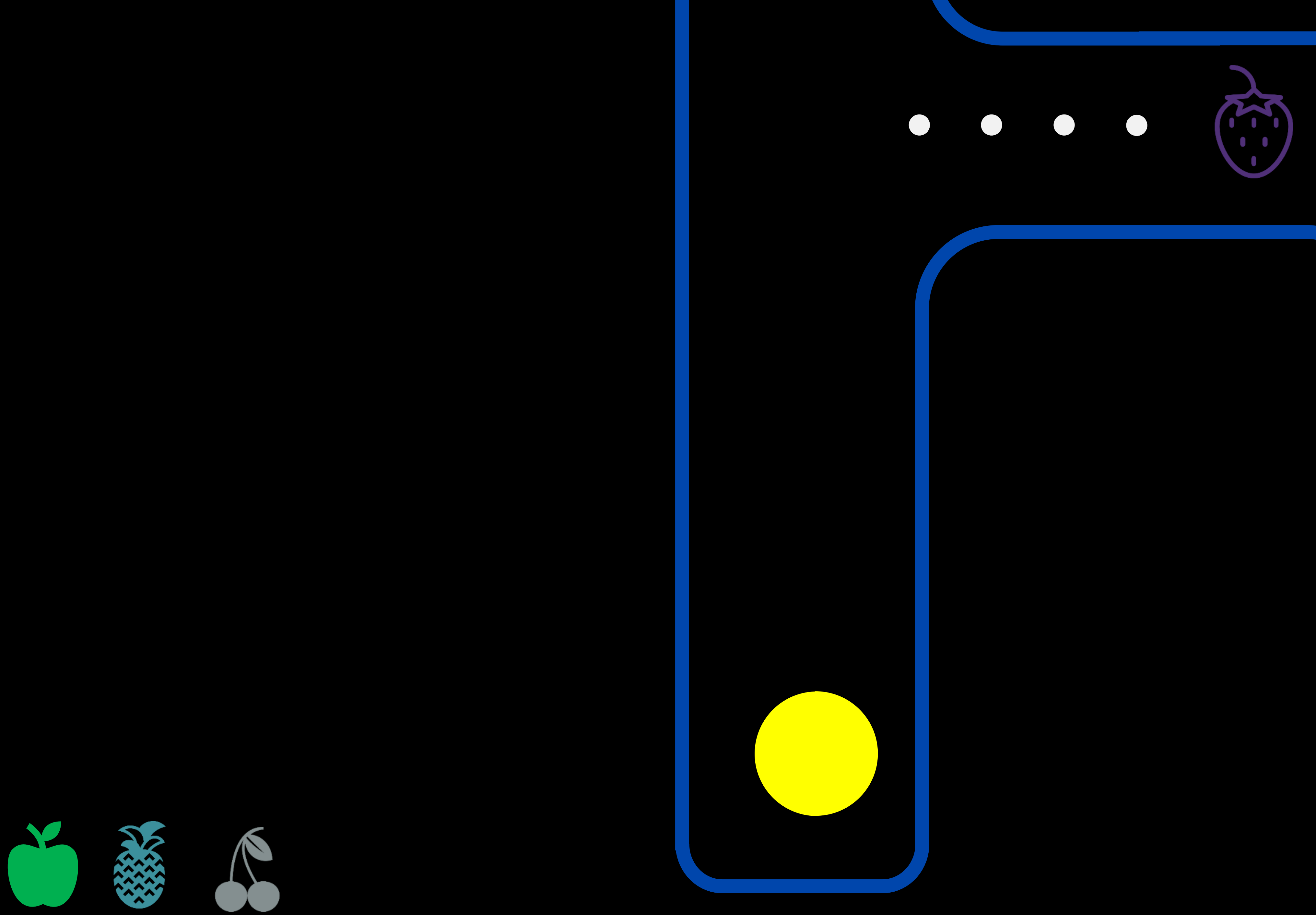


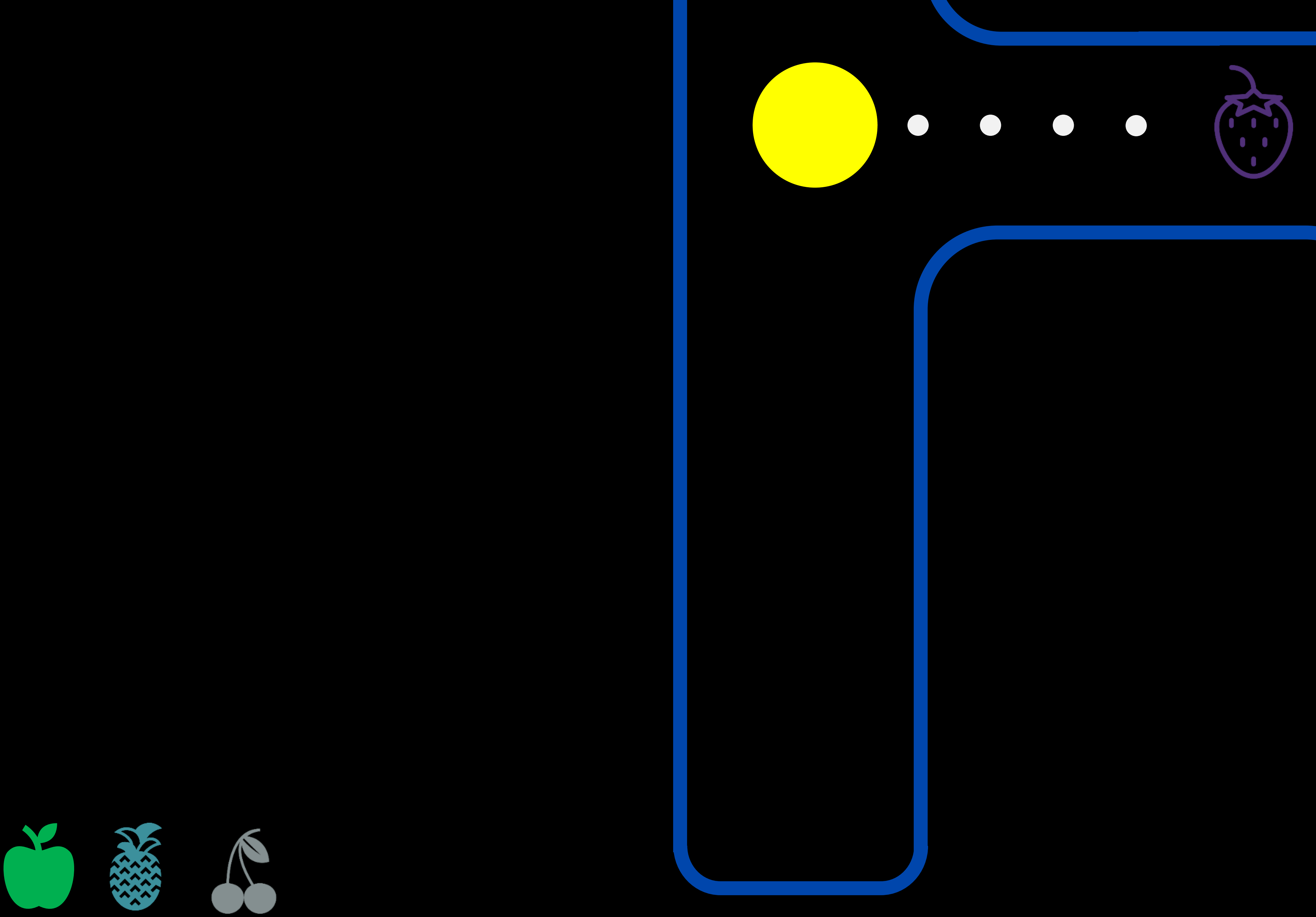




Robert, another dead end ?

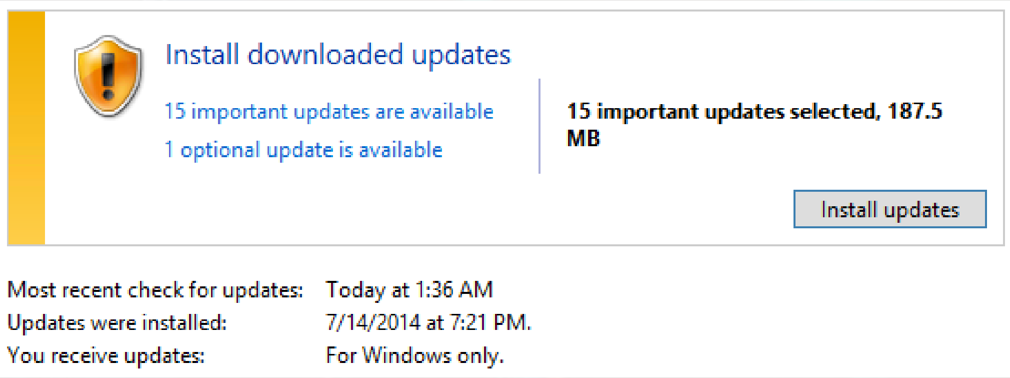






Obsolete operating system

- **Unauthenticated Remote Code Execution**



Install downloaded updates

15 important updates are available

1 optional update is available

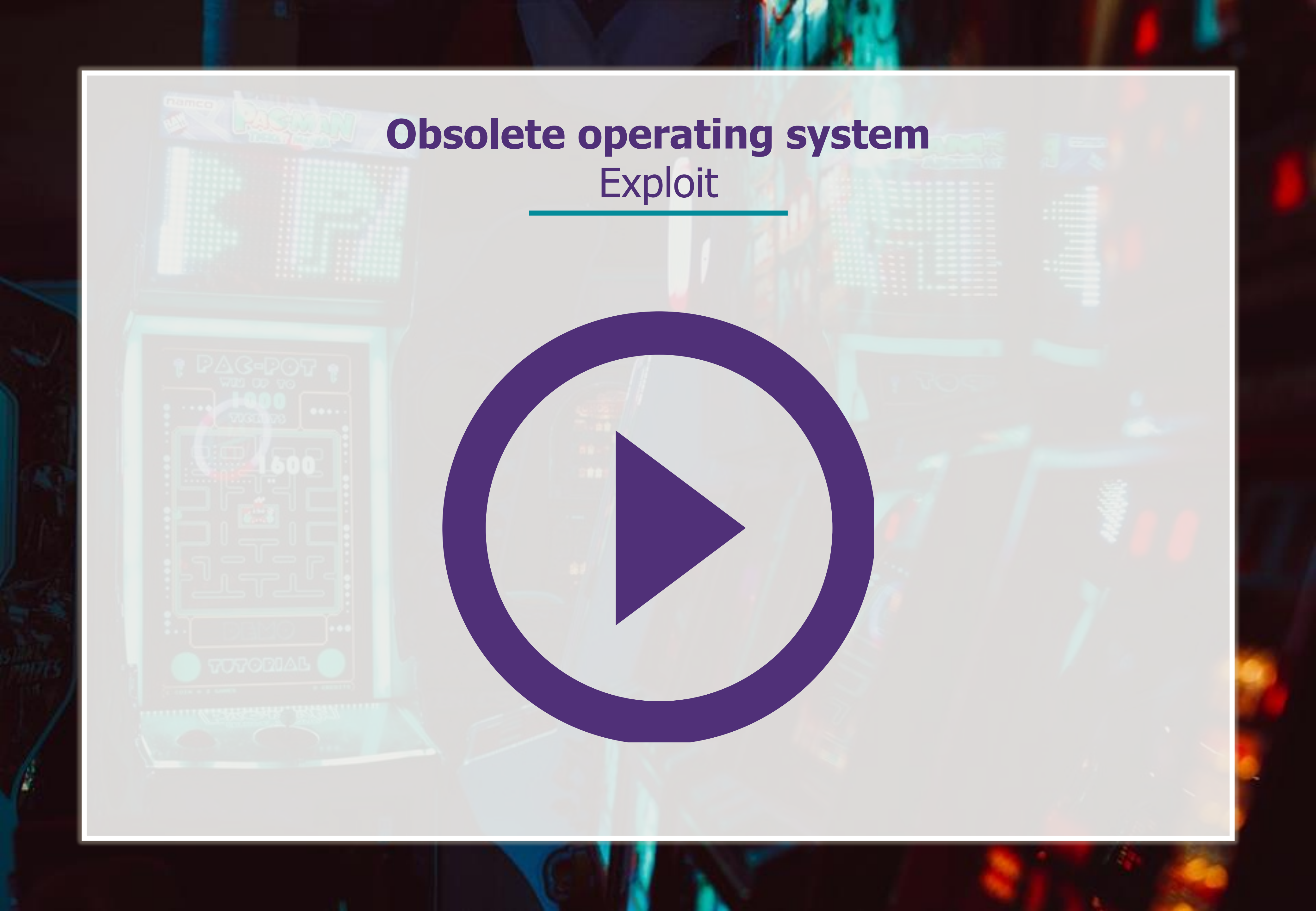
15 important updates selected, 187.5 MB

Most recent check for updates: Today at 1:36 AM
Updates were installed: 7/14/2014 at 7:21 PM.
You receive updates: For Windows only.

- **Easy to find & Easy to exploit**
- MS08-067 (#conficker) or MS17-010 (#eternalblue)

