Windows API Exploitation Recipes
for
Red – Blue Teams

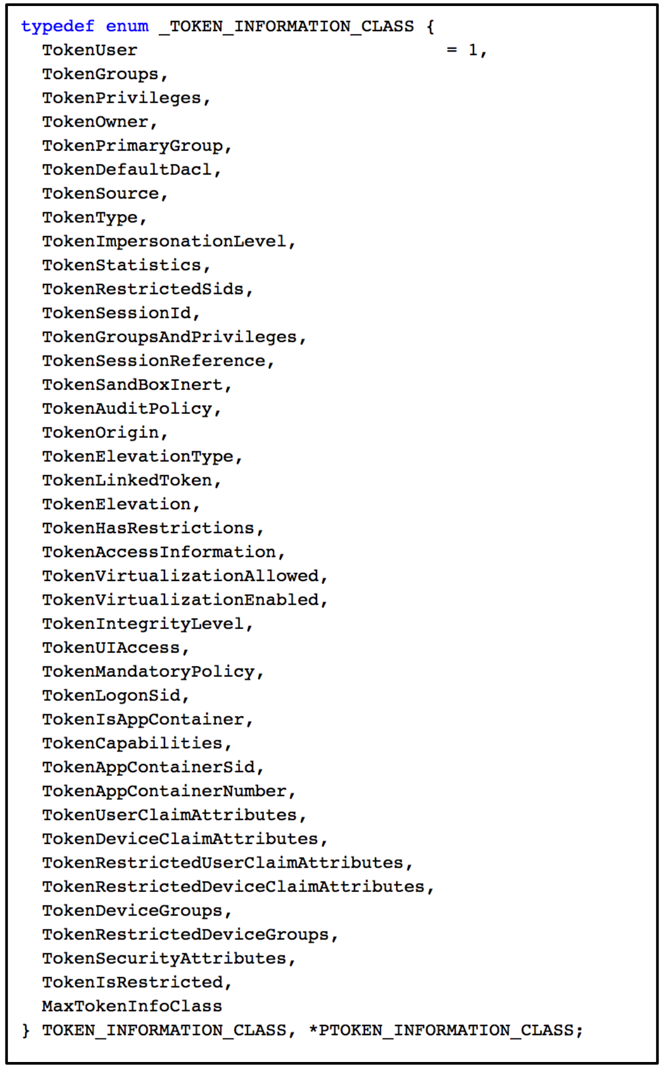
Vivek Ramachandran

Chief Trainer, Pentester Academy

http://PentesterAcademy.com

Process Token Dumper: Part 2
Code Walkthrough

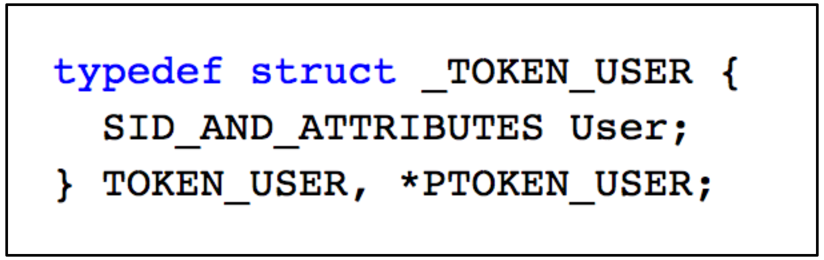
Token Information



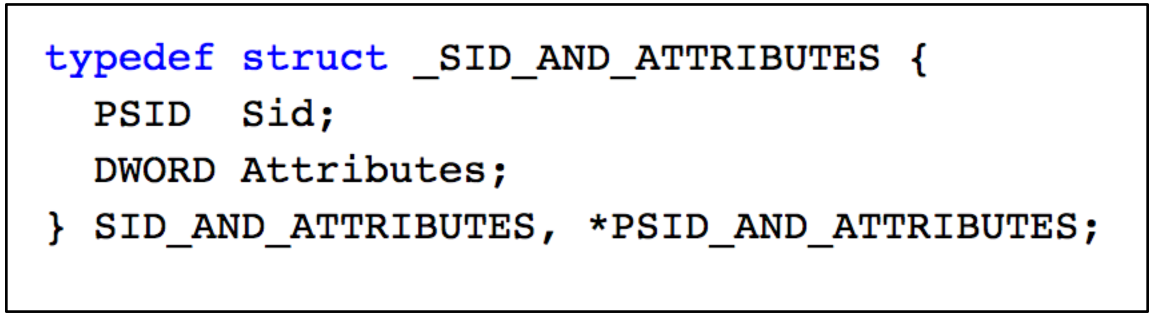
```
typedef enum _TOKEN_INFORMATION_CLASS {
  TokenUser                             = 1,
  TokenGroups,
  TokenPrivileges,
  TokenOwner,
  TokenPrimaryGroup,
  TokenDefaultDacl,
  TokenSource,
  TokenType,
  TokenImpersonationLevel,
  TokenStatistics,
  TokenRestrictedSids,
  TokenSessionId,
  TokenGroupsAndPrivileges,
  TokenSessionReference,
  TokenSandBoxInert,
  TokenAuditPolicy,
  TokenOrigin,
  TokenElevationType,
  TokenLinkedToken,
  TokenElevation,
  TokenHasRestrictions,
  TokenAccessInformation,
  TokenVirtualizationAllowed,
