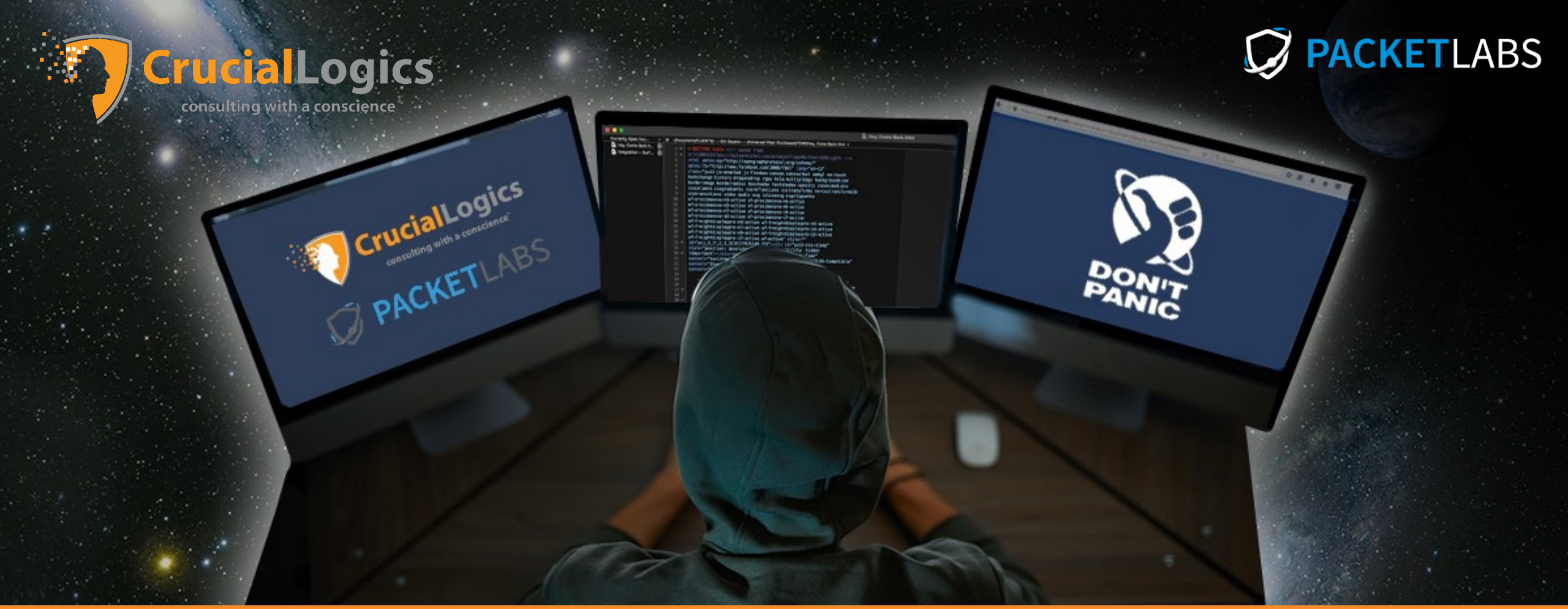
CrucialLogics
consulting with a conscience

PACKETLABS



The Hitchhikers Guide To Hacking

4 Hacks And How To Avoid Them

Thank you for joining us today!

- This session is being recorded for replay
- Listen-only mode during the presentation
- Ask questions! Please submit questions via the chat

Speaker

Amol Joshi

Partner Enterprise Services, CrucialLogics

Amol is a senior security executive with over 16 years of experience in leading and executing complex IT transformations and security programs. He's a firm believer in achieving security through standardization, avoiding complexity and that security be achieved using native, easy-to-use technologies. Amol approaches business challenges in a detail-oriented way and demonstrates quantifiable results throughout the course of highly technical and complex engagements.

Speaker

Richard Rogerson

Managing Partner, Packetlabs

Richard leads a team of ethical hackers who find critical vulnerabilities in client systems before a breach. He has 10+ years of professional consulting experience delivering and leading offensive campaigns. He has several of the most advanced cybersecurity certifications and has been featured in the media several times for his views on cybersecurity breaches including Business E-mail Compromise, Ransomware and Nation-state APTs.

