

LMNTRIX **RED** TEAM CASE STUDY

A Curious Case of Privacy Policy

YOU ARE NEVER AS SECURE AS YOU MAY THINK

This worldwide shipping conglomerate with an excellent well-funded security program would have rated well against any of the many frameworks and maturity assessments. They certainly would have withstood a standard script-based penetration test, but soon came undone when this LMNTRIX Red Team applied a more human approach to exploitation, highlighting the need for continual testing and improvement of your security program with regular real-life challenges.

Our client was keen to identify the weaknesses that remained by requesting us to infiltrate the organization using an externally based threat actor to leverage an initial foothold and gain access to this multi-national corporation's sensitive data.

Please take the time to read the account written by the LMNTRIX Red Team actor to appreciate that persistence will prevail for anyone who has the time to apply their skills and create corporate catastrophe for any hapless organisation targeted.

Determined, the team of only 2 'captured the flag' on just the fourth day of the assignment through careful research and creativity, proving the need to continuously review policy, procedure, user awareness and compliance around phishing and passwords, as well as apply detection and response capability beyond exploit signature matching and malware detection, that was at no time required for this breach to prove to be so potentially devastating.

This Red Team exercise reinforced the reality that threat actors need to get lucky once, while the rest of us need to remain lucky all of the time.

DAY 1.

POLICIES LOST AND URL'S FOUND

On day 1 I began work enumerating an external foothold, scanning the external servers for the information needed to begin our campaign, while my colleague began gathering OSINT (Open Source Intelligence) on the target's employees, including email addresses. We also began studying their interactions with recent suppliers to potentially emulate these interactions for a phishing campaign.

We found an externally exposed URL of the target organization on an AWS bucket which contained the privacy policy of the organization.

We then used this to initiate a carefully crafted phishing campaign. This campaign would target the employees in Sales and Accounts to accept an updated privacy policy for the organization.

We used Gophish, Mailgun and a fronted domain over Azure to setup the phishing infrastructure as detailed in one of our previous articles.

We simply sent an email to the target employees requesting they accept the latest privacy policy and added the CEO's image in the mail to make it look legitimate.

This malicious privacy policy document was hosted on a website, which when accessed, asked the user to download a Word document and click on "Enable Editing" and "Enable Macros" in order to accept the privacy policy.

We built the macro in such a way that it hid itself in the header of the Word Document.

We sent the mail to only 20 selected employees. Gophish showed that 7 of 20 clicked on the download link but only 3 enabled the macro and executed the payload. Of course we only needed one!

As soon as we gained the initial foothold, we executed another payload on 2 of those 3 systems which allowed us a backup beacon.

After gaining the initial access, we used the Internal Monologue tool to get the NetNTLMv2 hash of the user. Internal Monologue does not require administrative privileges but it's also limited to return only the current user's hash. Our aim was to escalate our privilege and maintain a persistent beacon at this point. We did this for all the three users and executed hashcat with the crackstation wordlist and 'One Rule to Rule Them All' rule to check for crackable passwords. We enumerated the hosts side by side to check for any misconfigurations or vulnerability so that we could maintain persistence, but Windows had a 1909 build, which meant at the time it was fully patched.

That evening, we lost our beacons, most likely since it was end of the day and the users might have shutdown their laptops. We were back to square one.

 **REAL-WORLD ATTACK SCENARIOS**

The methodology used by LMNTRIX used realistic attack scenarios using tactics, techniques, and procedures seen in real-world attacks.

 **CUSTOMIZABLE OBJECTIVES**

This was a tailored engagement to meet this client's needs, with objectives based on the most relevant risks to their organization.

Sample objectives:

- Obtain access to PCI data
- Obtain access to personally identifiable information (PII)
- Obtain access to trade secrets

DAY 2.