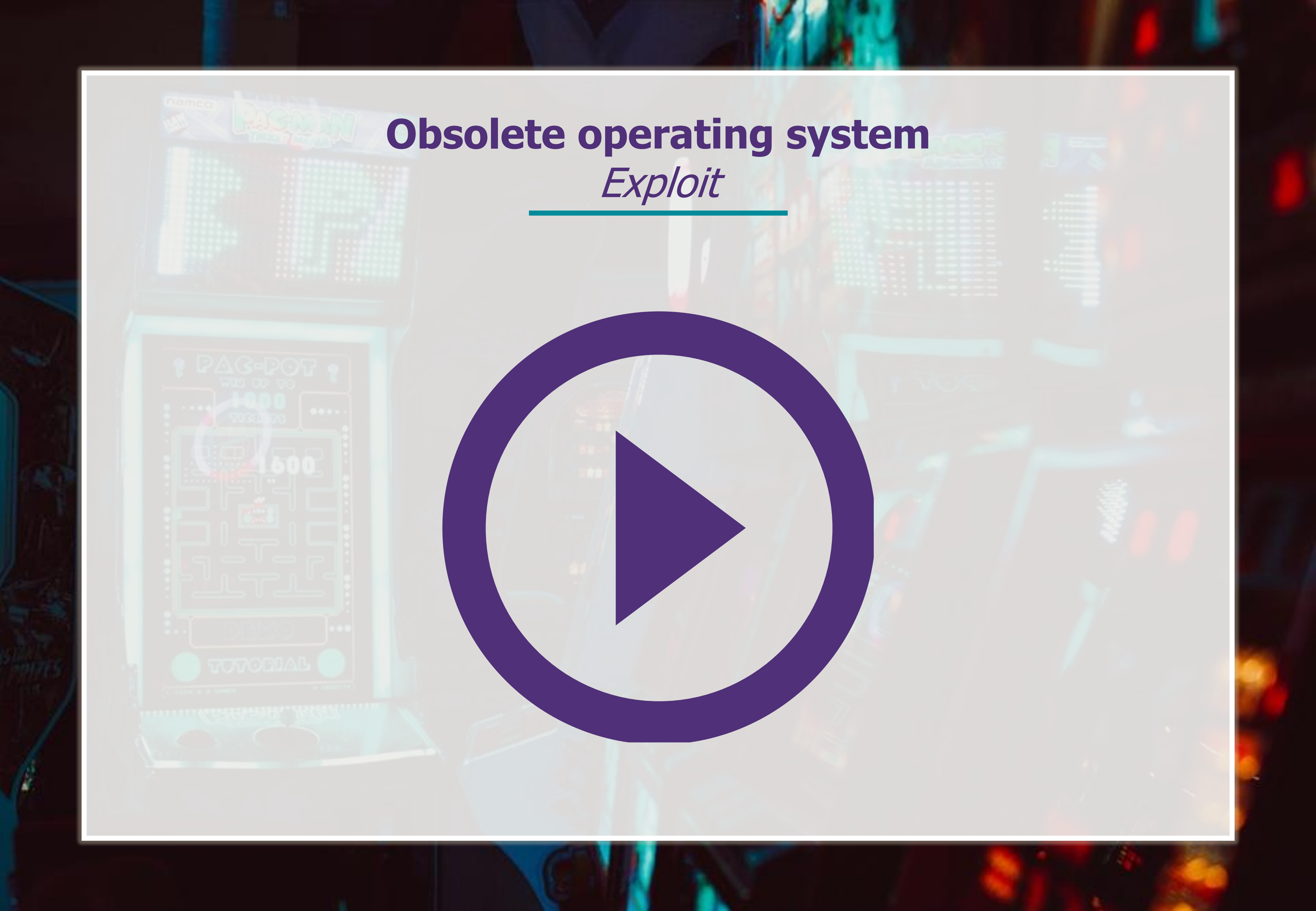
Obsolete operating system

Exploit



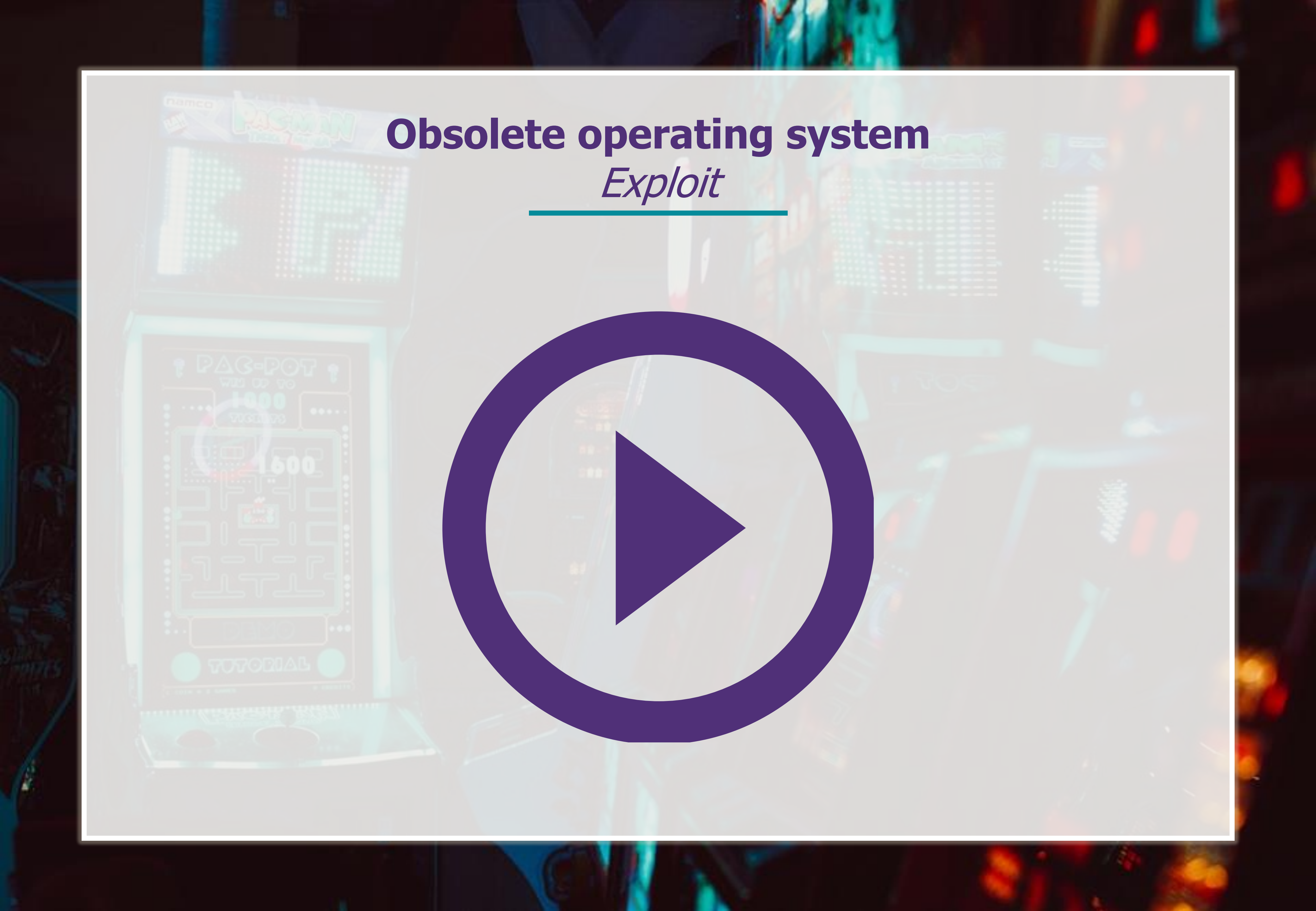
Obsolete operating system

Exploit



Obsolete operating system

Exploit



Obsolete operating system

Harden

Obsolete operating system

Harden

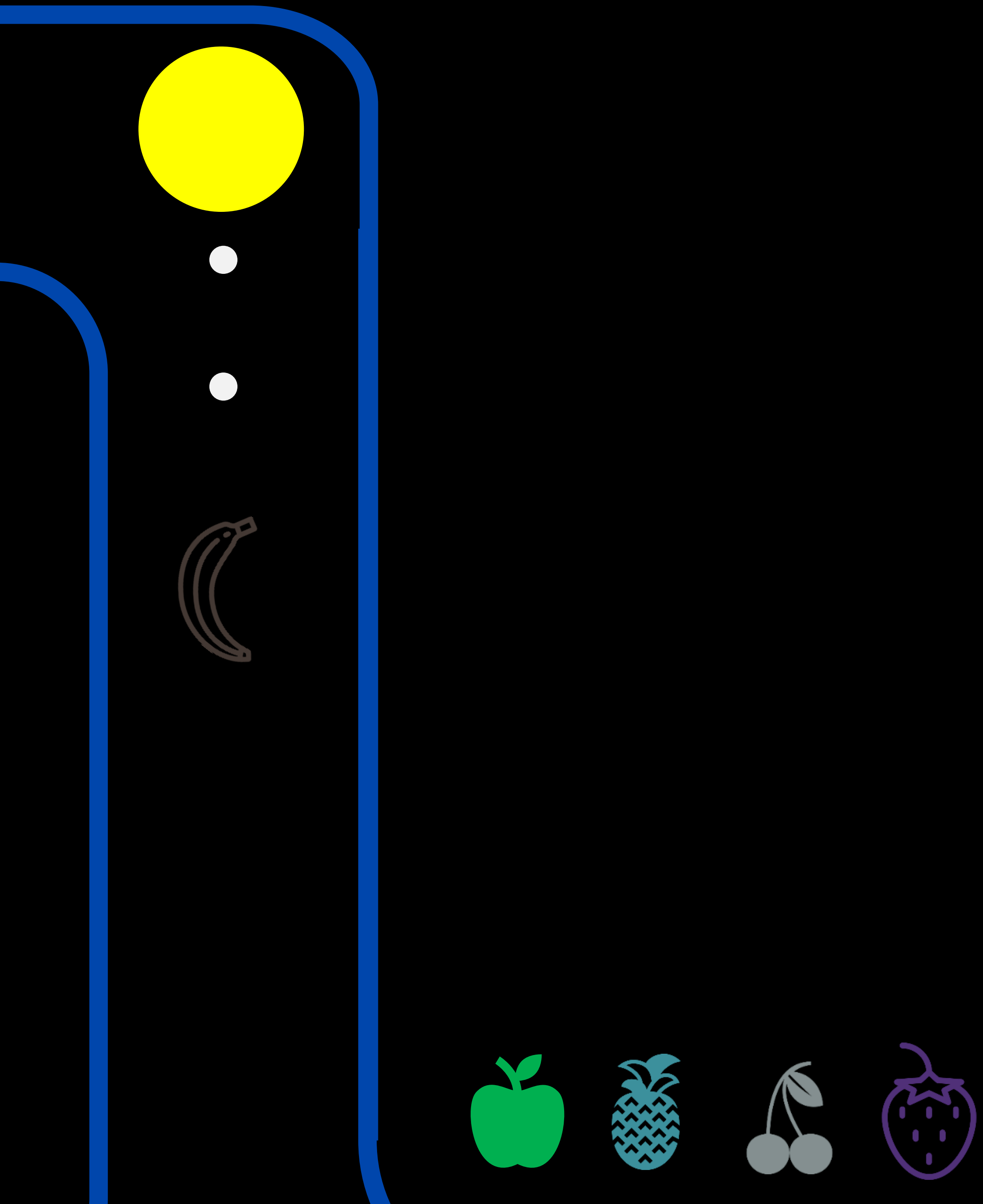
Try to know and control your Windows fleet

1/ Harmonize your fleet database to avoid forgetting systems

Antivirus database : **6 812 computers**
Configuration Management Database (CMDB) : **12 683 computers**
Active Directory Database : **5 000 computers**

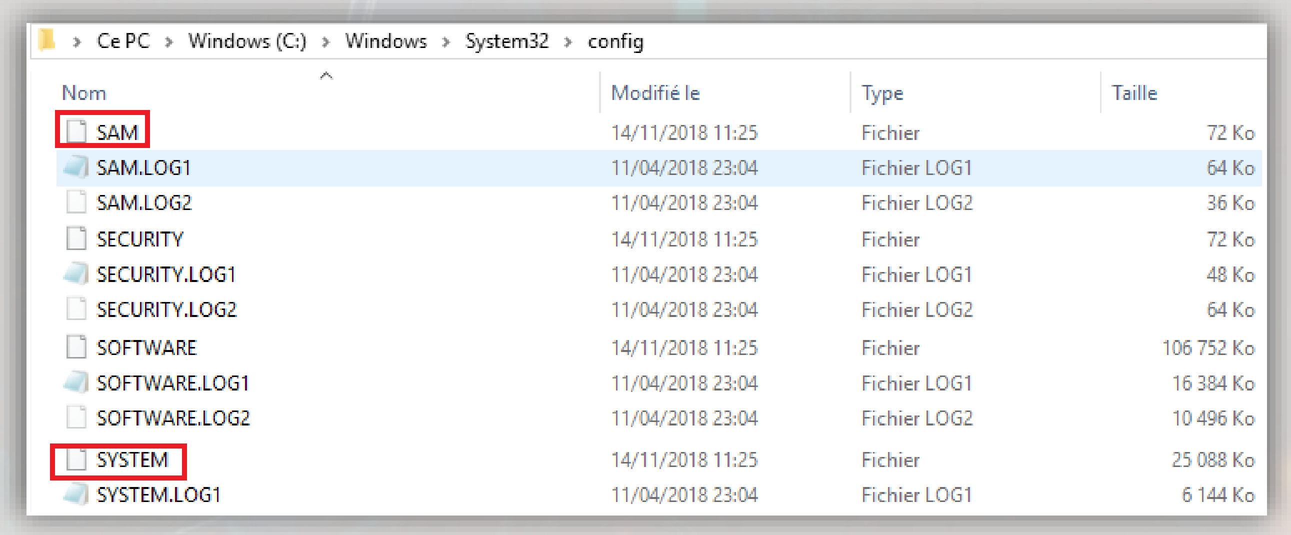
2/ Isolate computers that need "specific requirements"

Can you put them inside a dedicated DMZ ?
Can you put them outside the domain ?
Can you try virtual patching solution ?
…



Pass the hash with local account

- **Local Accounts' NTLM hashes are stored in the registry** in the Security Account Manager (SAM) hive:



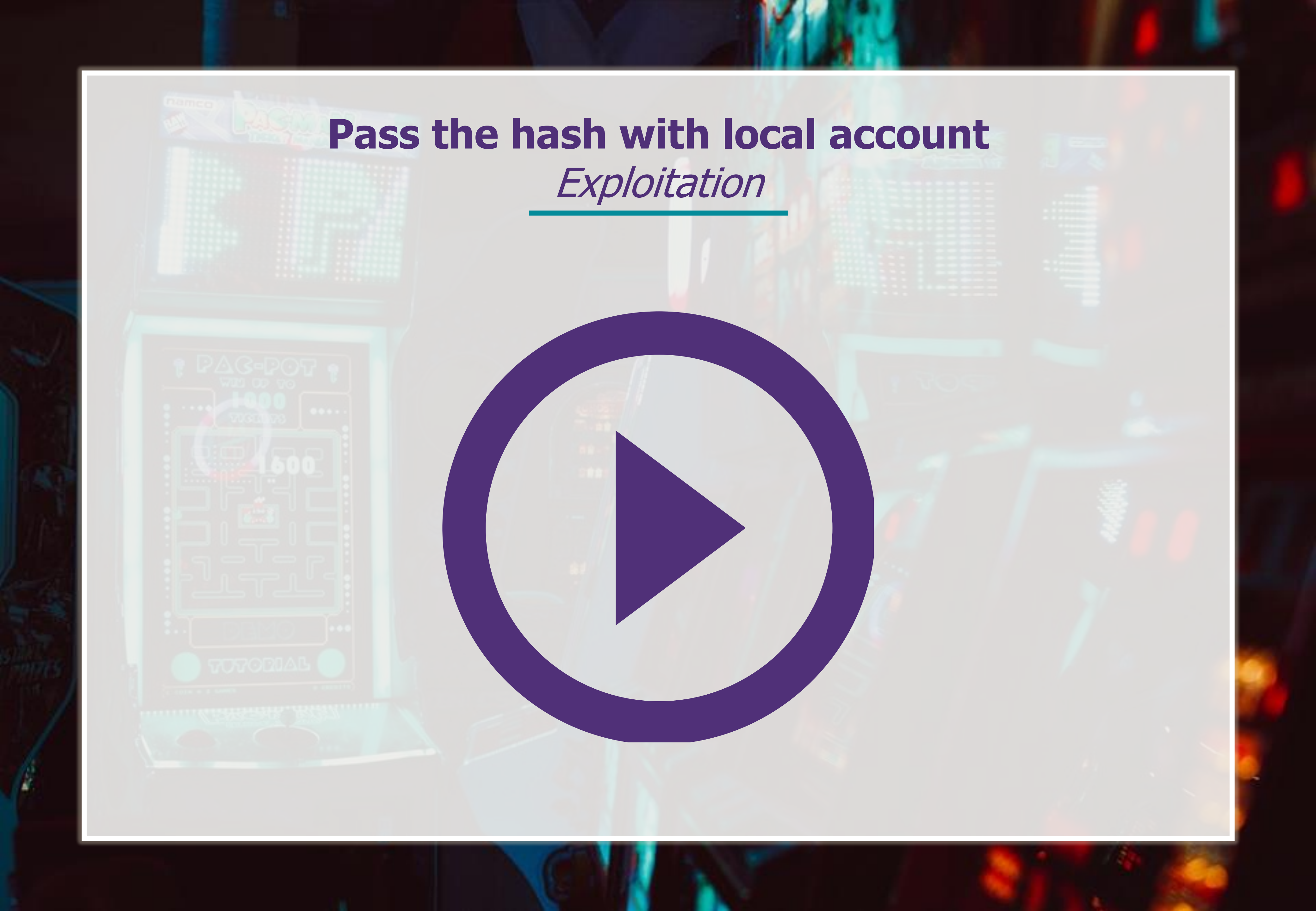
Ce PC › Windows (C:) › Windows › System32 › config

Nom	Modifié le	Type	Taille
SAM	14/11/2018 11:25	Fichier	72 Ko
SAM.LOG1	11/04/2018 23:04	Fichier LOG1	64 Ko
SAM.LOG2	11/04/2018 23:04	Fichier LOG2	36 Ko
SECURITY	14/11/2018 11:25	Fichier	72 Ko
SECURITY.LOG1	11/04/2018 23:04	Fichier LOG1	48 Ko
SECURITY.LOG2	11/04/2018 23:04	Fichier LOG2	64 Ko
SOFTWARE	14/11/2018 11:25	Fichier	106 752 Ko
SOFTWARE.LOG1	11/04/2018 23:04	Fichier LOG1	16 384 Ko
SOFTWARE.LOG2	11/04/2018 23:04	Fichier LOG2	10 496 Ko
SYSTEM	14/11/2018 11:25	Fichier	25 088 Ko
SYSTEM.LOG1	11/04/2018 23:04	Fichier LOG1	6 144 Ko

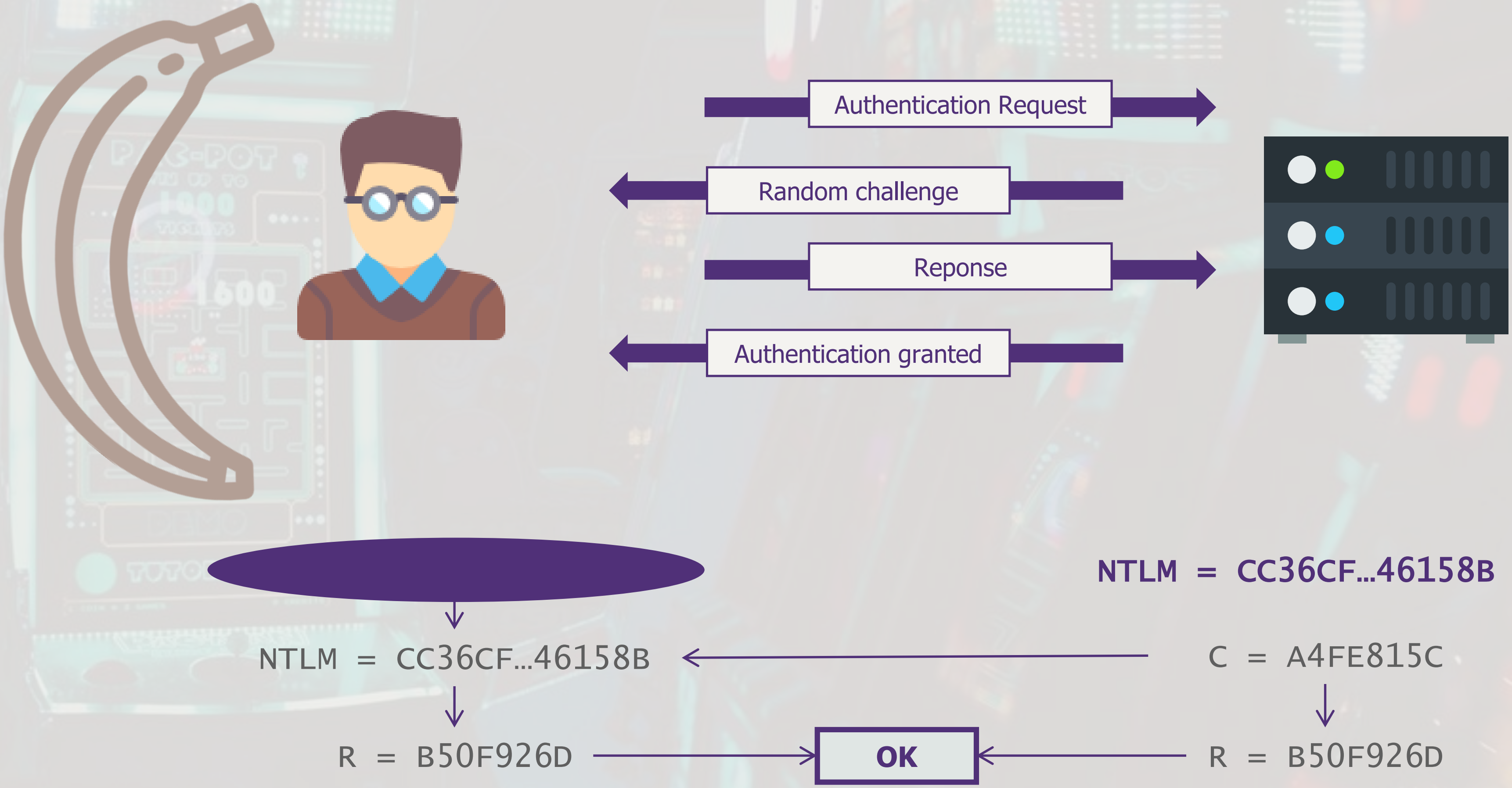
- SYSTEM hive is necessary to decrypt SAM hive