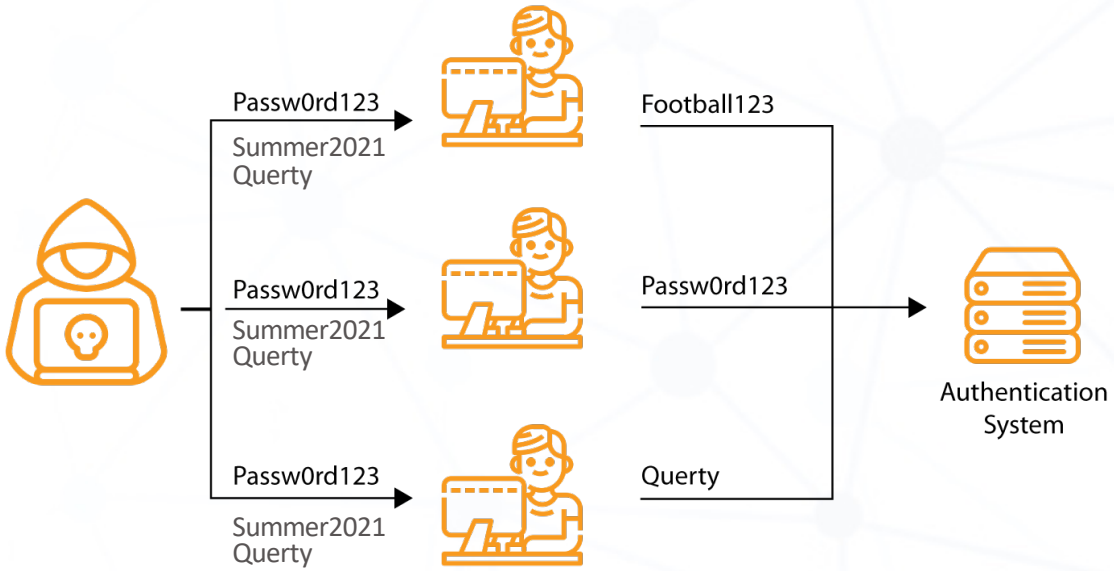
Todays 4 hacks

1. Credentials spraying and stuffing (MSOLSpray)
2. Credential access due to legacy protocols - Responder (Netbios)
3. Active Directory privilege escalation (Bloodhound)
4. Credential access due to insecure storage (Mimikatz)

Credential Spraying and Credential Stuffing

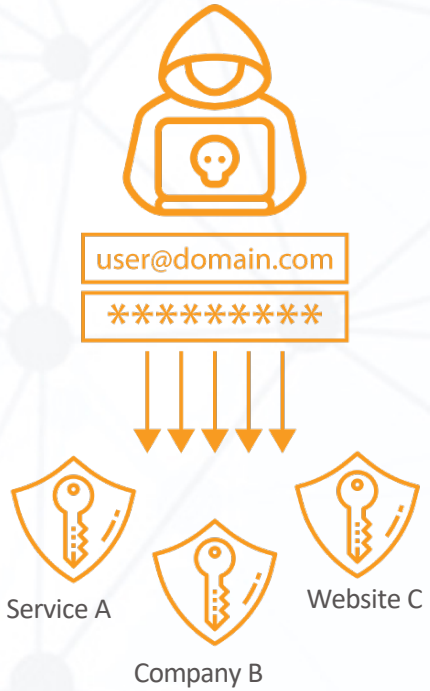
Credential Spraying

- Using tools such as MSOLSpray (powershell) or other such spraying toolkits
- Hackers target a domain and try and exploit dictionary attack to guess a weak password. All they need is to gain access into the **handful** of users on domain/tenant to exploit further
- Uses multiple passwords into multiple accounts