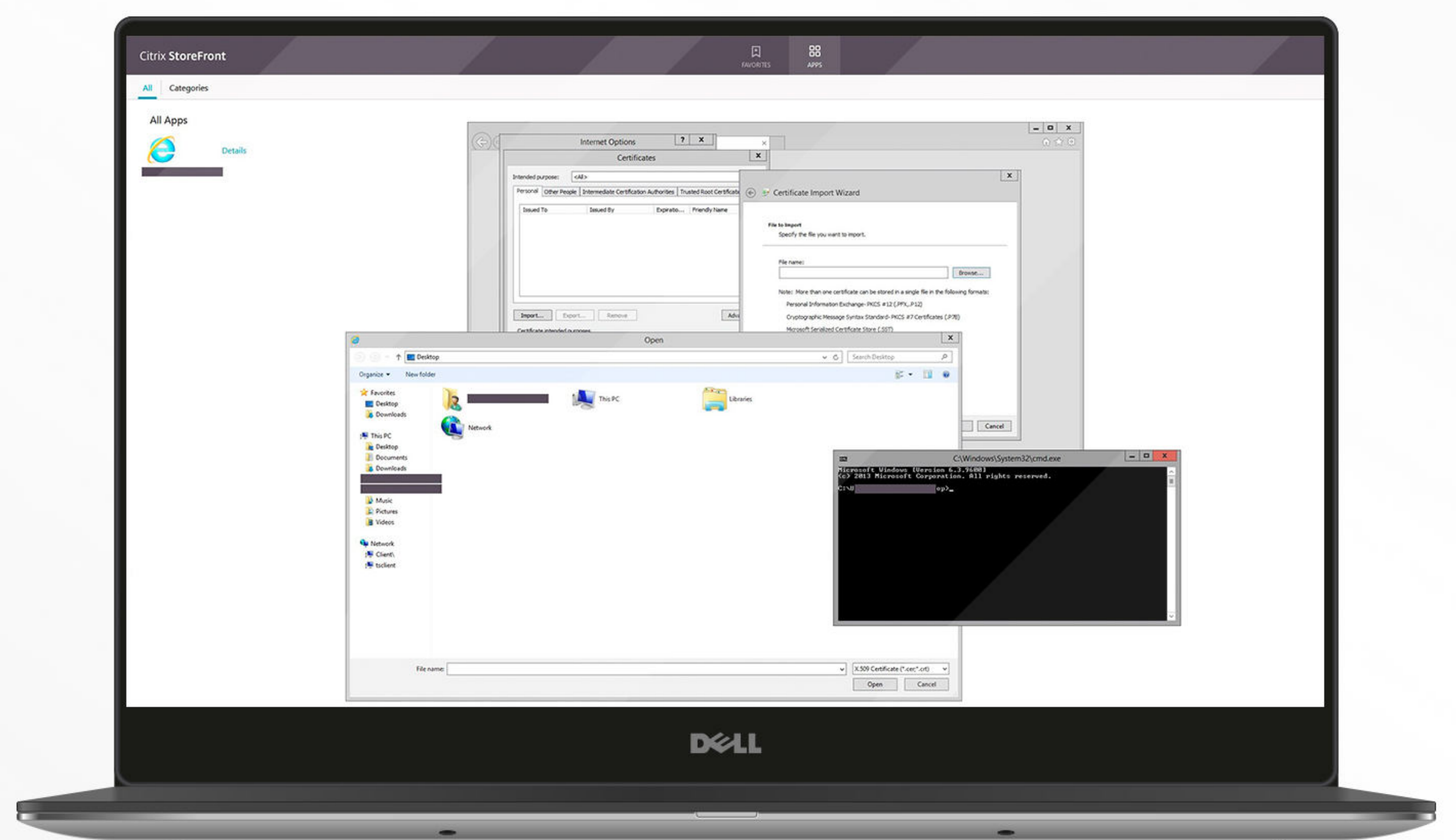
THE NECROMANCER

We came back on the second morning with more enthusiasm and luckily one of the passwords for user 'John Doe' was cracked. The password was 'Necromancer@2020'.

Since we lost all our beacons, we went back to scanning external login portals to validate our cracked credential. O365, Okta, Global Protect VPN, and almost everything had Multi Factor Authentication (MFA). It was almost the end of the second day when we found that the client had a Citrix Gateway too. With our hopes up, we tried to access the Citrix Gateway with our cracked credential and lo and behold, **we were in!**

The user had access to an intranet application within Citrix. We knew that the Citrix sandbox wasn't hard to evade, so we accessed the intranet application and it opened up the application in Internet Explorer. We executed C:\\Windows\\System32\\explorer.exe in the URL path to open a remote File Explorer, but we got 'access denied'. We also tried to execute cmd and powershell, but both were disabled by the administrator. Pulling up our hacker socks, we tried to be a little bit more creative and navigated to the **Internet Options->Certificates->Certificate Import Wizard->Browse and Bam!** We executed File Explorer successfully and from here on in things were easy. We executed cmd.exe from File Explorer and successfully received Cmd.exe access.