Pass the hash with local account

Exploitation



Pass the hash with local account



Authentication Request

Random challenge

Reponse

Authentication granted

NTLM = CC36CF…46158B

NTLM = CC36CF…46158B

C = A4FE815C

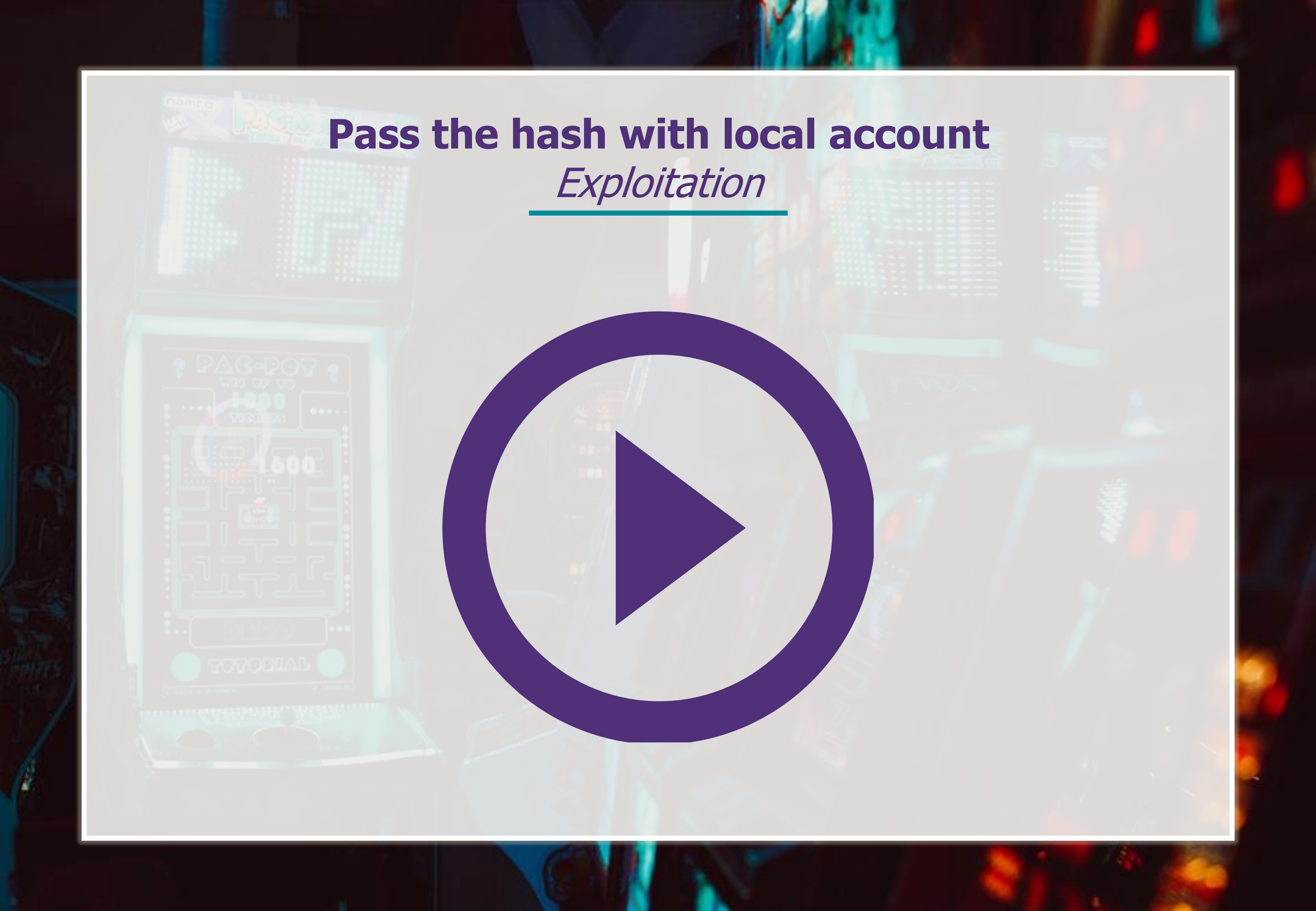
R = B50F926D

OK

R = B50F926D

Pass the hash with local account

Exploitation



Pass the hash with local account

Harden

Deploy Local Admin Password Solution (LAPS)

1/ Install LAPS

Perform an AD schema extension to add 2 attributes on computer object

Create a Group Policy to deploy LAPS on each computer and store the password in AD

Delegate the right to read the password (stores in the AD) to your administrator

Pass the hash with local account

Harden

Deploy Local Admin Password Solution (LAPS)

1/ Install LAPS Management and deploy it with GPO

⚠ **Password will be stored in clear texte inside the "ms-Mcs-AdmPwd" attribute, be careful with your delegation**

https://technet.microsoft.com/en-us/mt227395.aspx
https://flamingkeys.com//deploying-the-local-administrator-password-solution-part-1/

Pass the hash with local account

Harden

Deploy Local Admin Password Solution (LAPS)

1/ Install LAPS Management and deploy it with GPO

Password will be stored in clear texte inside the "ms-Mcs-AdmPwd" attribute, be careful with your delegation

2/ Review all your local administrative account, LAPS only deals with BUILT IN account

3/ Take a look at http://admpwd.com/ to handle password history

https://technet.microsoft.com/en-us/mt227395.aspx
https://flamingkeys.com//deploying-the-local-administrator-password-solution-part-1/

Pass the hash with local account

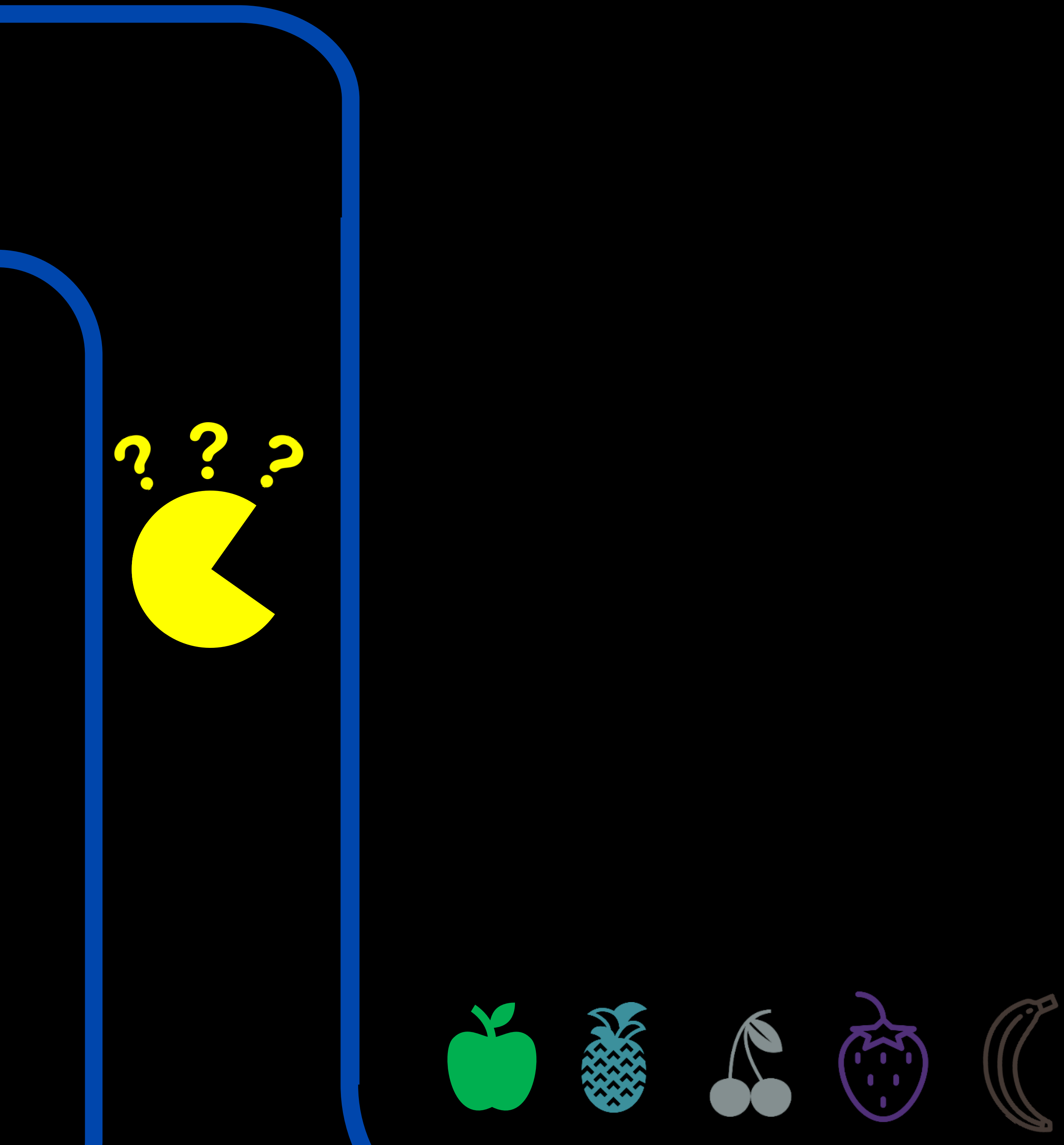
Feedback

EPIC FAIL

IT deploys LAPS on each computer but create a new local administrator with the same password everywhere… Backup you know

STATISTICS

Even if LAPS is deployed, there is always another local account…



Mimikatz

- Windows authentication relies on **credentials providers**:
  - They cache credentials (optionally encrypted) to provide with Single Sign-On (SSO) capabilities
  - The OS must be able to decrypt encrypted credentials in a transparent way for the user
  - Credentials include: cleartext passwords, NTLM hashes, Kerberos TGT & TGS
  - **These credentials are present in the memory of the lsass.exe process**
- Benjamin "gentilkiwi" Delpy has developed the "Mimikatz" tools which runs with local admin privileges and:
  - Requests the "SE_DEBUG" privilege and queries the lsass.exe process memory
  - Relies on Windows API to decrypt encrypted credentials