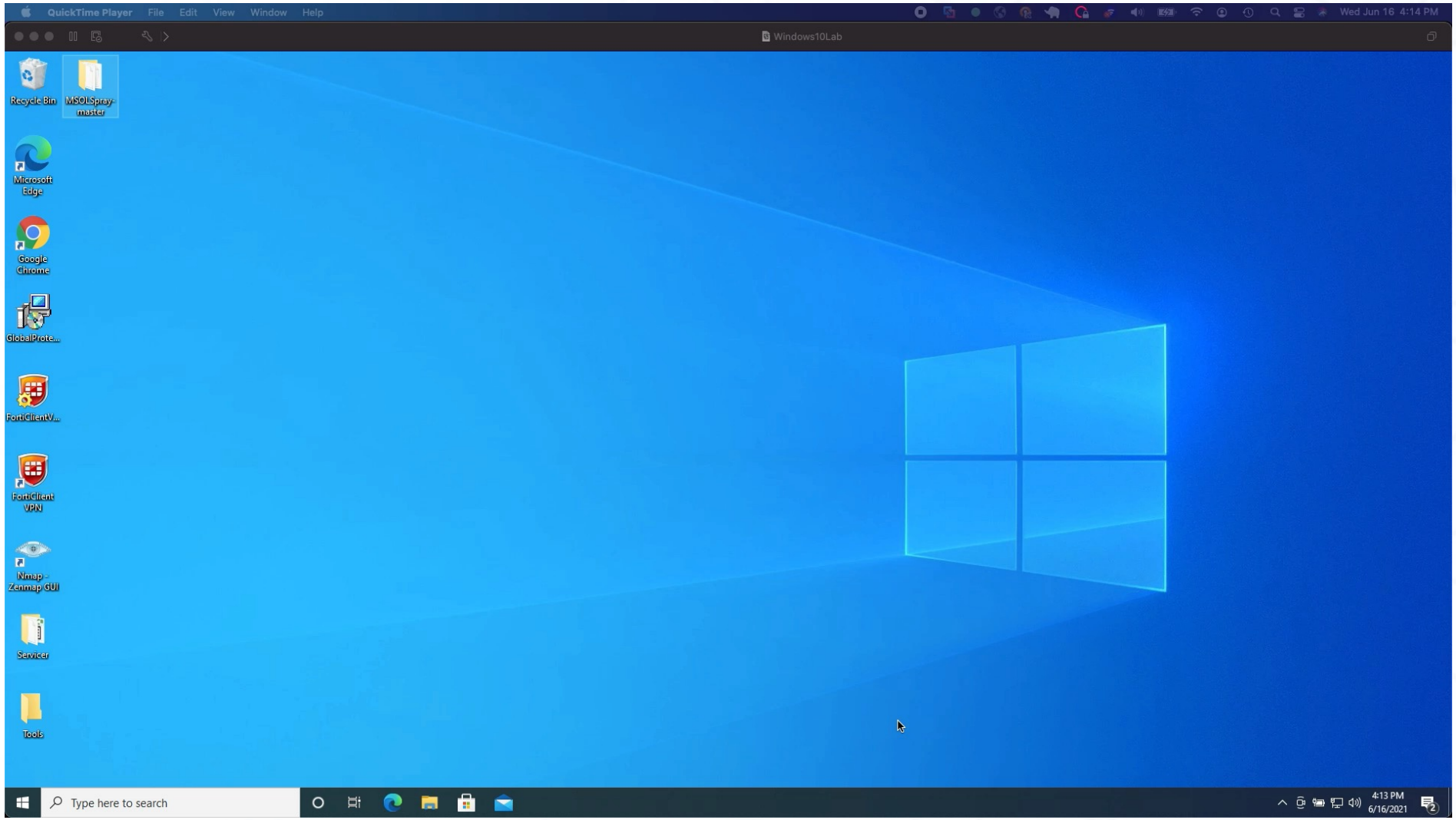
Credential Stuffing

- Test for known compromised passwords on multiple targets to search for credential reuse
- Assumes most people reuse the same credentials on multiple sites