  TokenVirtualizationEnabled,
  TokenIntegrityLevel,
  TokenUIAccess,
  TokenMandatoryPolicy,
  TokenLogonSid,
  TokenIsAppContainer,
  TokenCapabilities,
  TokenAppContainerSid,
  TokenAppContainerNumber,
  TokenUserClaimAttributes,
  TokenDeviceClaimAttributes,
  TokenRestrictedUserClaimAttributes,
  TokenRestrictedDeviceClaimAttributes,
  TokenDeviceGroups,
  TokenRestrictedDeviceGroups,
  TokenSecurityAttributes,
  TokenIsRestricted,
  MaxTokenInfoClass
} TOKEN_INFORMATION_CLASS, *PTOKEN_INFORMATION_CLASS;
```

https://msdn.microsoft.com/en-us/library/windows/desktop/aa379626(v=vs.85).aspx

Token User



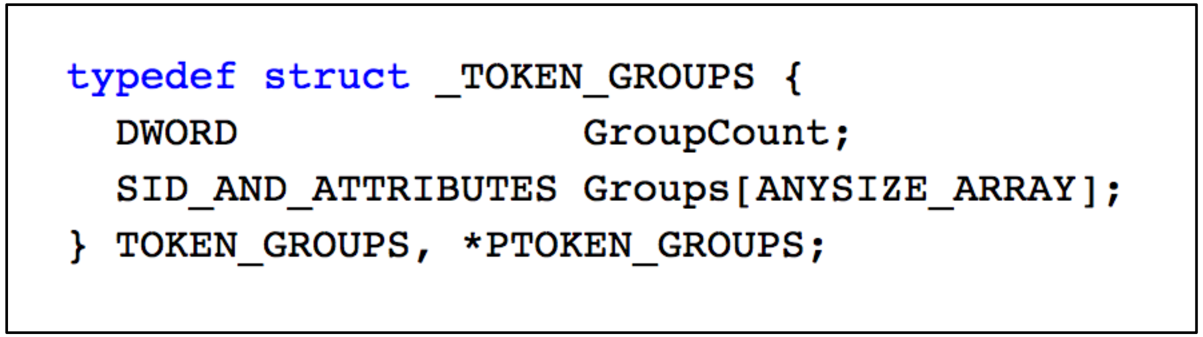
```
typedef struct _TOKEN_USER {
  SID_AND_ATTRIBUTES User;
} TOKEN_USER, *PTOKEN_USER;
```



```
typedef struct _SID_AND_ATTRIBUTES {
  PSID  Sid;
  DWORD Attributes;
} SID_AND_ATTRIBUTES, *PSID_AND_ATTRIBUTES;
```