Mimikatz

⚠

Stay a good guy,

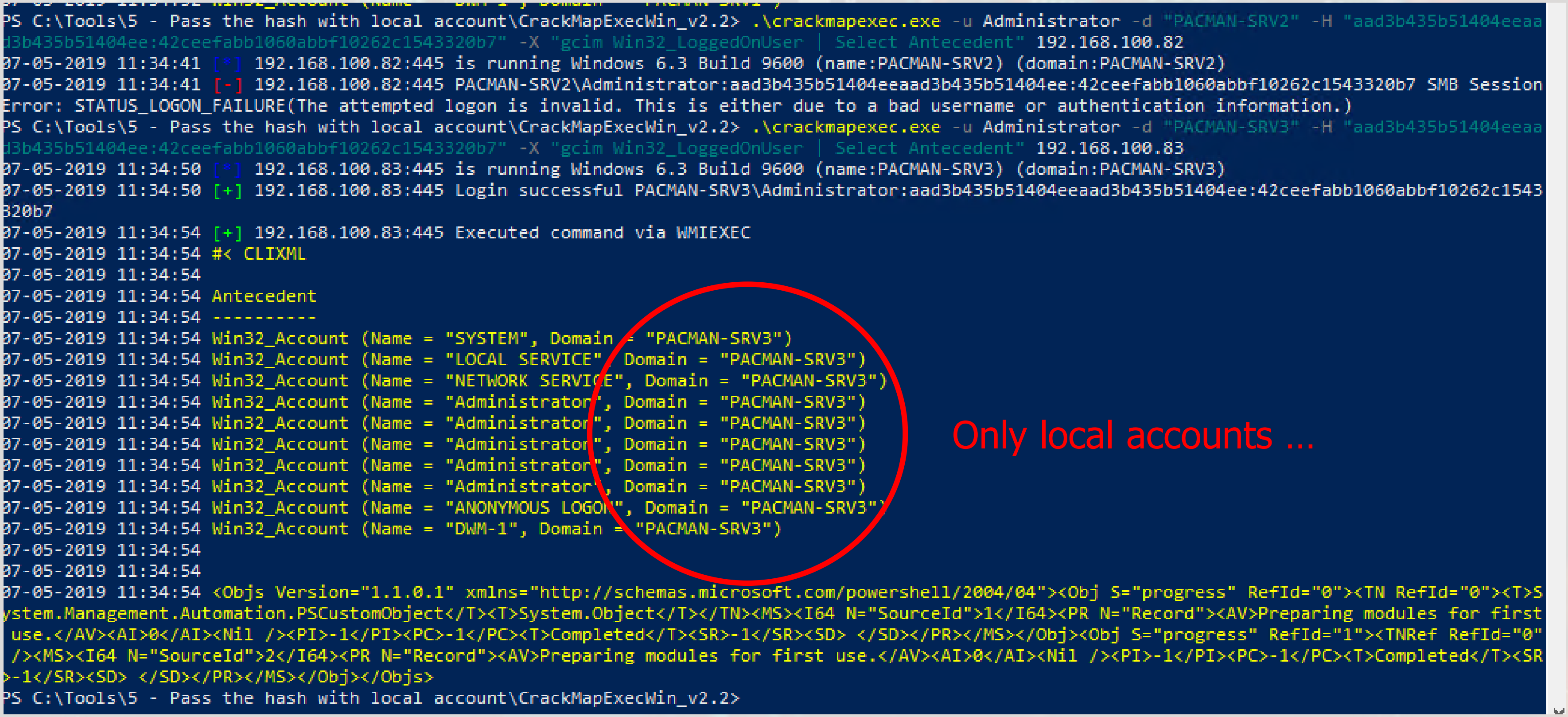
Never launch mimikatz on production

Just dump lsass.exe

And perform offline mimikatz

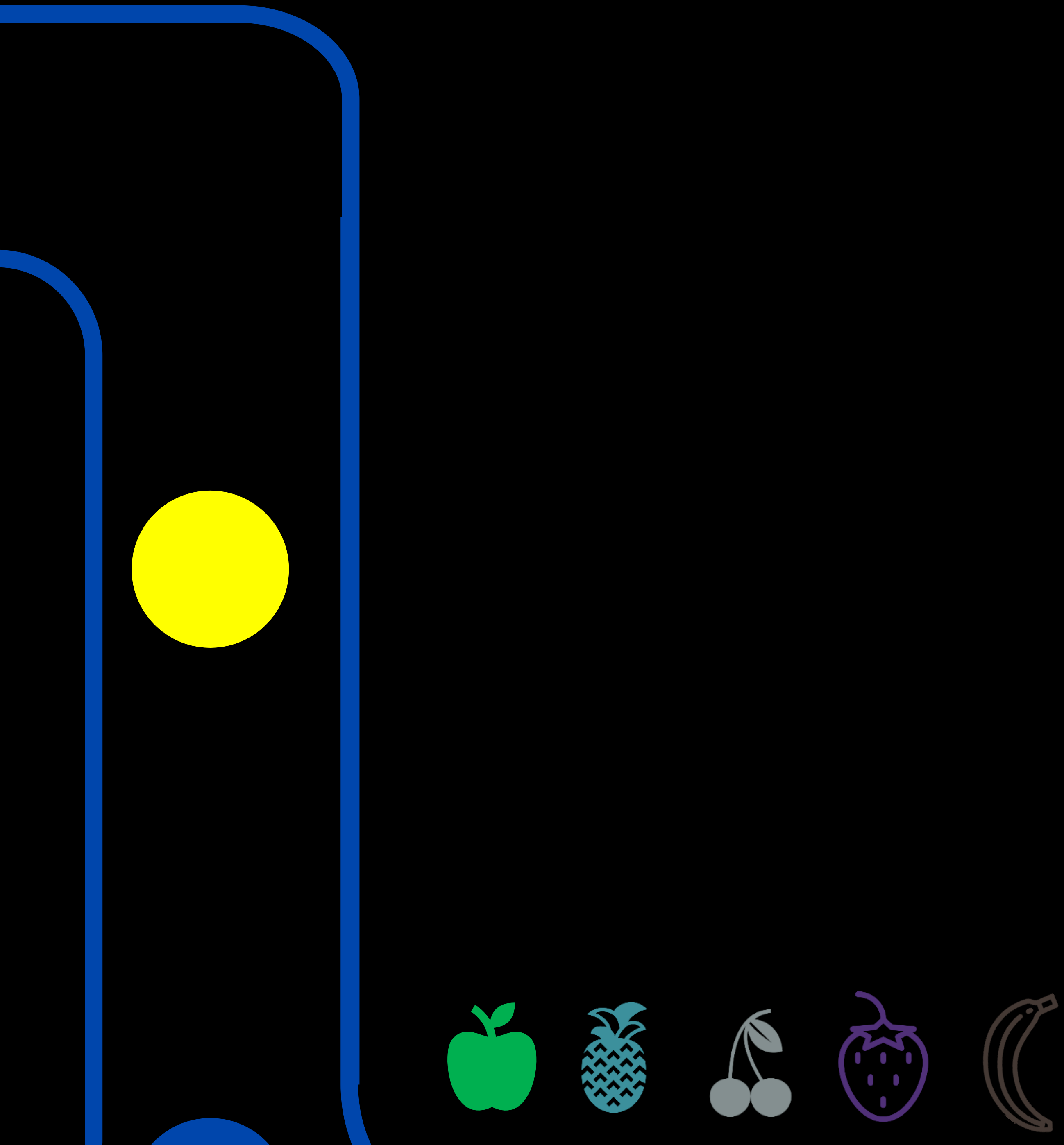
Mimikatz

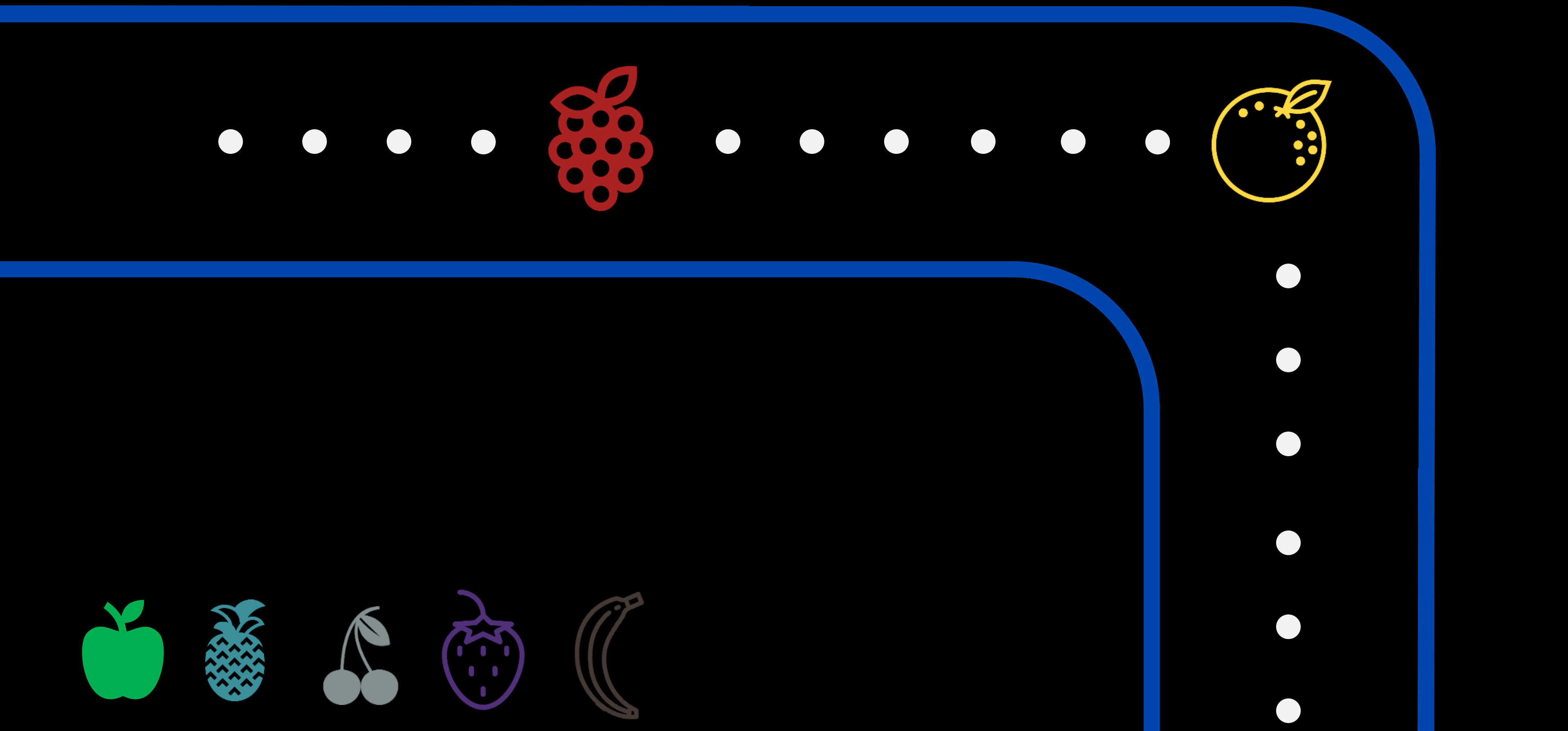
Not yet



```
PS C:\Tools\5 - Pass the hash with local account\CrackMapExecWin_v2.2> .\crackmapexec.exe -u Administrator -d "PACMAN-SRV2" -H "aad3b435b51404eeaad3b435b51404ee:42ceefabb1060abbf10262c1543320b7" -X "gcim Win32_LoggedOnUser | Select Antecedent" 192.168.100.82
07-05-2019 11:34:41 [*] 192.168.100.82:445 is running Windows 6.3 Build 9600 (name:PACMAN-SRV2) (domain:PACMAN-SRV2)
07-05-2019 11:34:41 [-] 192.168.100.82:445 PACMAN-SRV2\Administrator:aad3b435b51404eeaad3b435b51404ee:42ceefabb1060abbf10262c1543320b7 SMB Session Error: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
PS C:\Tools\5 - Pass the hash with local account\CrackMapExecWin_v2.2> .\crackmapexec.exe -u Administrator -d "PACMAN-SRV3" -H "aad3b435b51404eeaad3b435b51404ee:42ceefabb1060abbf10262c1543320b7" -X "gcim Win32_LoggedOnUser | Select Antecedent" 192.168.100.83
07-05-2019 11:34:50 [*] 192.168.100.83:445 is running Windows 6.3 Build 9600 (name:PACMAN-SRV3) (domain:PACMAN-SRV3)
07-05-2019 11:34:50 [+] 192.168.100.83:445 Login successful PACMAN-SRV3\Administrator:aad3b435b51404eeaad3b435b51404ee:42ceefabb1060abbf10262c1543320b7
07-05-2019 11:34:54 [+] 192.168.100.83:445 Executed command via WMIEXEC
07-05-2019 11:34:54 #< CLIXML
07-05-2019 11:34:54
07-05-2019 11:34:54 Antecedent
07-05-2019 11:34:54 ----------
07-05-2019 11:34:54 Win32_Account (Name = "SYSTEM", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "LOCAL SERVICE", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "NETWORK SERVICE", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "Administrator", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "Administrator", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "Administrator", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "Administrator", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "Administrator", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "ANONYMOUS LOGON", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54 Win32_Account (Name = "DWM-1", Domain = "PACMAN-SRV3")
07-05-2019 11:34:54
07-05-2019 11:34:54
07-05-2019 11:34:54 <Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj><Obj S="progress" RefId="1"><TNRef RefId="0" /><MS><I64 N="SourceId">2</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj></Objs>
PS C:\Tools\5 - Pass the hash with local account\CrackMapExecWin_v2.2>
```

Only local accounts ...





Spot Domain Admins

- **Enumerate workstation information from a remote host without administrative privilege**

  Local Group and Local Group Member

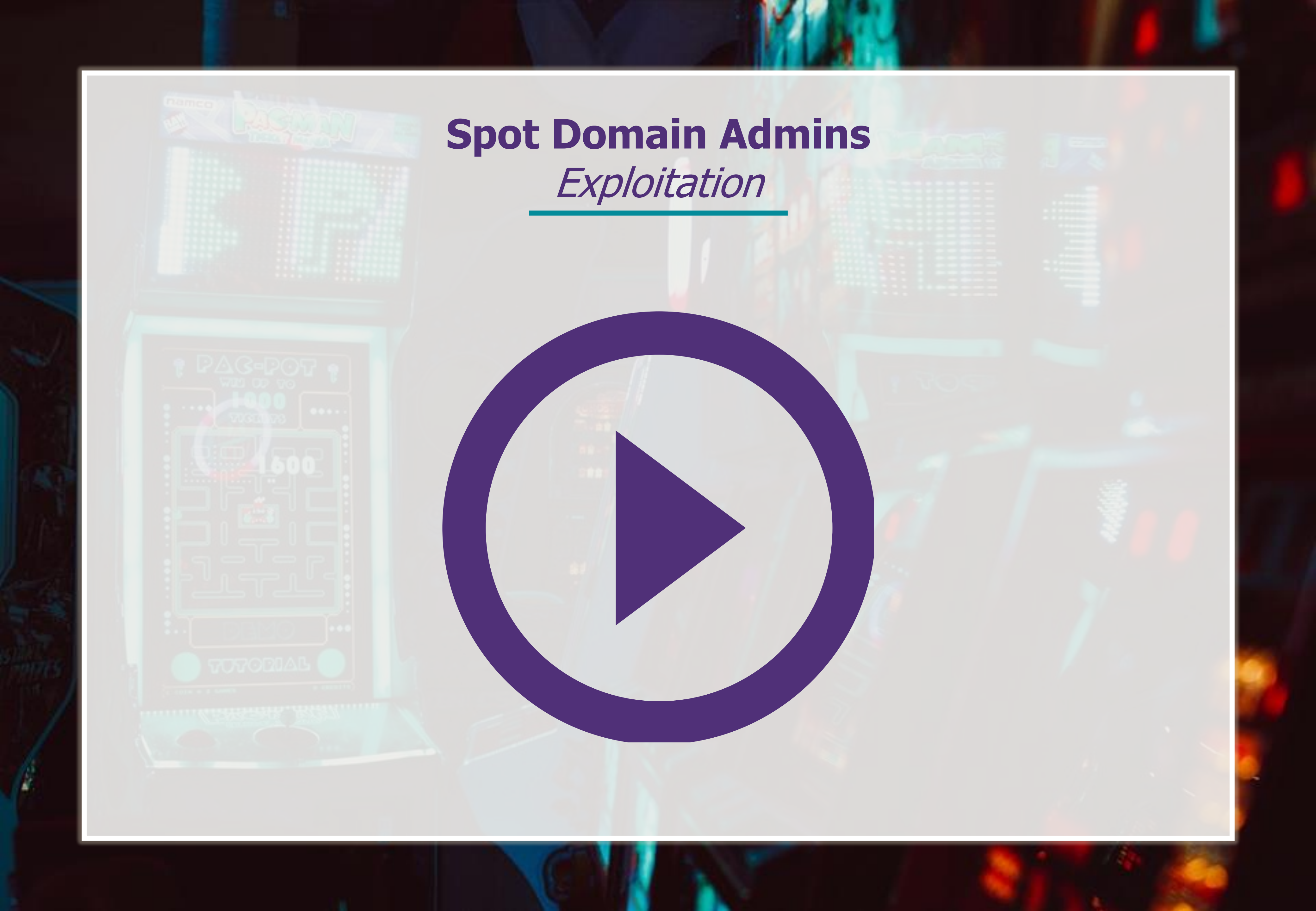
  Shares

  SMB sessions

  Windows version

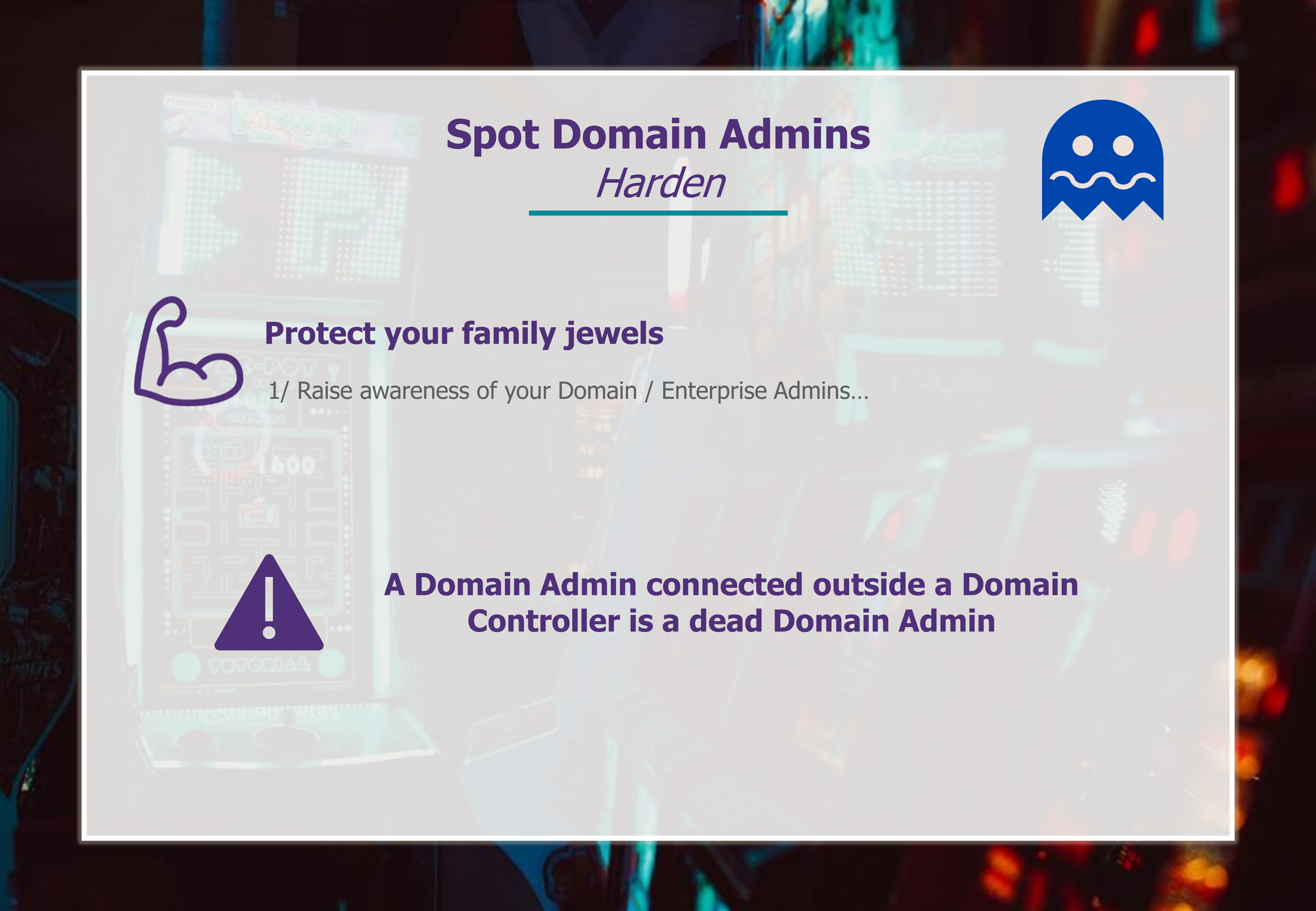
  Windows last reboot time

- Working thanks to netapi library



Spot Domain Admins

Exploitation



Spot Domain Admins

Harden

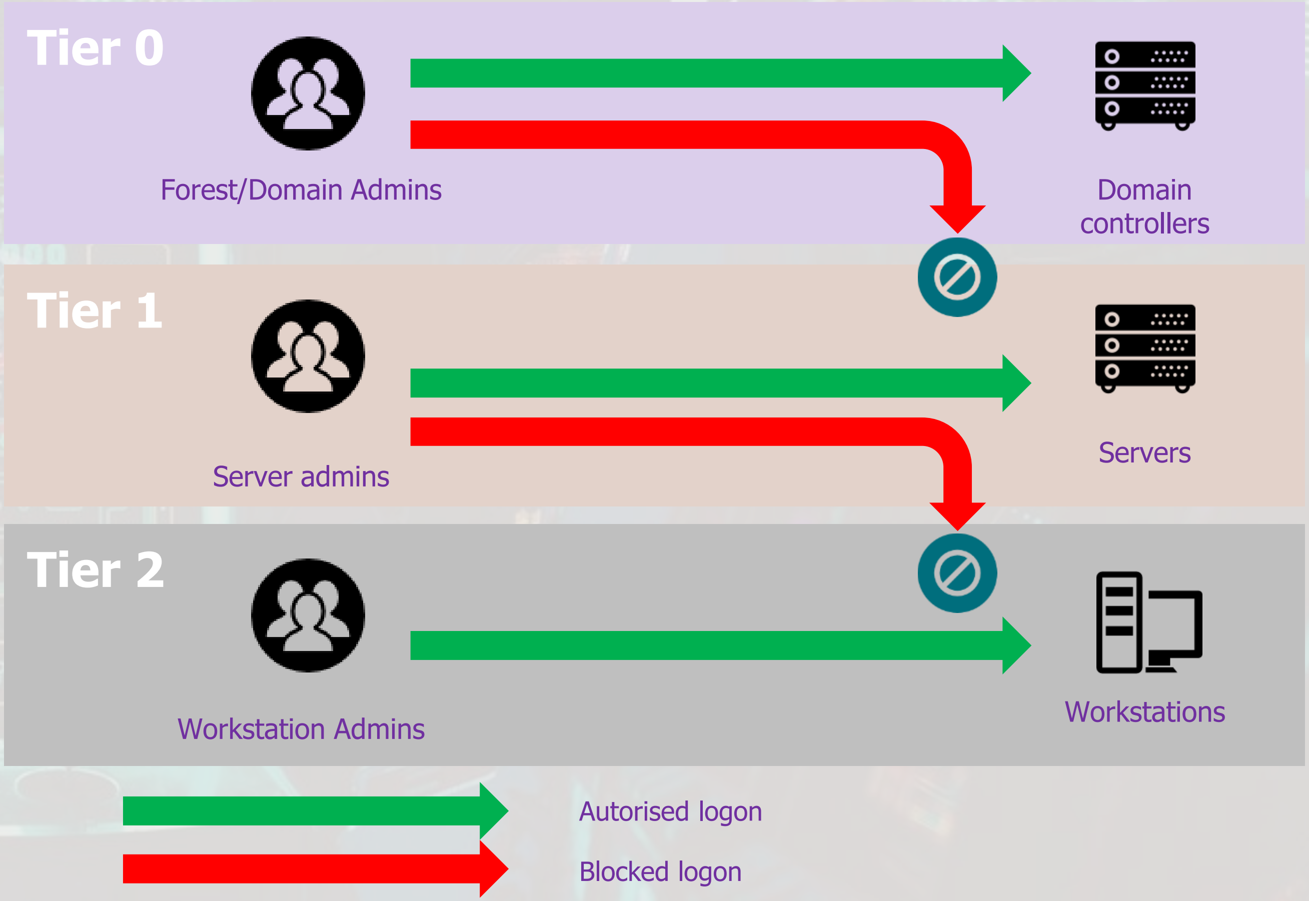
Protect your family jewels

1/ Raise awareness of your Domain / Enterprise Admins…

⚠ **A Domain Admin connected outside a Domain Controller is a dead Domain Admin**