CrucialLogics
consulting with a conscience™

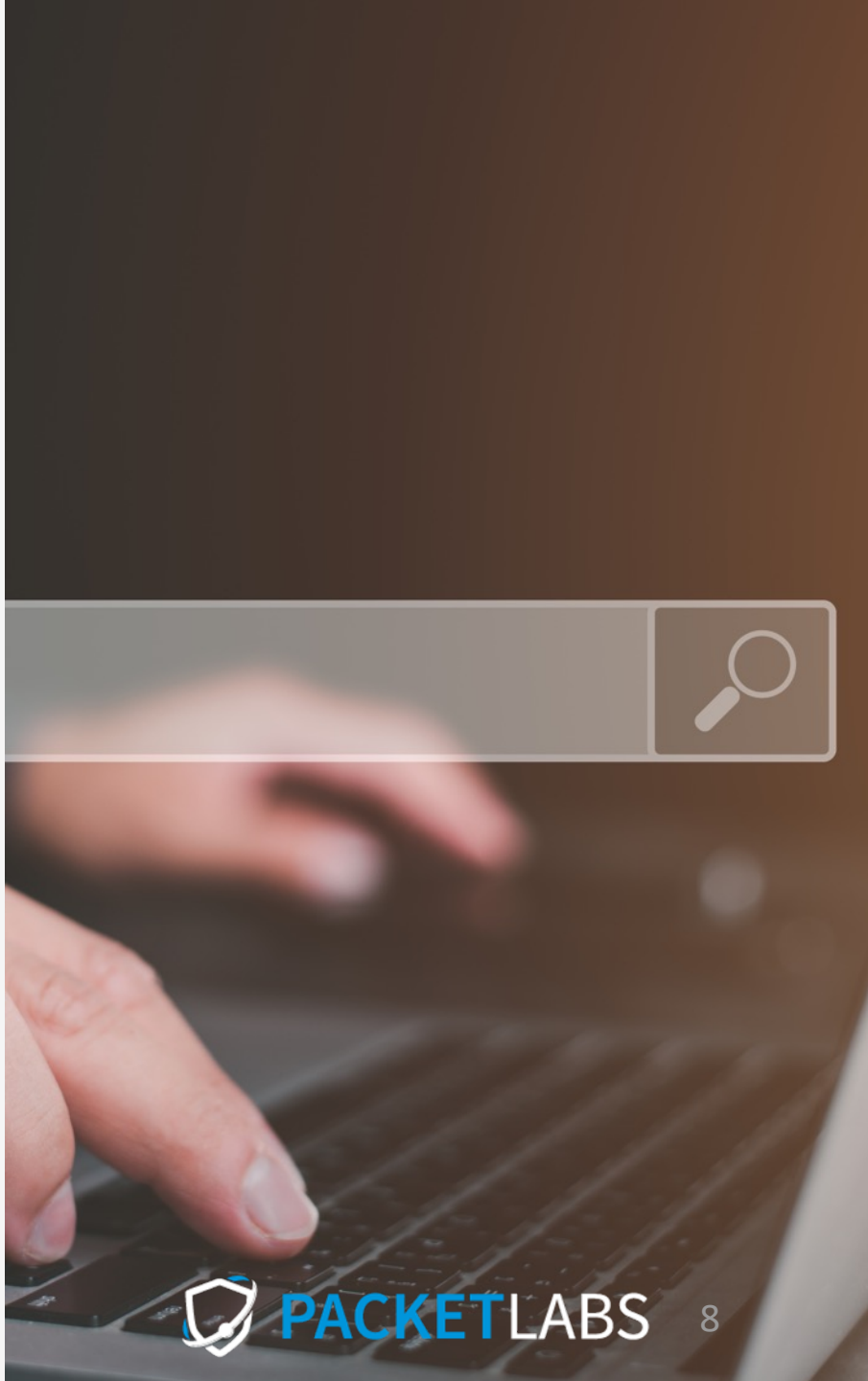
Credentials spraying demonstration



CrucialLogics
consulting with a conscience™

How to mitigate credential attacks

1. **Obvious choices**
    1. MFA
    2. Strong Passwords
    3. Identity Protection policies and configurations
    4. For third-party apps SSO integration into your AD so Identity polices can traverse between applications
    5. Account lockouts
    6. Using different passwords for different services if SSO integration isn't possible
    7. Password Manager
2. **Less obvious choices**
    1. Conditional access to block access from unauthorized devices
    2. Configure Alerts or Review Suspicious logon attempts
    3. Password Audit to ensure policy is effective



CrucialLogics
consulting with a conscience™

PACKETLABS

Responder Hack Explanation

1. User is trying to access a file share and computer checks the DNS for file share IP address

2. If user mistypes the file share name or DNS entry for that file share is misconfigured or for variety of other reasons where the DNS resolution fails resolve the query