- User account associated with the Access Token

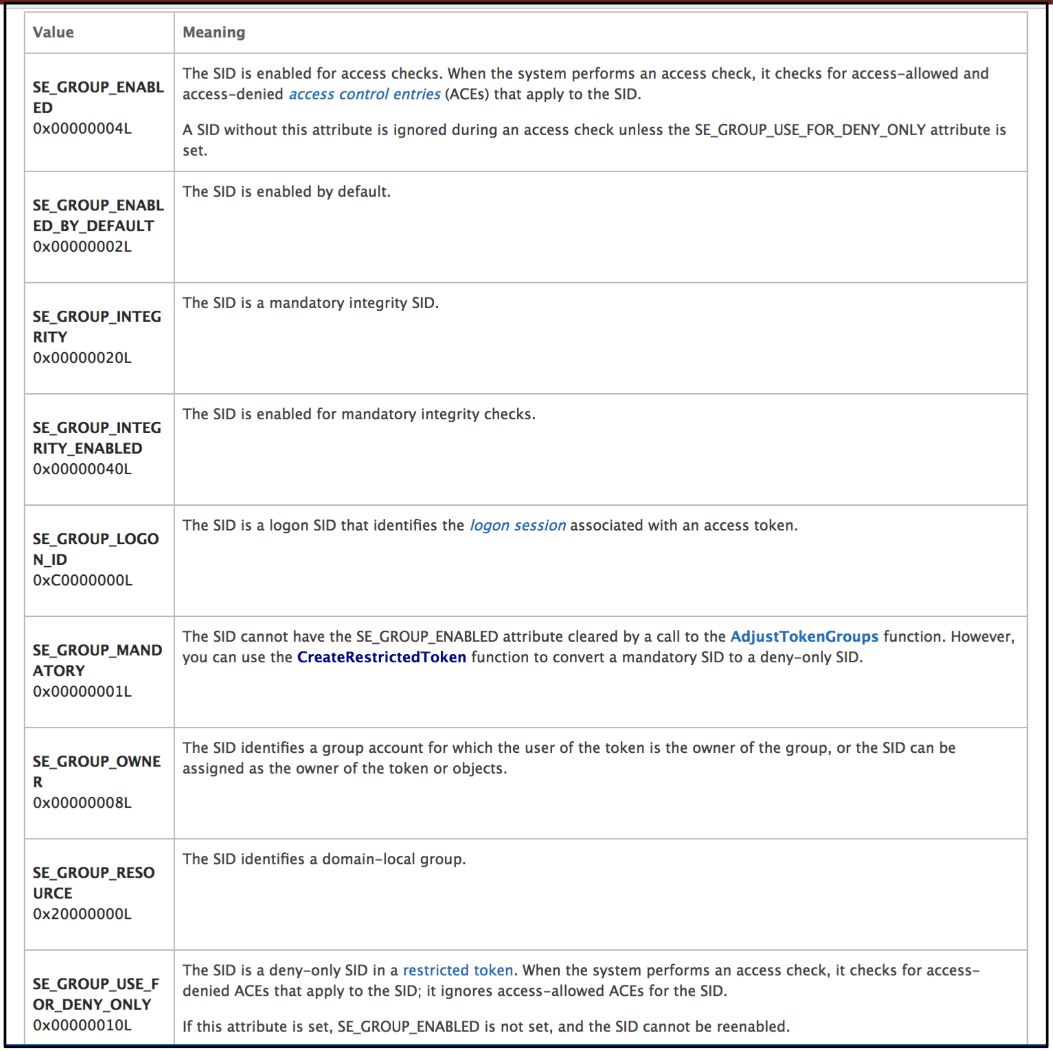
Token Groups



```
typedef struct _TOKEN_GROUPS {
  DWORD                GroupCount;
  SID_AND_ATTRIBUTES Groups[ANYSIZE_ARRAY];
} TOKEN_GROUPS, *PTOKEN_GROUPS;
```