Spot Domain Admins

Harden



https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Spot Domain Admins

Harden

Protect your family jewels

1/ Raise awareness of your Domain / Enterprise Admins…

2/ Remove Domain Admins from local administrative groups

3/ Deploy dedicated workstation (without Internet access)

4/ Deny access / log on for Domain Admins (EA…) everywhere outside Tier 0

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Spot Domain Admins

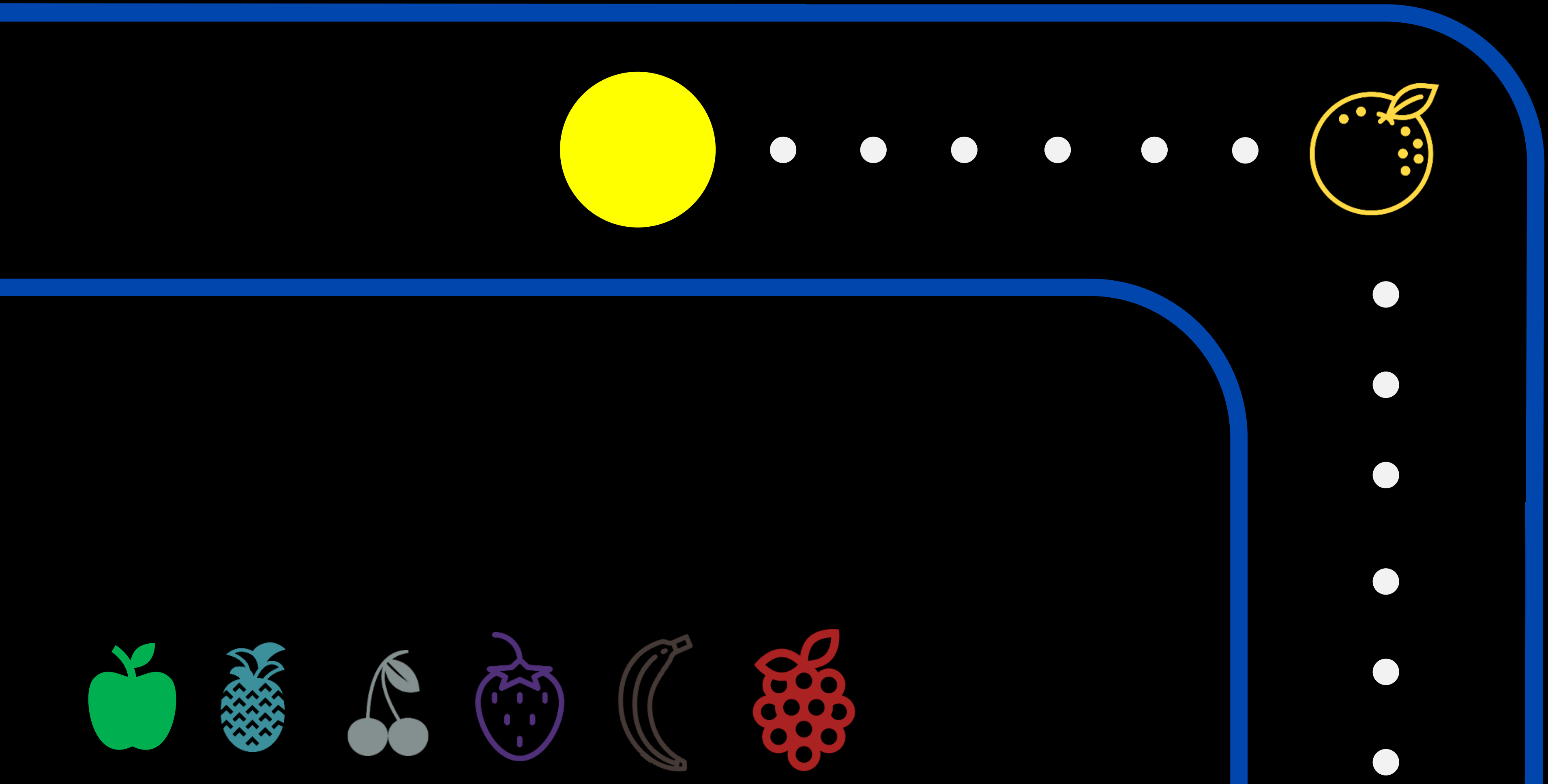
Feedback

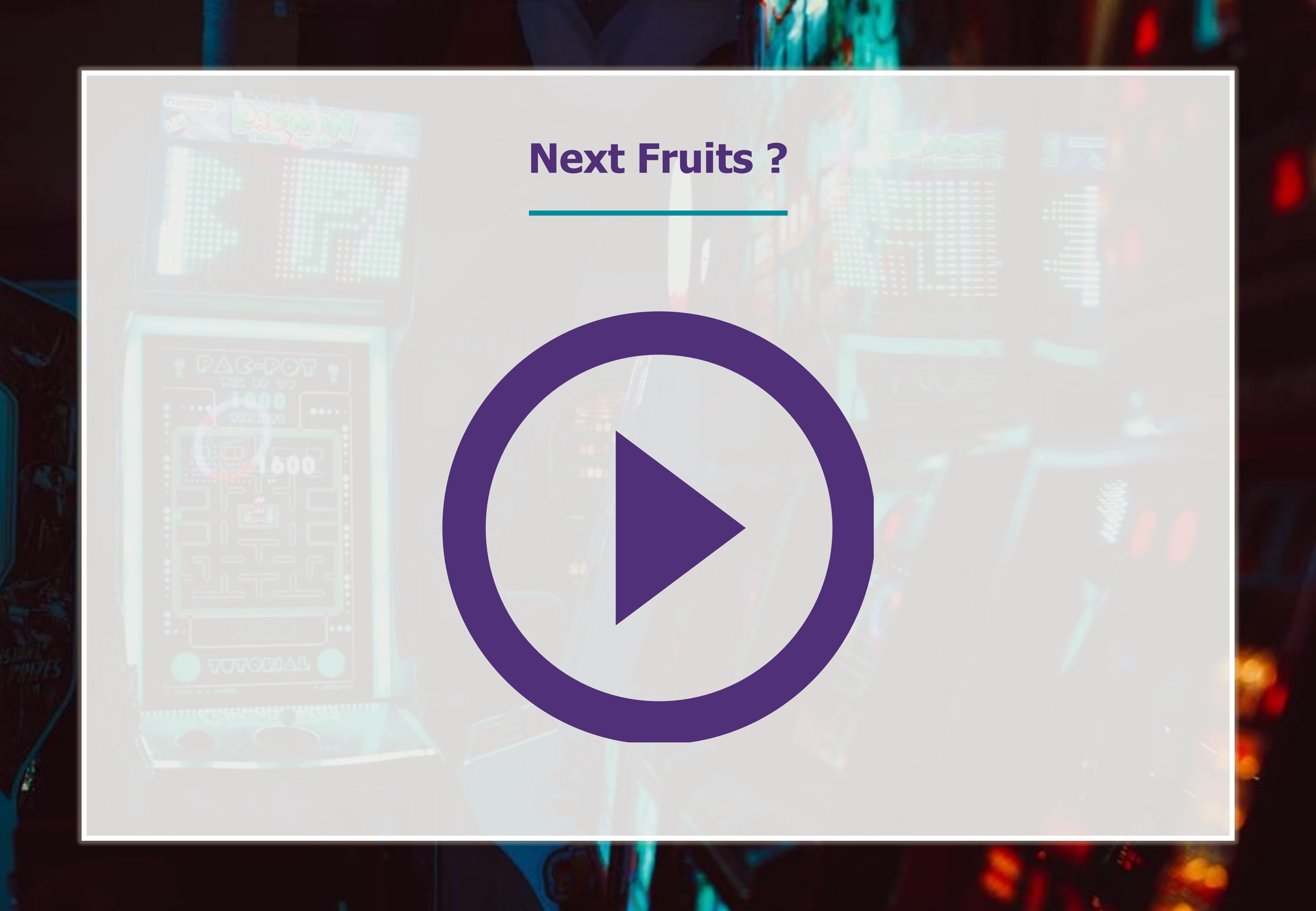
EPIC FAIL

Authenticated scan with Nessus on Windows workstation with Domain Admins creds each week

WE NEED YOU

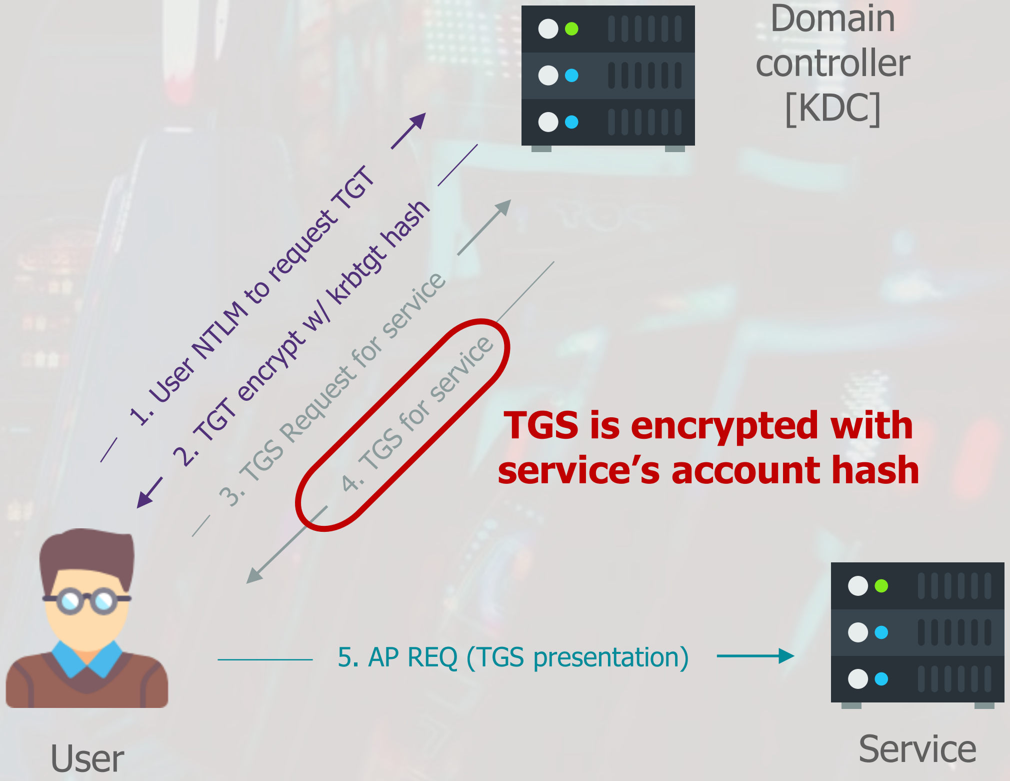
Tier 0 is the FIRST recommendation to deploy, if not everything else is useless





Next Fruits ?

Targeted Kerberoasting


Domain controller [KDC]
1. User NTLM to request TGT
2. TGT encrypt w/ krbtgt hash
3. TGS Request for service
4. TGS for service
TGS is encrypted with service's account hash
5. AP REQ (TGS presentation)
User
Service

Targeted Kerberoasting

Exploitation

Targeted Kerberoasting

Exploitation

Targeted Kerberoasting

Harden & Trap

Define a fine grained password policy for user account with a ServicePrincipalName

1/ Create a group with all user defined with a ServicePrincipalName

2/ Apply a really strong password policy on this group: min 25 characters

Set a user honeypot

1/ Create a decoy user with a ServicePrincipalName (SPN)

2/ Detect when a Kerberoast service ticket (TGS) was requested or renewed
Events ID 4769 and 4770

Targeted Kerberoasting

Check the Trap

Targeted Kerberoasting

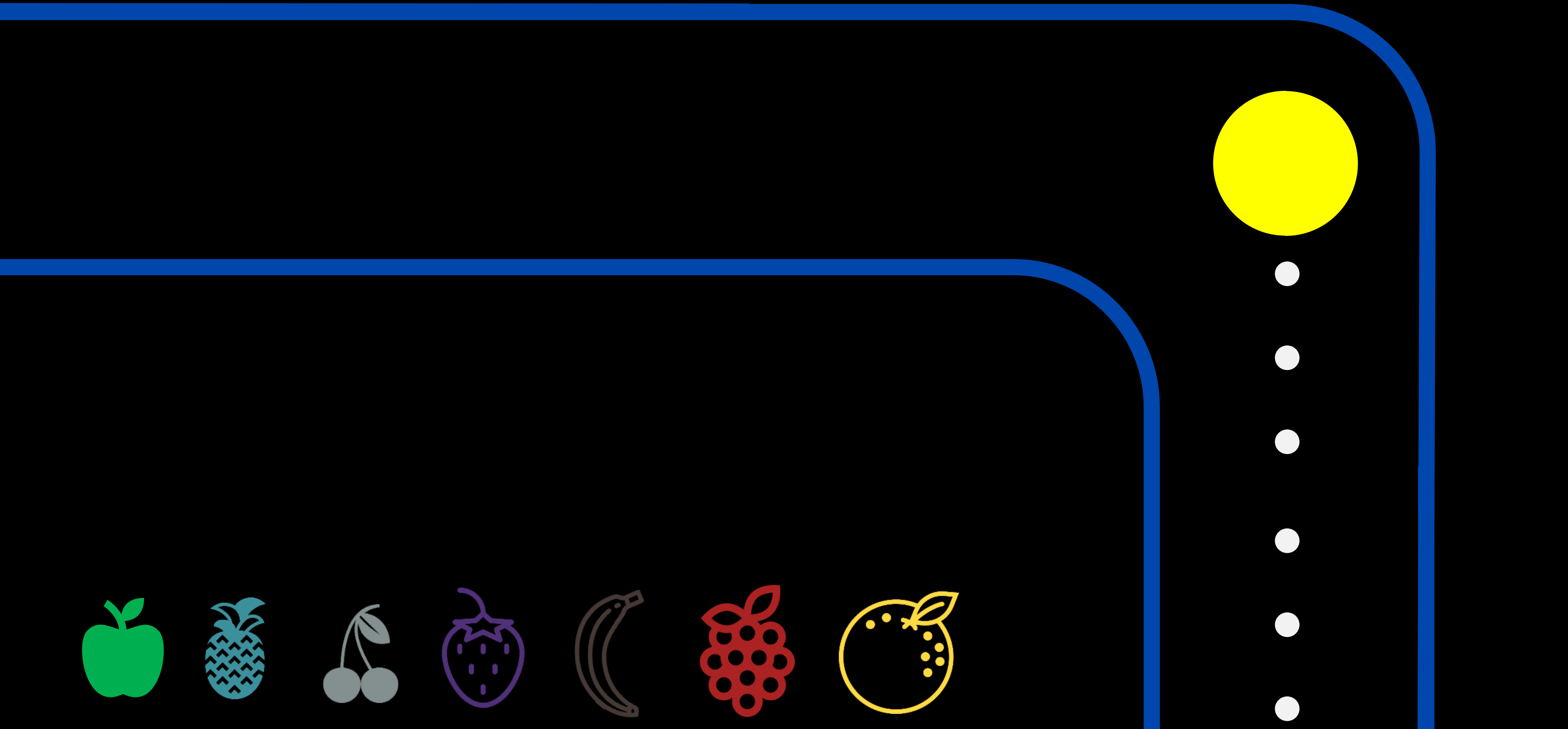
Feedback

EPIC FAIL

A **Service Principal Name** was defined on **built'in Administrator** (SID 500), easy win

STATISTICS

30 % of the time, we are able to crack the TGS



I saw your
credentials!
mimikatz

Mimikatz

Exploitation

WINNER !