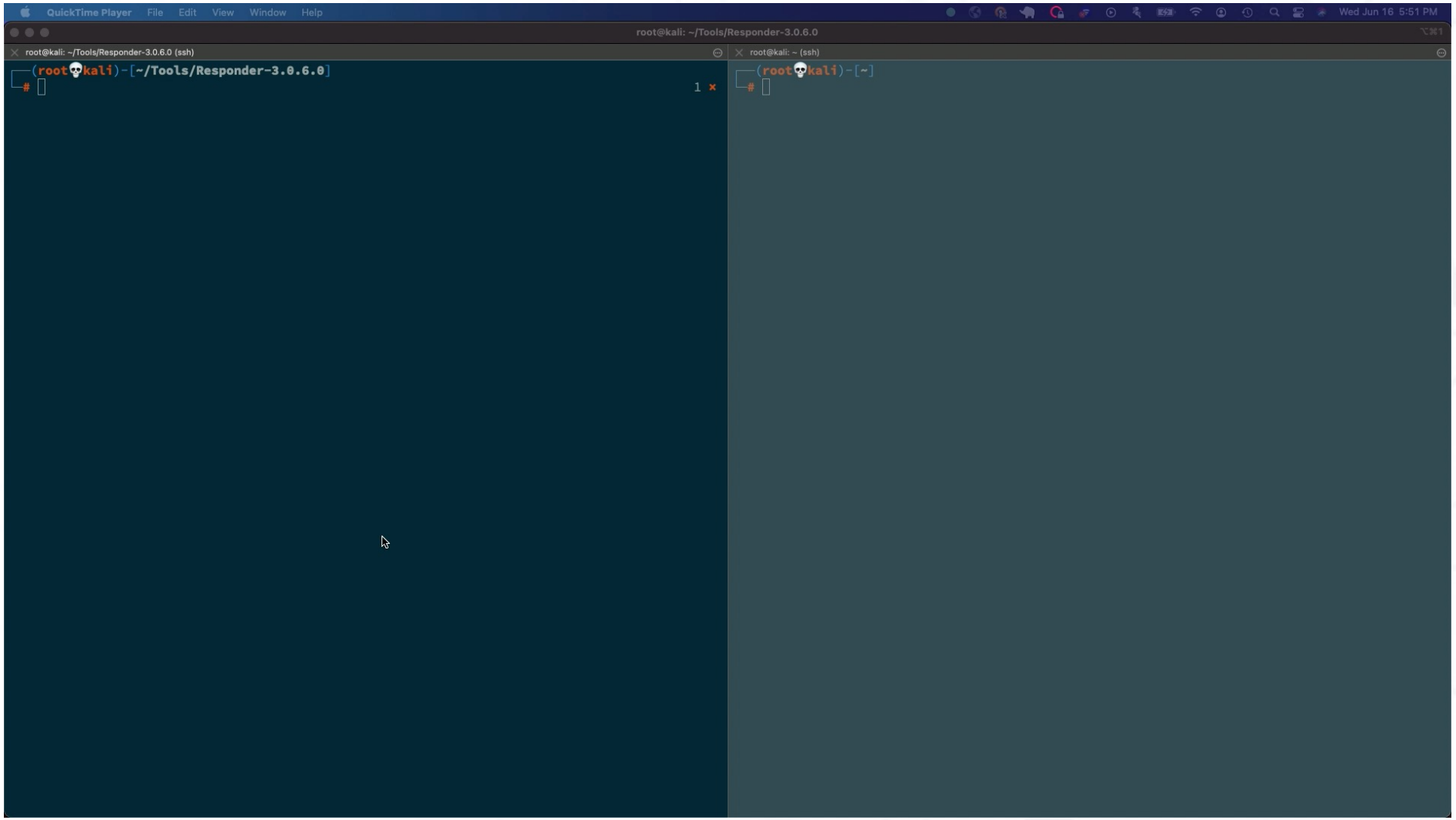
3. Reply is sent for the query saying it doesn't know where the requested file share is

4. The computer will then broadcast the query to the wider network requesting other computers for the whereabouts of the requested file share
   - This is managed by three main protocols **NBT-NS** (NetBIOS Name Service), **LLMNR** (Link-Local Multicast Name Resolution) and **mDNS** (multicast DNS)

5. Our attacker who has already gained access via the credential spraying or stuffing has the responder toolkit installed on the domain

6. The attacker will now respond back using to the search query redirecting the authentication over to a compromised machine harvesting passwords

Responder demonstration



How to mitigate against Responder

1. Disable LLMNR and NBT-NS

2. If #1 is not possible then setup monitoring for LLMNR and NBT-NS ports on the hosts, monitor for event id **4697** and **7045** which signify relay attacks & monitor for changes to registry DWORD EnableMulticast

3. Enable SMB signing in your Group Policy

4. Segment your network, and isolate sensitive/administrative systems

CrucialLogics
consulting with a conscience™

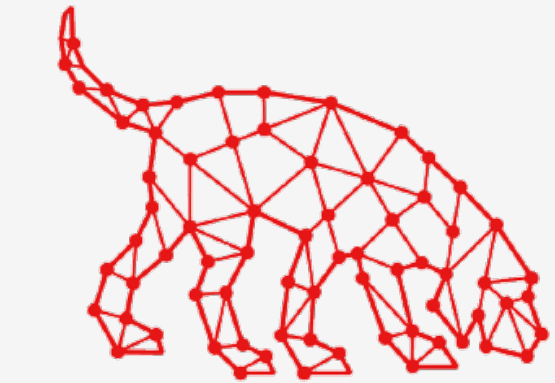
PACKETLABS

Bloodhound

1. Sole purpose of this application is to visualize the shortest path to compromising the domain.

2. Provides ability for attackers to move laterally and elevate privileges

3. Evaluates sensitive permissions that can be granted to attackers such as Reset password, add member, full control, Write Owner and plenty more