- Groups SIDs associated with the Token

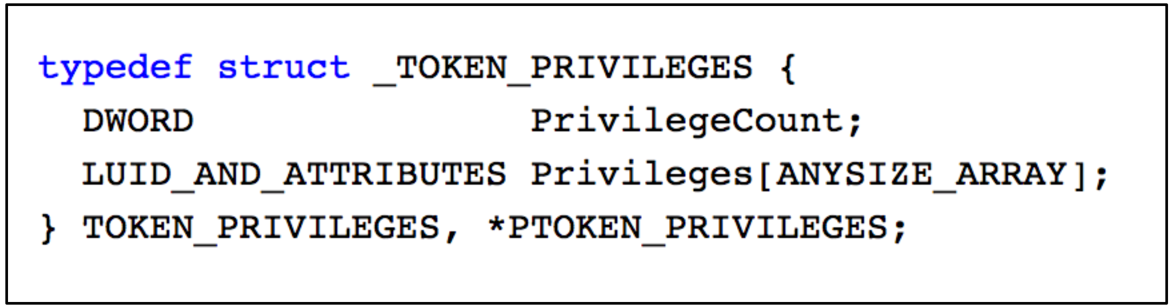
Token Groups SID Attributes



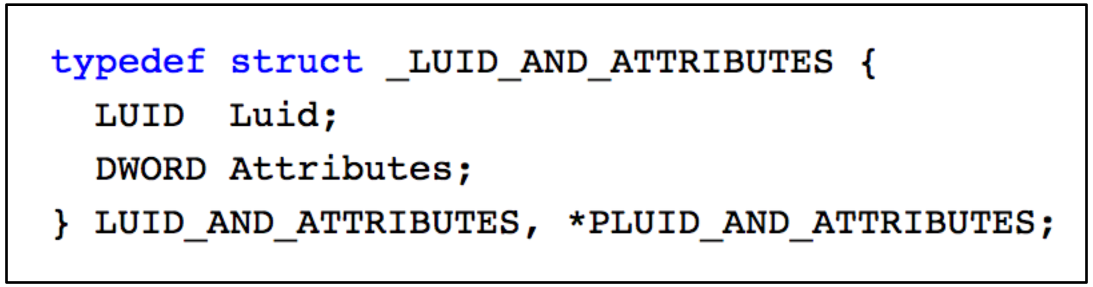
Value	Meaning
SE_GROUP_ENABLED 0x00000004L	The SID is enabled for access checks. When the system performs an access check, it checks for access-allowed and access-denied *access control entries* (ACEs) that apply to the SID. A SID without this attribute is ignored during an access check unless the SE_GROUP_USE_FOR_DENY_ONLY attribute is set.
SE_GROUP_ENABLED_BY_DEFAULT 0x00000002L	The SID is enabled by default.
SE_GROUP_INTEGRITY 0x00000020L	The SID is a mandatory integrity SID.
SE_GROUP_INTEGRITY_ENABLED 0x00000040L	The SID is enabled for mandatory integrity checks.
SE_GROUP_LOGON_ID 0xC0000000L	The SID is a logon SID that identifies the *logon session* associated with an access token.
SE_GROUP_MANDATORY 0x00000001L	The SID cannot have the SE_GROUP_ENABLED attribute cleared by a call to the **AdjustTokenGroups** function. However, you can use the **CreateRestrictedToken** function to convert a mandatory SID to a deny-only SID.
SE_GROUP_OWNER 0x00000008L	The SID identifies a group account for which the user of the token is the owner of the group, or the SID can be assigned as the owner of the token or objects.
SE_GROUP_RESOURCE 0x20000000L	The SID identifies a domain-local group.
SE_GROUP_USE_FOR_DENY_ONLY 0x00000010L	The SID is a deny-only SID in a restricted token. When the system performs an access check, it checks for access-denied ACEs that apply to the SID; it ignores access-allowed ACEs for the SID. If this attribute is set, SE_GROUP_ENABLED is not set, and the SID cannot be reenabled.

https://msdn.microsoft.com/en-us/library/windows/desktop/aa379624(v=vs.85).aspx

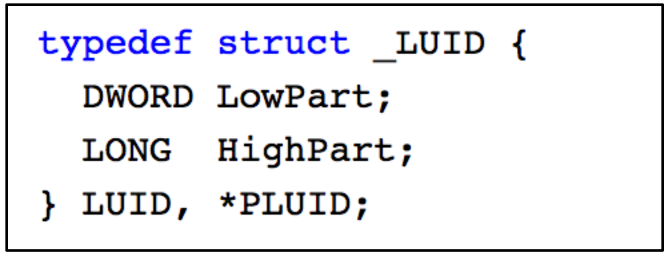
Token Privileges



```
typedef struct _TOKEN_PRIVILEGES {
  DWORD               PrivilegeCount;
  LUID_AND_ATTRIBUTES Privileges[ANYSIZE_ARRAY];
} TOKEN_PRIVILEGES, *PTOKEN_PRIVILEGES;
```



```
typedef struct _LUID_AND_ATTRIBUTES {
  LUID  Luid;
  DWORD Attributes;
} LUID_AND_ATTRIBUTES, *PLUID_AND_ATTRIBUTES;
```