Mimikatz

Harden & Detect

⚠

A Domain Admin connected outside a Domain Controller is a dead Domain Admin

Don’t try to detect a tool …

Educate your Admin !

Mimikatz

Harden & Detect

https://twitter.com/gentilkiwi/status/1152650531845877762

Mimikatz

Harden & Detect

“Try” to detect Mimikatz or lsass.exe accesses

1/ Identify processes that interact with LSASS : For example In Windows 10, a default process SACL was added to LSASS.exe to log processes attempting to access LSASS.exe

2/ Enable PowerShell Module Logging / Whitelisting / …

Activate Virtual Secure Mode in your W10 / WS2016

1/ Migrate all your asset in W10 or WS2016 operating system

2/ Active Virtual Secure Mode

Mimikatz
Feedback

EPIC FAIL

Previous Red Team operations let a “mimikatz” executable on production server, **easy to re-use**

STATISTICS

When **Wdigest** is set to 1, the **password** is stored in **clear-text** in memory

Mimikatz

Detection attempts

⚠ **Be careful with false positives!!!**

Can we do it faster ?

Do you like SpeedRun ?

BloodHound

Six Degrees of Domain Admin

BLOODHOUND

Opensource tool permitting to automatically discover compromise paths in an Active Directory environment

The compromise paths research using BloodHound requires three steps:

1/ Extraction of the information using a C# executable

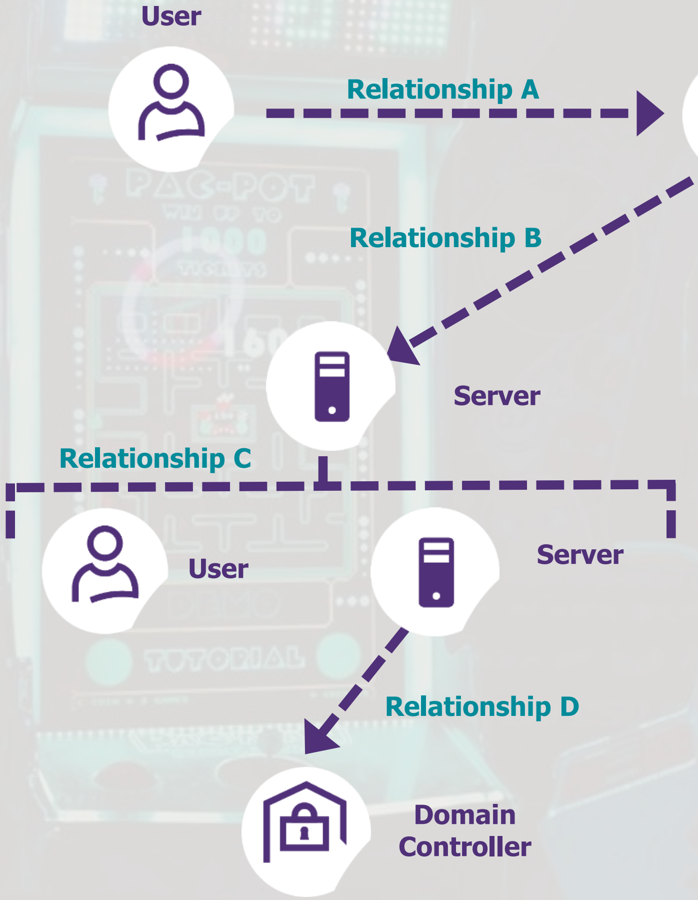
2/ Import of these information in the tool database

3/ Analysis of the results in regard of the context

https://github.com/BloodHoundAD/BloodHound

BloodHound

Six Degrees of Domain Admin



BloodHound creates a graph to reveal relationship between Active Directory object:

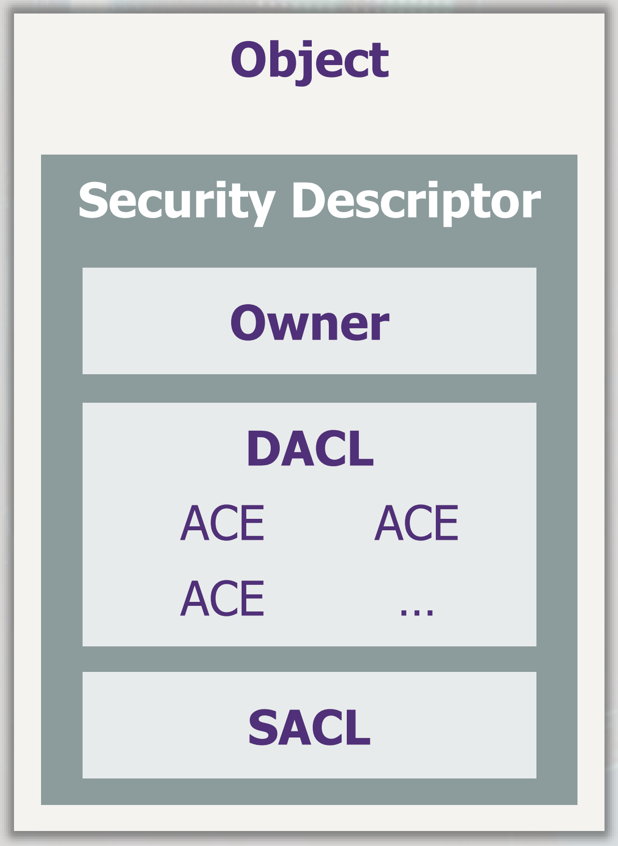
Local privilege on a computer : administrator / can RDP / COM execute

Domain privilege on an object through ACL / GPO / group membership

And many more …

BloodHound

What is an ACL ?



Object

Security Descriptor

Owner

DACL

ACE ACE

ACE …

SACL

- All **securable objects** in Windows (including Active Directory) have a **Security Descriptor**

- A **Security Descriptor** contains :

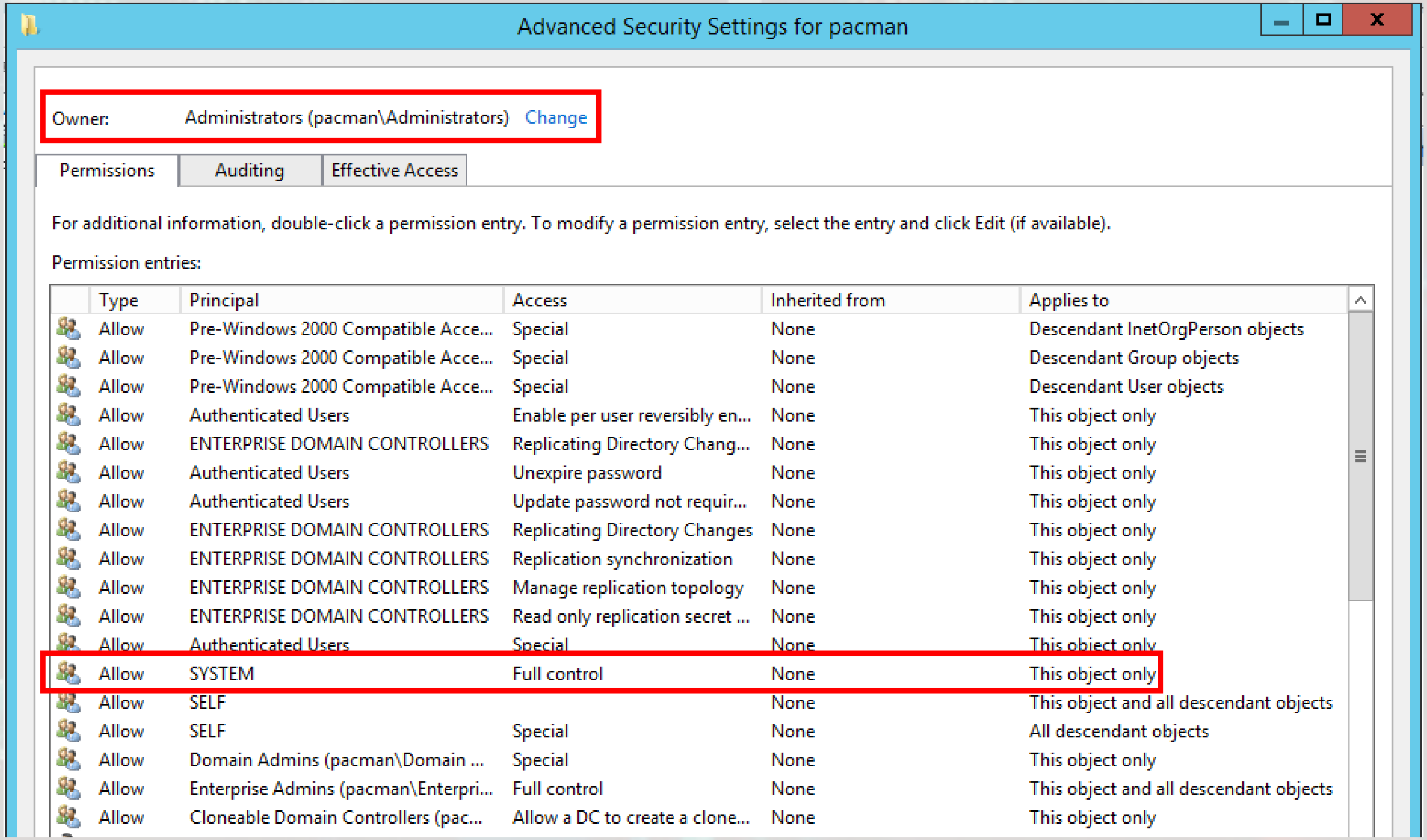
Owner : by default the creating user

DACL : specifies the access rights (an ACE) allowed or denied to particular users or groups.

SACL : specifies the types of access attempts that generate audit records for the object.

BloodHound

What is an ACL ?



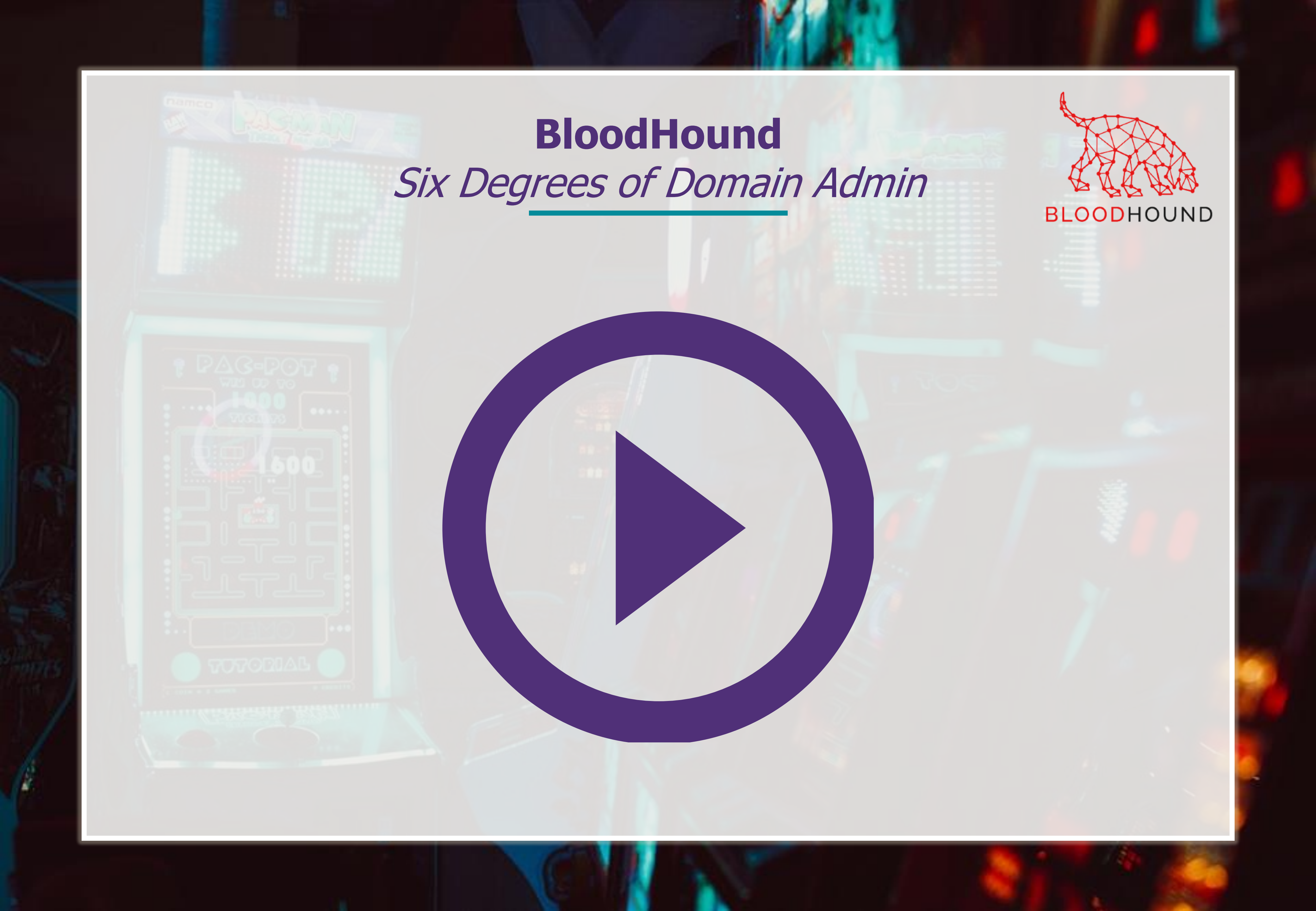
Advanced Security Settings for pacman

Owner: Administrators (pacman\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Pre-Windows 2000 Compatible Acce...	Special	None	Descendant InetOrgPerson objects
Allow	Pre-Windows 2000 Compatible Acce...	Special	None	Descendant Group objects
Allow	Pre-Windows 2000 Compatible Acce...	Special	None	Descendant User objects
Allow	Authenticated Users	Enable per user reversibly en...	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Replicating Directory Chang...	None	This object only
Allow	Authenticated Users	Unexpire password	None	This object only
Allow	Authenticated Users	Update password not requir...	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Replicating Directory Changes	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Replication synchronization	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Manage replication topology	None	This object only
Allow	ENTERPRISE DOMAIN CONTROLLERS	Read only replication secret ...	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	SELF		None	This object and all descendant objects
Allow	SELF	Special	None	All descendant objects
Allow	Domain Admins (pacman\Domain ...	Special	None	This object only
Allow	Enterprise Admins (pacman\Enterpri...	Full control	None	This object and all descendant objects
Allow	Cloneable Domain Controllers (pac...	Allow a DC to create a clone...	None	This object only



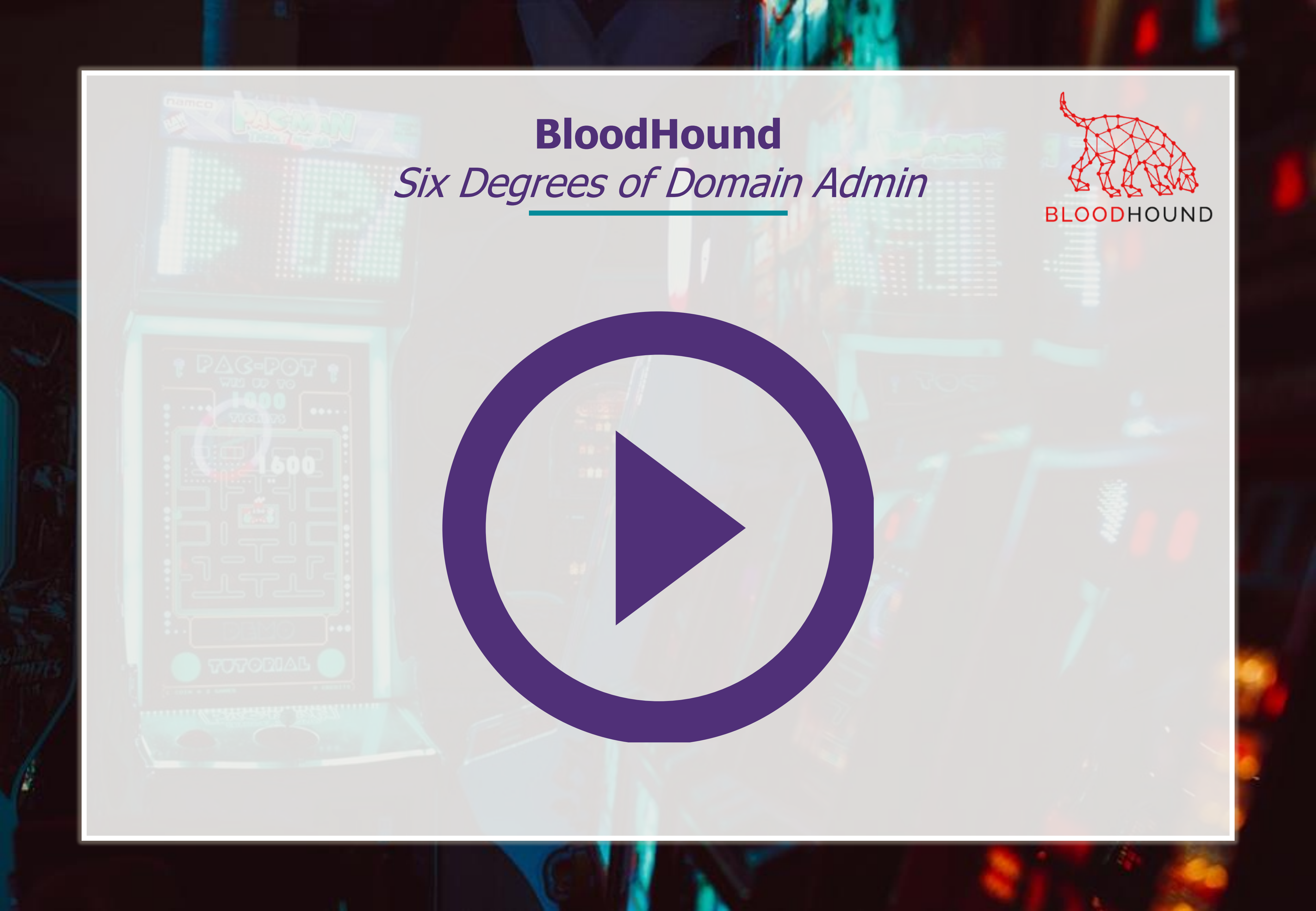
BloodHound

Six Degrees of Domain Admin

BloodHound

Six Degrees of Domain Admin

BLOODHOUND



BloodHound

LAPS return

- **LAPS will store the Administrator password in clear text inside the “ms-Mcs-AdmPwd” attribute**
- Be careful when **delegate the right to read the password** (stores in the AD) to users