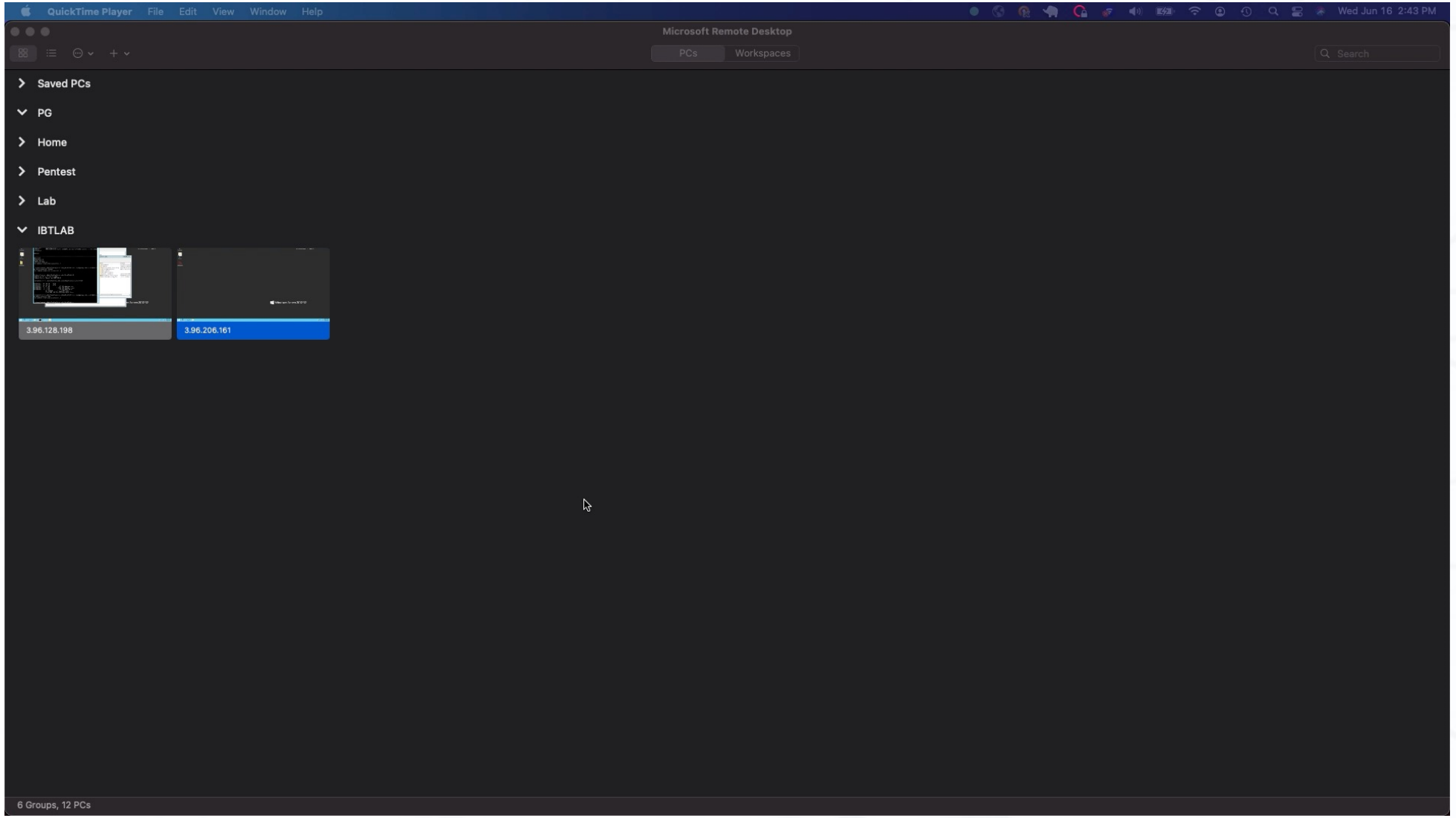


BLOODHOUND

CrucialLogics
consulting with a conscience™

PACKETLABS

Bloodhound demonstration



How to mitigate against Bloodhound

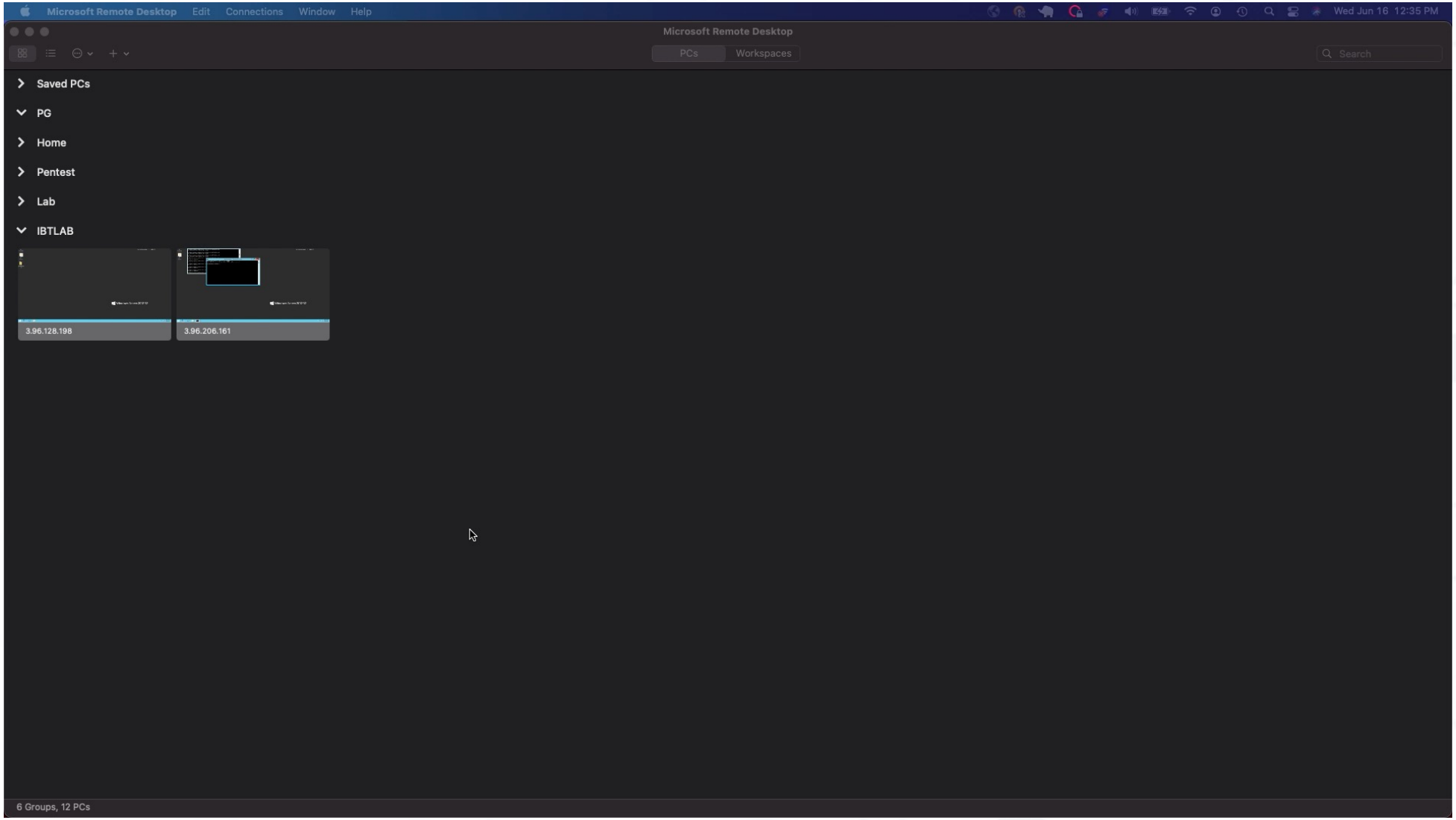
1. Leverage tools that will detect Bloodhound
   ex – Microsoft Defender ATP and other such EDR tools
2. Manage your computers individually vs.
   having them tied to the domain (new way)
3. Do not leave domain admin sessions active, ensure that groups policies exists to terminate domain admin sessions when logging off
4. Revoke domain admin privileges from all server admins and delegate authority via server admins group to perform actives on each server using the principle of least privilege .
5. Minimize cache credentials from 10 to 0 if possible. Endpoints 1 or Servers 0
6. Hardening based on CIS, NIST, Microsoft SCM.
7. Mitigation against lateral movement, implement LAPS
8. **Run Bloodhound in your own environment**

CrucialLogics
consulting with a conscience™

Mimikatz

1. Benjamin Delphy created open source Mimikatz tool as a Proof of concept in 2007. The intention was to show Microsoft that their authentication protocol was vulnerable to attack.
2. Instead, this tool is now the most widely used and downloaded by the hackers.
3. Mimikatz takes advantage of a Windows feature called Wdigest, a feature intended for users to authenticate to applications within the computer or over the internet by remembering the logins and reusing them.
4. Although the password is encrypted in the memory the decryption key is stored on the computer too.
   " It's like storing a password-protected secret in an envelope with the password in the same email." Benjamin Delphy
5. Mimikatz is used to gain access to stored passwords on the computer.