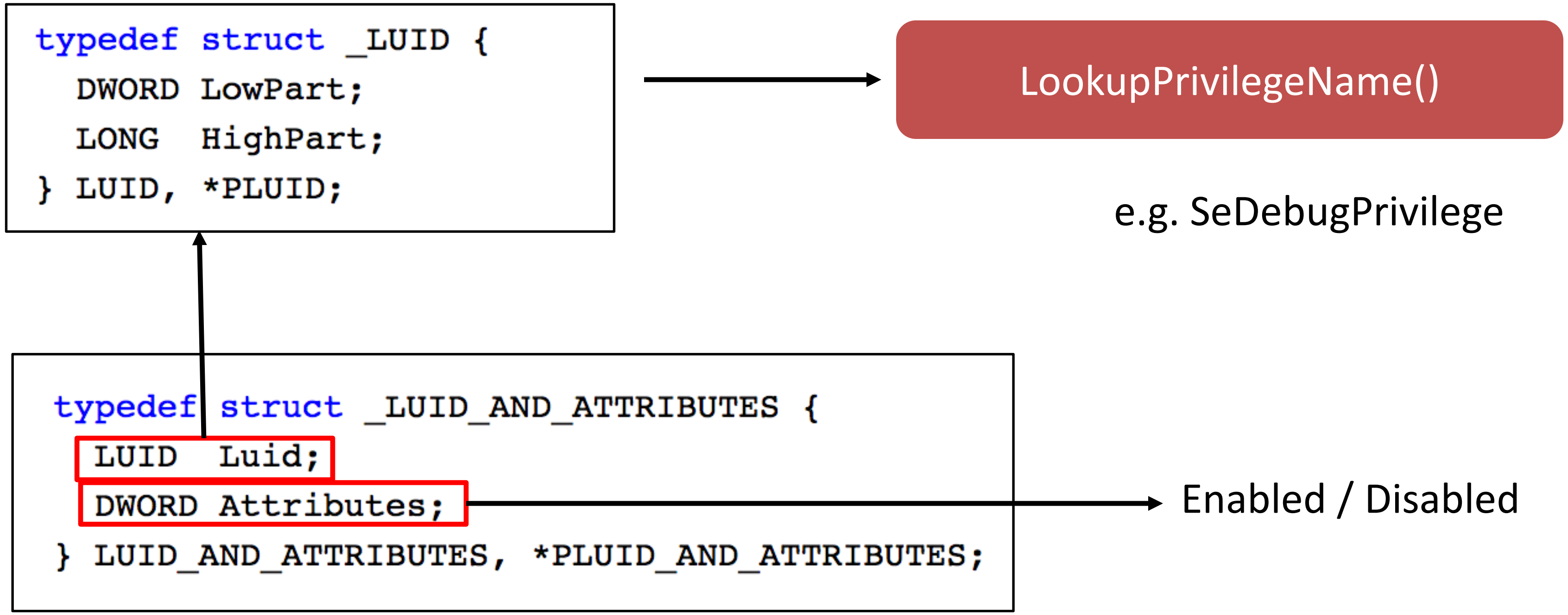


```
typedef struct _LUID {
  DWORD LowPart;
  LONG  HighPart;
} LUID, *PLUID;
```

64-bits

- Available Privilege Set in the Token
- Individual privileges might be enabled / disabled

Token Privileges



```
typedef struct _LUID {
  DWORD LowPart;
  LONG  HighPart;
} LUID, *PLUID;
```

LookupPrivilegeName()