BloodHound

LAPS - Exploitation

BloodHound

DCSync / DCShadow

- **Major feature added to Mimkatz is "DCSync" which effectively "impersonates" a Domain Controller and requests account password data from the targeted Domain Controller**

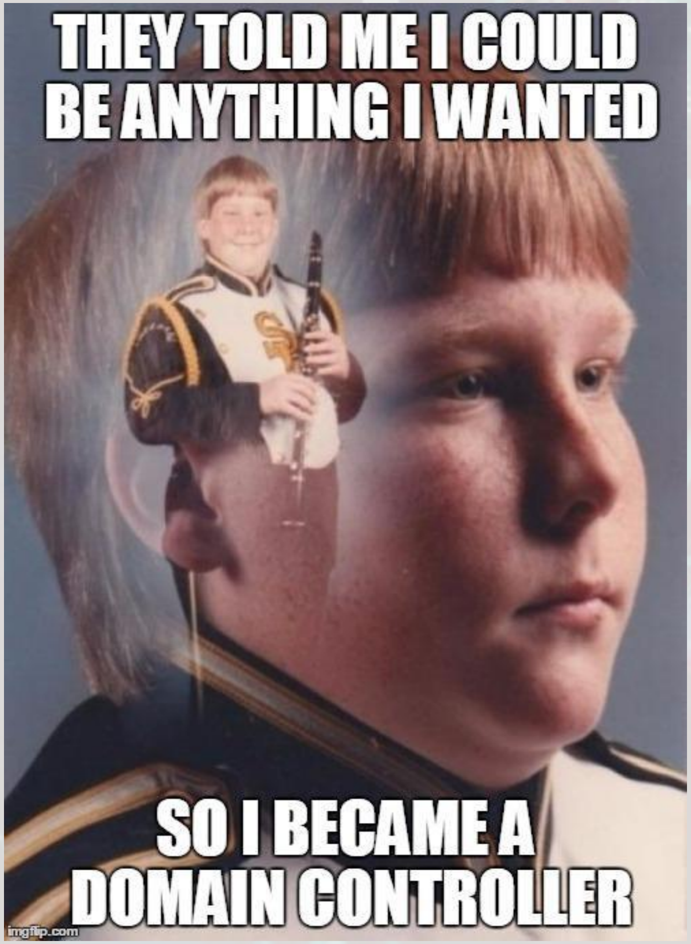
- Two privileges need

  Replicating Directory Changes (DS-Replication-Get-Changes)

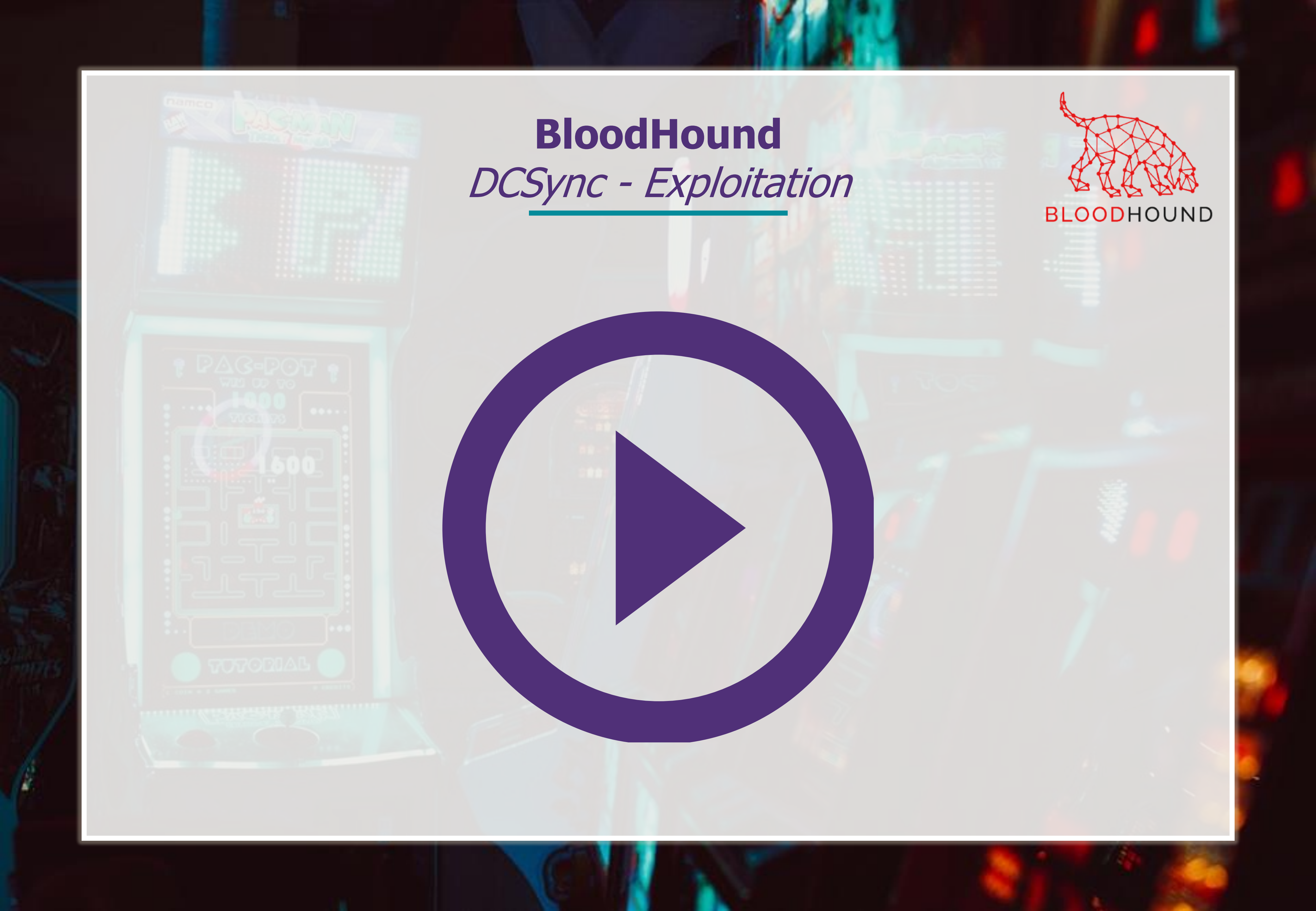
  Replicating Directory Changes All (DS-Replication-Get-Changes-All)

BloodHound

DCSync / DCShadow


THEY TOLD ME I COULD BE ANYTHING I WANTED
SO I BECAME A DOMAIN CONTROLLER
imgflip.com

https://www.dcshadow.com/



BloodHound

DCSync - Exploitation

BloodHound

DCSync – a direct link to Golden ticket

Kiwi's

GOLDEN TICKET

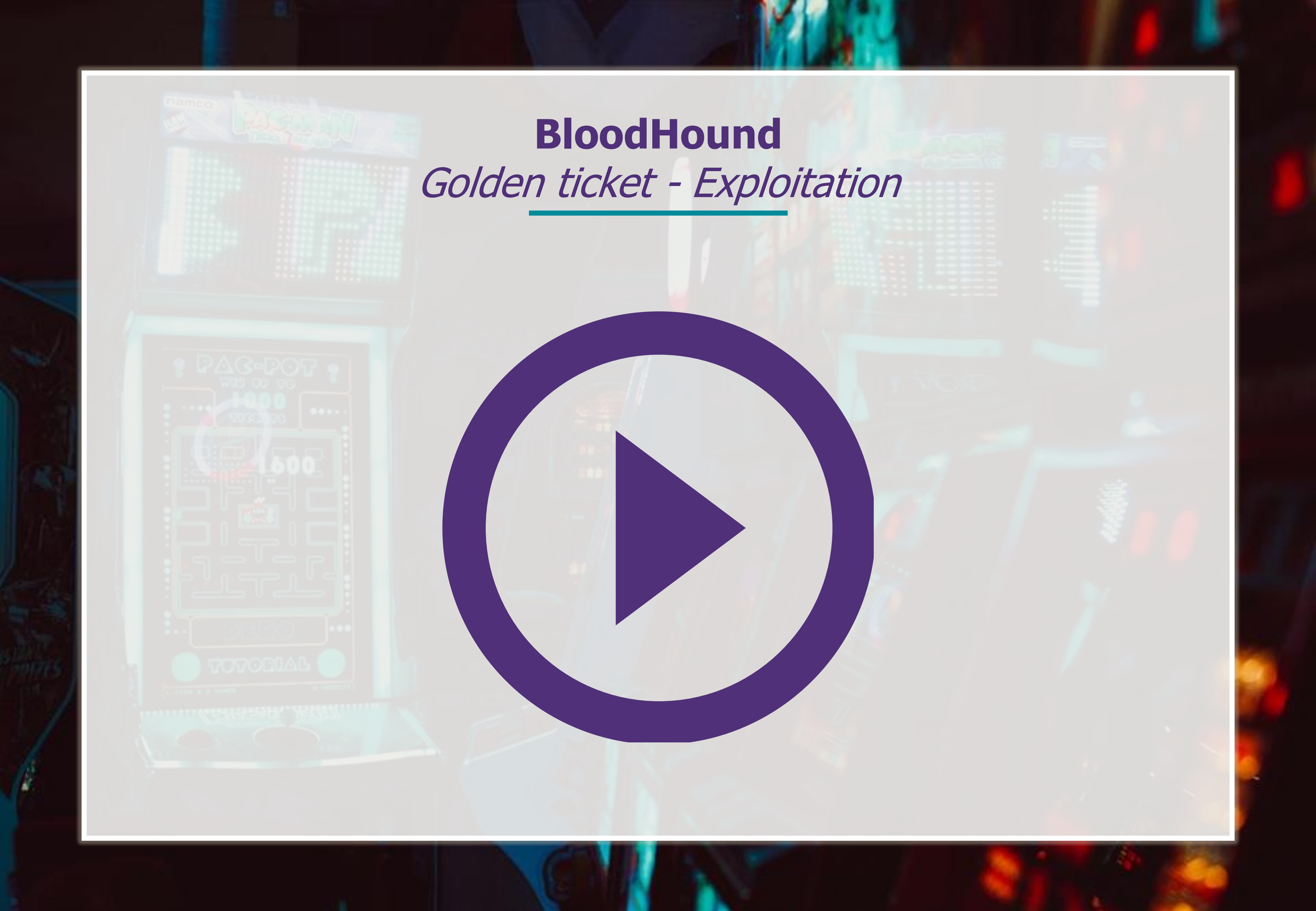
GREETINGS TO YOU, THE LUCKY FINDER OF THIS GOLDEN TICKET!...

PRESENT THIS TICKET TO THE KEY DISTRIBUTION CENTER WHEN YOU WANT...
YOU CAN BE LATE, AND YOU MAY BRING WITH YOU **mimikatz**!
In your wildest dreams you could not imagine the marvelous RIGTHS that await YOU!

- The Kerberos authentication is based on the **KRBTGT password account**
- **The KRBTGT password permits to craft any TGT**
- A Golden Ticket is a craft TGT (valid 10 years) that gives a total and complete access to the domain