Mimikatz demonstration



CrucialLogics
consulting with a conscience™

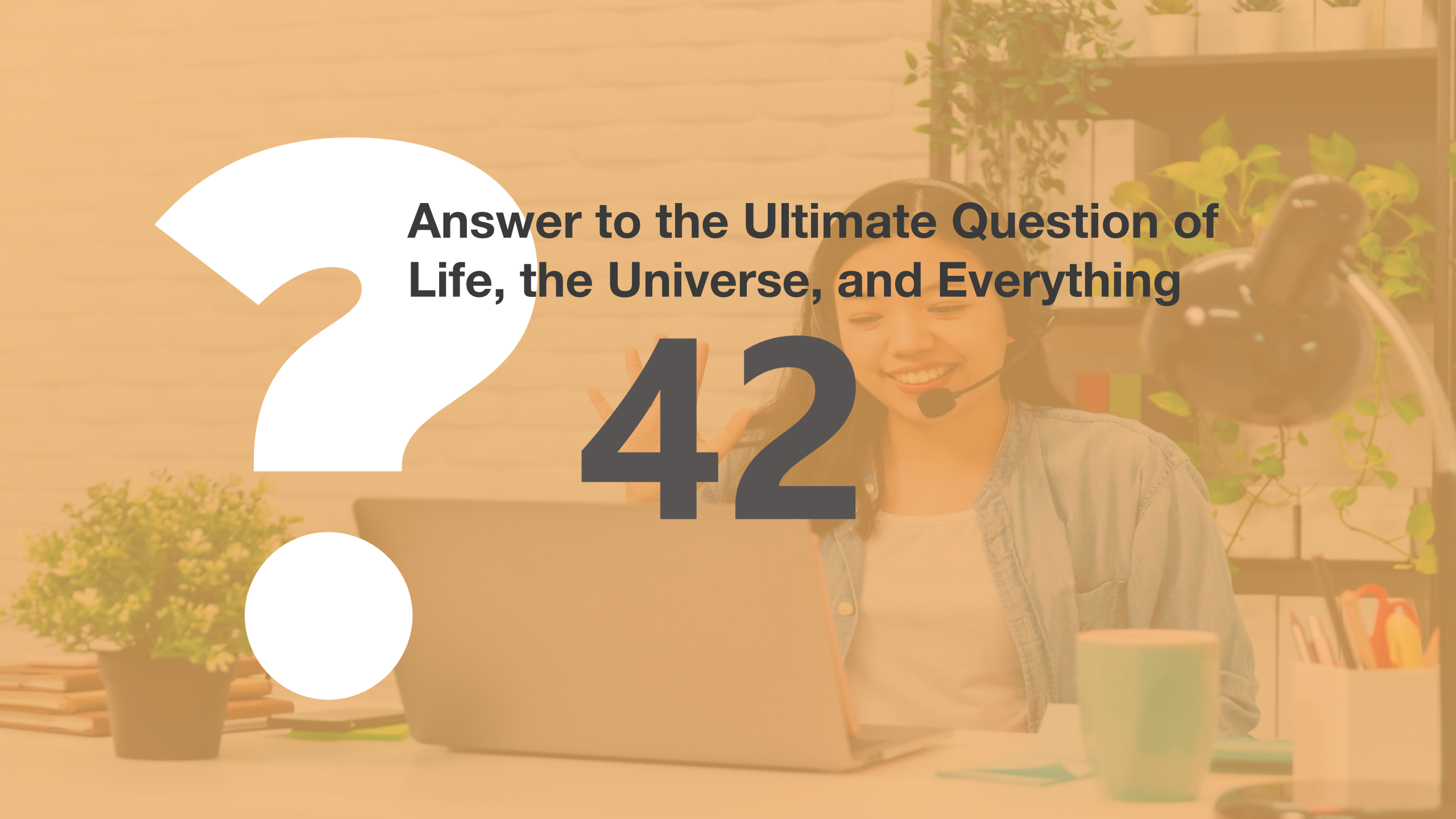
How to mitigate against Mimikatz

1. Disable local admin on all servers and workstations
2. Disable credential caching
3. Upgrade the schema and functional level of your forest and domain to at least 2012 R2. Introduces a new group called “Protected Users” and members of this user group are unable to authenticate using NTLM, Digest Authentication or CredSSP making it effective safeguard against Mimikatz
4. Upgrade to Microsoft Windows 8 (support ends 2023) or newer, these operating system disable Wdigest protocols
5. LSA protection – Windows has a service that is used to validate local and remote logins on a windows system called Local Security Authority Server Service. LSA protection will prevent untrusted processes from communicating with LSA
6. Monitor LSA access events via Sysmon (event ID 10) and Event ID 4656 in the Security Event Log for Windows 10.

CrucialLogics
consulting with a conscience™

Questions?

To ask our speakers a question, type your question into the Chat located in the bottom right portion of the screen.



Answer to the Ultimate Question of Life, the Universe, and Everything

42

Thank you for joining us today.

Amol Joshi
CrucialLogics
Amol.Joshi@cruciallogics.com

Richard Rogerson
Packetlabs
Rogerson@packetlabs.net