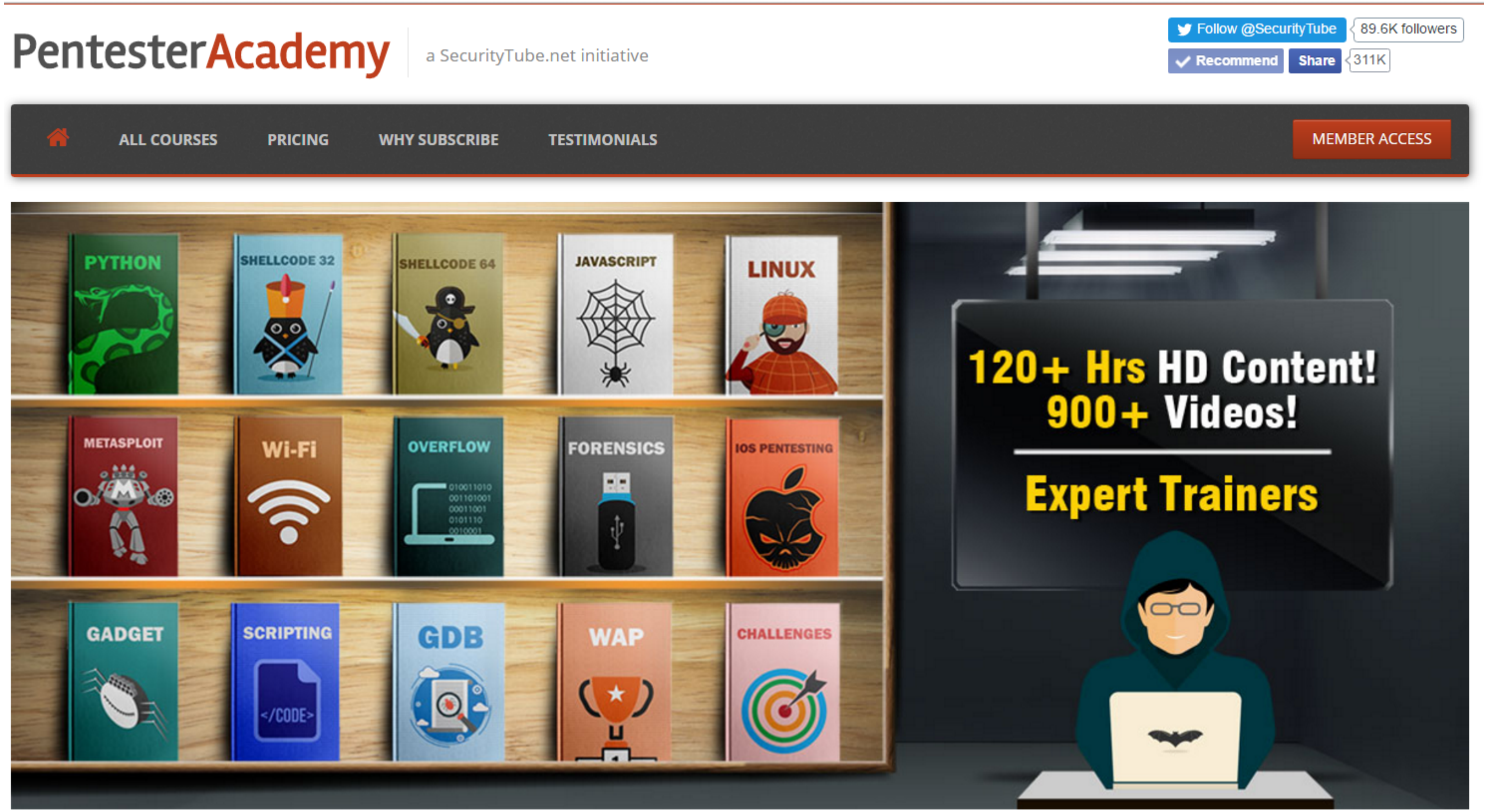
e.g. SeDebugPrivilege

```
typedef struct _LUID_AND_ATTRIBUTES {
  LUID  Luid;
  DWORD Attributes;
} LUID_AND_ATTRIBUTES, *PLUID_AND_ATTRIBUTES;
```

Enabled / Disabled

- LUID values maps to Privileges
- Check if Privilege is enabled/disabled

Thank You!


PentesterAcademy
a SecurityTube.net initiative
Follow @SecurityTube
89.6K followers
Recommend
Share
311K
ALL COURSES
PRICING
WHY SUBSCRIBE
TESTIMONIALS
MEMBER ACCESS
PYTHON
SHELLCODE 32
SHELLCODE 64
JAVASCRIPT
LINUX
METASPLOIT
Wi-Fi
OVERFLOW
FORENSICS
IOS PENTESTING
GADGET
SCRIPTING
</CODE>
GDB
WAP
CHALLENGES
120+ Hrs HD Content!
900+ Videos!
Expert Trainers