BloodHound

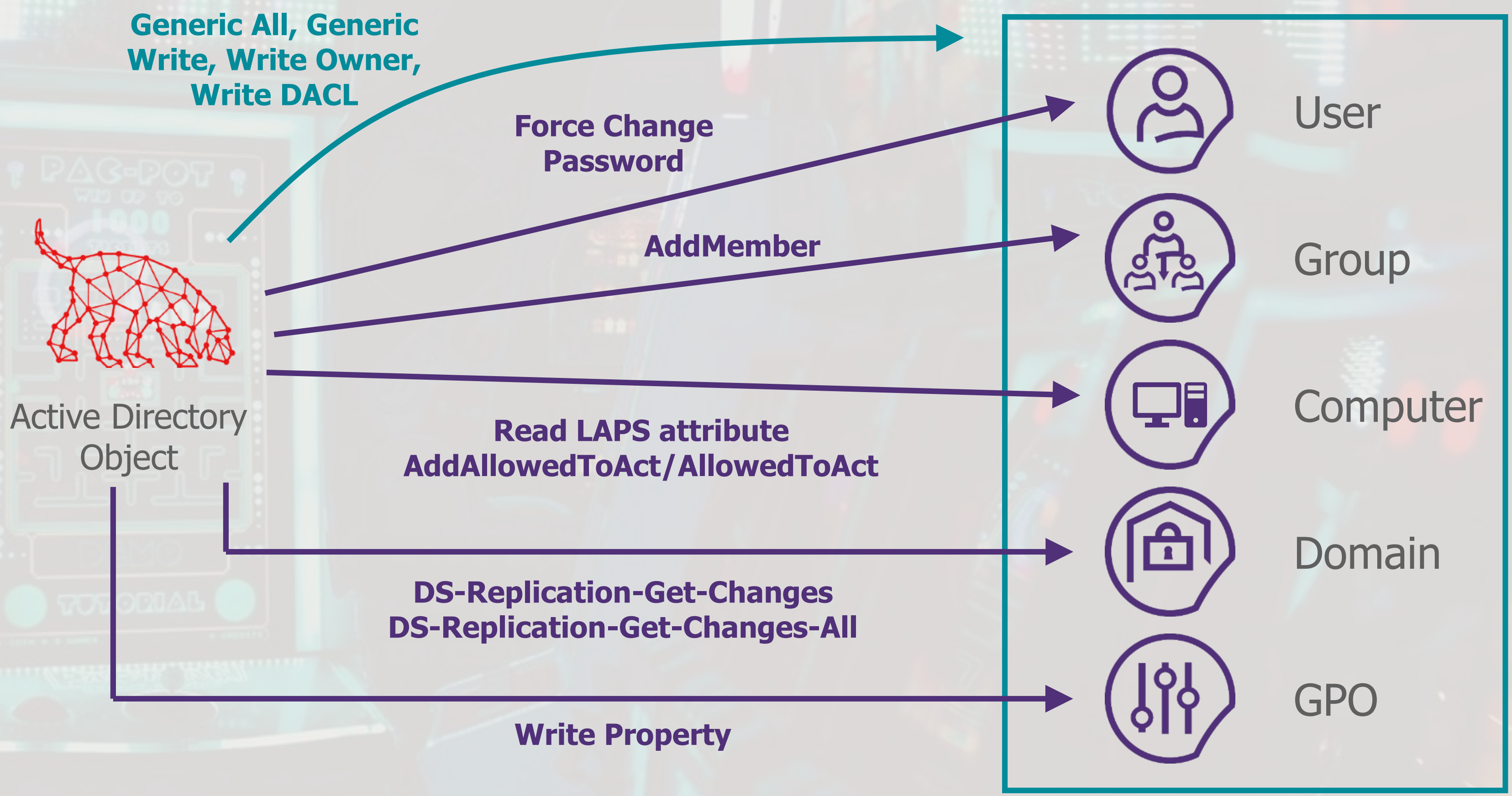
Golden ticket - Exploitation



BloodHound

Active Directory rights overview

BLOODHOUND



Generic All, Generic Write, Write Owner, Write DACL

Force Change Password

AddMember

Read LAPS attribute
AddAllowedToAct/AllowedToAct

DS-Replication-Get-Changes
DS-Replication-Get-Changes-All

Write Property

Active Directory Object

User

Group

Computer

Domain

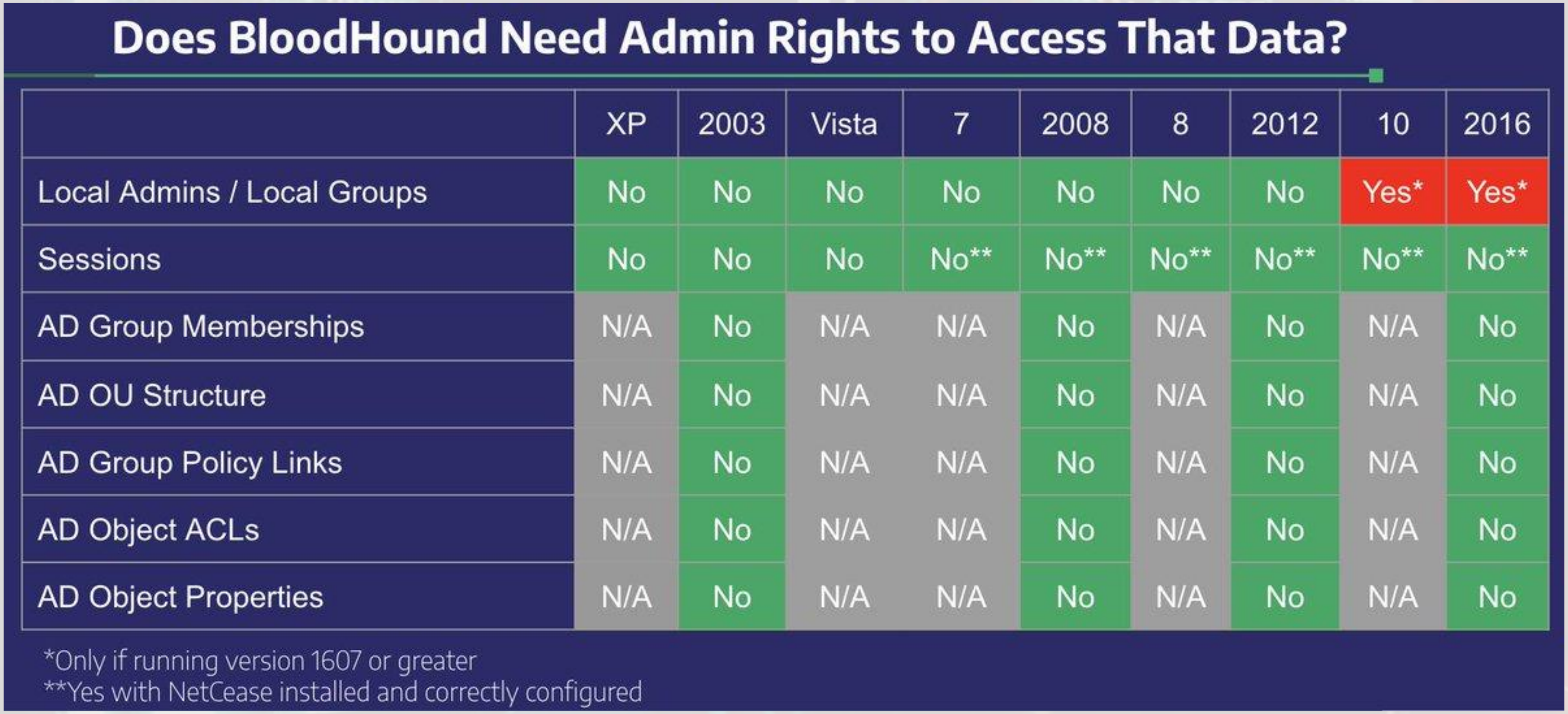
GPO

https://specterops.io/assets/resources/an_ace_up_the_sleeve.pdf

BloodHound

Six Degrees of Domain Admin

BLOODHOUND



Does BloodHound Need Admin Rights to Access That Data?

	XP	2003	Vista	7	2008	8	2012	10	2016
Local Admins / Local Groups	No	No	No	No	No	No	No	Yes*	Yes*
Sessions	No	No	No	No**	No**	No**	No**	No**	No**
AD Group Memberships	N/A	No	N/A	N/A	No	N/A	No	N/A	No
AD OU Structure	N/A	No	N/A	N/A	No	N/A	No	N/A	No
AD Group Policy Links	N/A	No	N/A	N/A	No	N/A	No	N/A	No
AD Object ACLs	N/A	No	N/A	N/A	No	N/A	No	N/A	No
AD Object Properties	N/A	No	N/A	N/A	No	N/A	No	N/A	No

*Only if running version 1607 or greater

**Yes with NetCease installed and correctly configured

https://twitter.com/_wald0/status/1103756044986171394

BloodHound

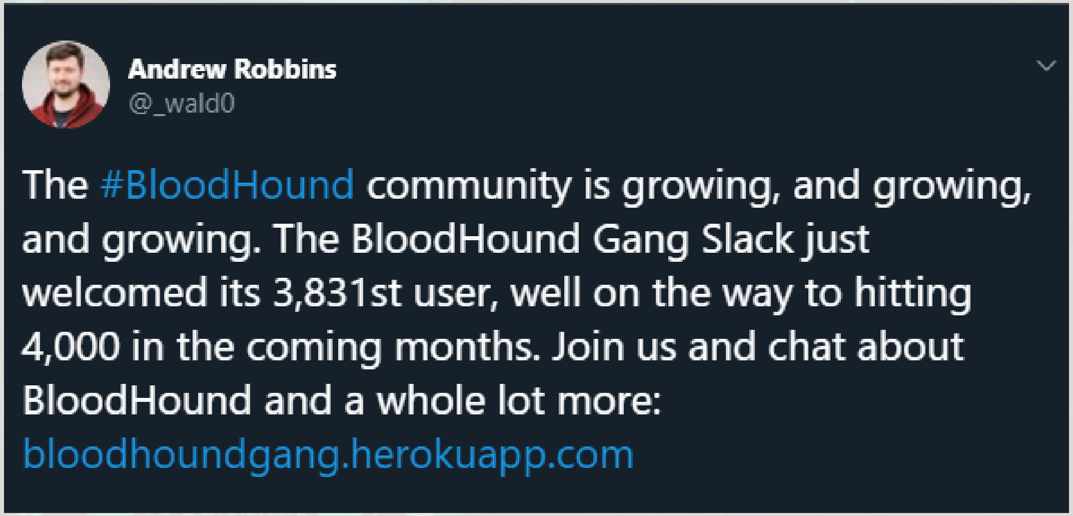
Six Degrees of Domain Admin

THE DOG WHISPERER'S HANDBOOK

A Hacker's Guide to the BloodHound Galaxy – @SadProcessor

https://insinuator.net/2018/11/the-dog-whisperers-handbook/

BloodHound
Gang Slack



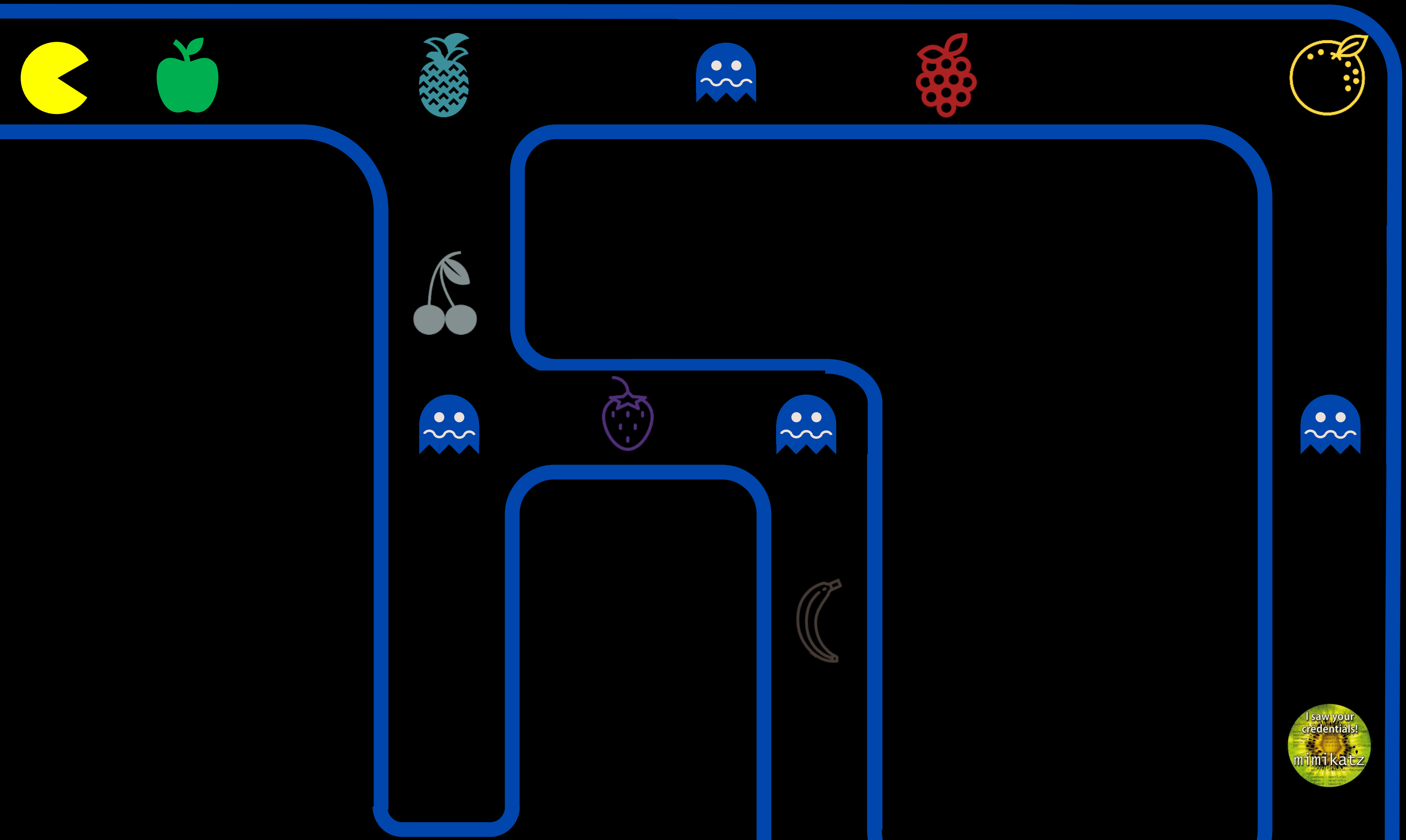
Andrew Robbins
@_wald0

The #BloodHound community is growing, and growing, and growing. The BloodHound Gang Slack just welcomed its 3,831st user, well on the way to hitting 4,000 in the coming months. Join us and chat about BloodHound and a whole lot more: bloodhoundgang.herokuapp.com

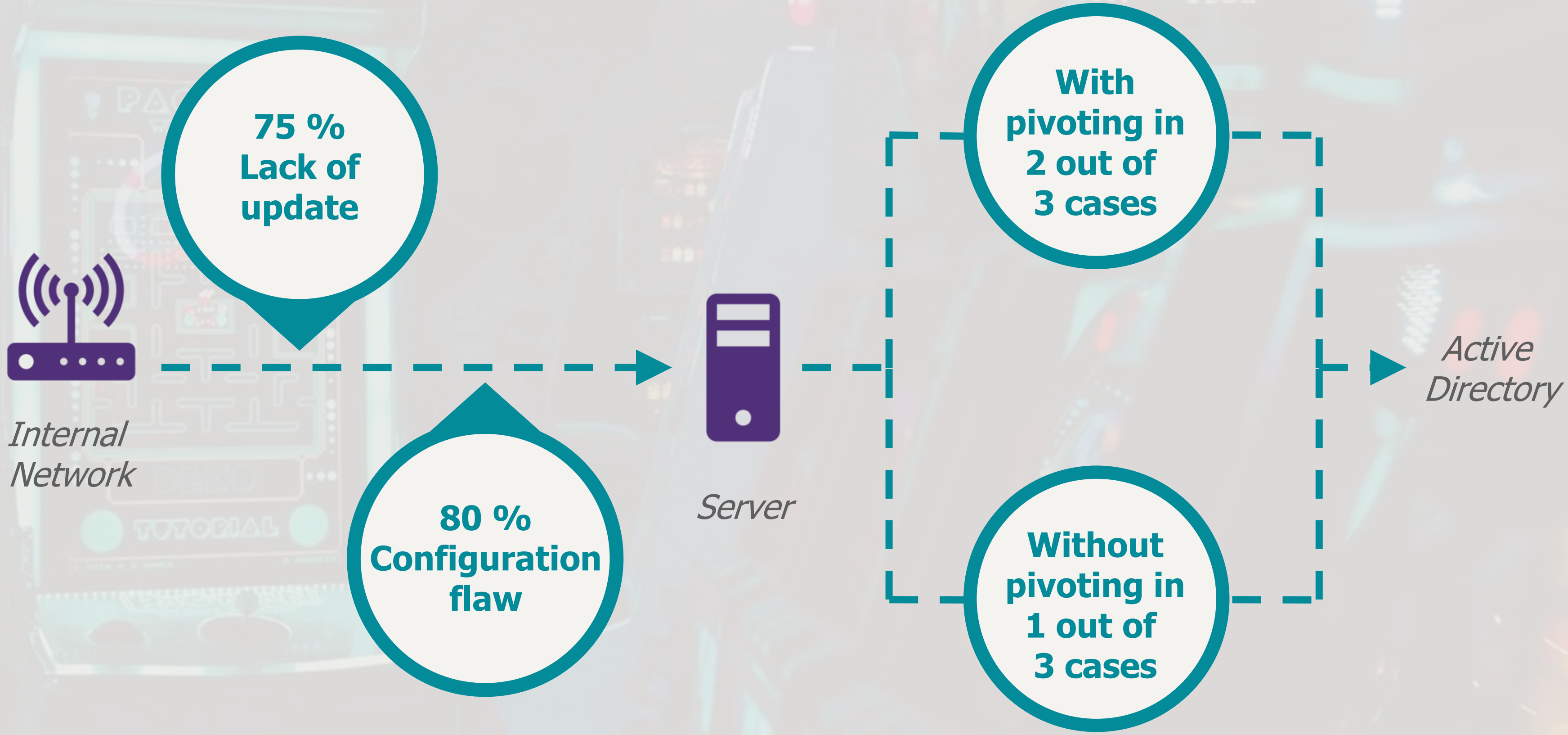
https://bloodhoundgang.herokuapp.com/

WINNER !

Another Game ?



In real life



First asset compromised

Overall compromise

75 % Lack of update

80 % Configuration flaw

With pivoting in 2 out of 3 cases

Without pivoting in 1 out of 3 cases

Commando VM

- **Windows Offensive Distribution**
- 140 Tools

  Active Directory Tools

  Evasion

  Exploitation

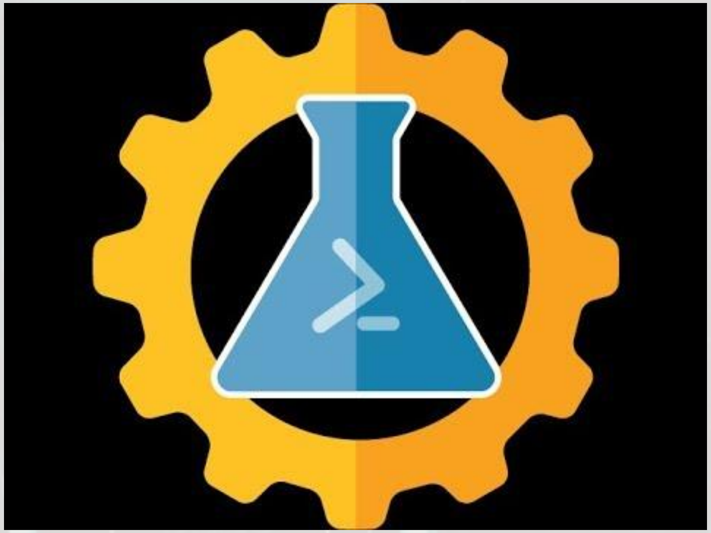
  Information Gathering

  Password Attacks

  …

https://www.fireeye.com/blog/threat-research/2019/03/commando-vm-windows-offensive-distribution.html

AutomatedLab



- **Provisioning framework that lets you deploy complex labs on HyperV and Azure with simple PowerShell scripts**
- Supported products:

  Windows 7, 2008, 8, 2012, 10, 2016

  SQL Server

  Exchange

  SCCM / MDT

  Office

  ……

https://github.com/AutomatedLab/AutomatedLab

Going further, free resources

- **This workshop**: https://github.com/wavestone-cdt/AD-security-workshop
- **SpectorOps Team**: Amazing blog posts and tools such as BloodHoound / SharpSploit / GhostPack / …

  https://specterops.io/resources/research-and-development
- **Adsecurity** (@PyroTek3): https://adsecurity.org/
- **Mimikaz** (@gentilkiwi) : http://blog.gentilkiwi.com/mimikatz
- **Grouper2** (@mikeloss): https://github.com/l0ss/Grouper2
- **PingCastle** (@mysmartlogon): https://www.pingcastle.com/
- **MITRE ATT&CK:** https://attack.mitre.org/
- **JPCERTCC**: https://jpcertcc.github.io/ToolAnalysisResultSheet/
- **Wavestone**: https://github.com/wavestone-cdt/wavecrack

Thank you !

@remiescourrou

@nicolas_dbresse