We now had successfully evaded the Citrix Sandbox. However, we still had only the privileges of the current user 'John Doe' so we called it a night as we now knew we had gained persistent access to Citrix and could access it whenever we chose to.

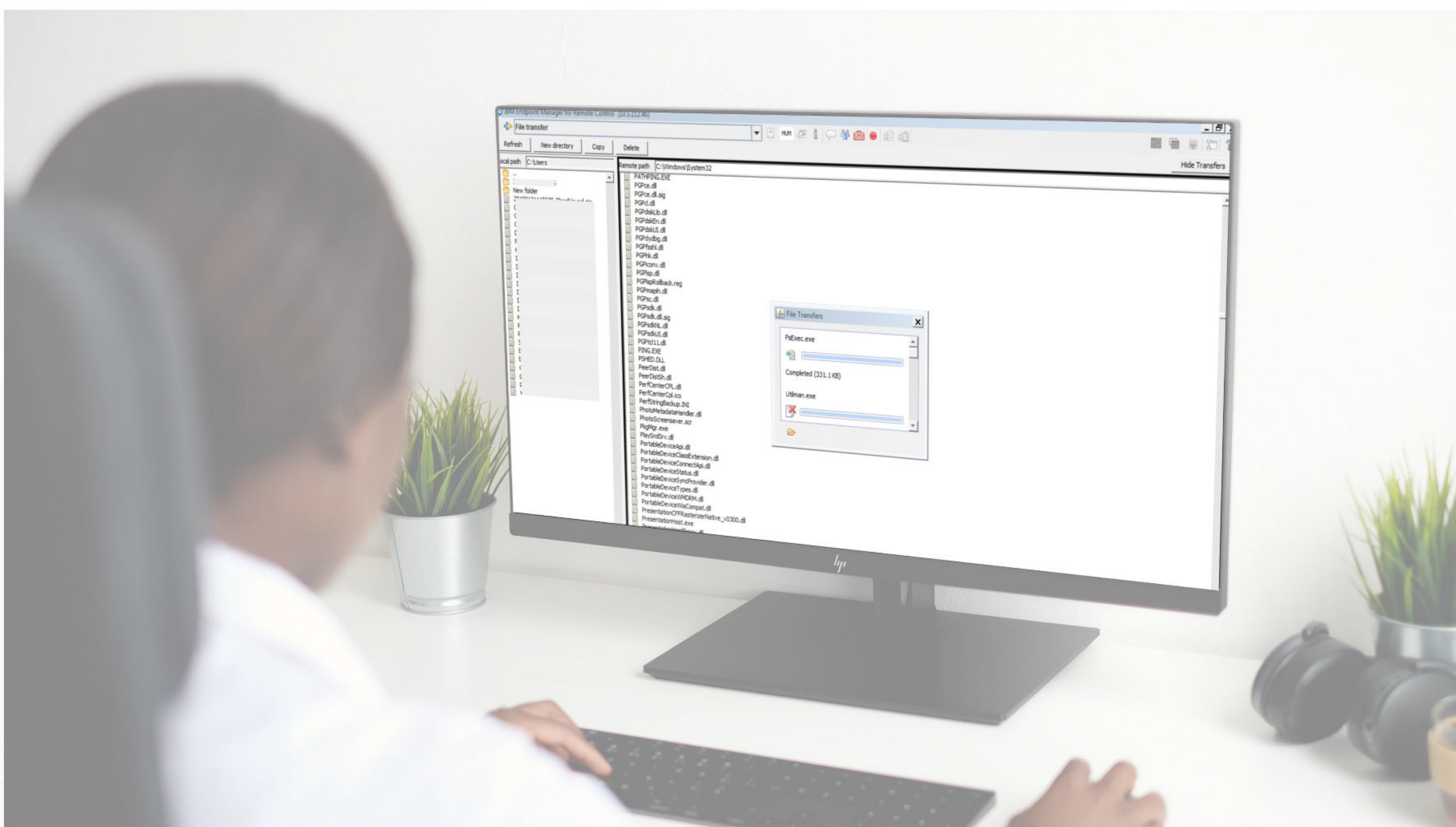


DAY 3.

BUG OR FEATURE

Day 3 started by accessing the Intranet Application and trying to find a way to execute a beacon on the server, but unfortunately the server did not have internet access. We started enumerating for privilege escalation and found several folders of different users in the C:\Windows\Users directory. This meant that many people logged in to the Intranet Application and if we could escalate our privilege, we could hit the jackpot. We also found a proxy server configuration on the Internet Explorer for this server, but it had been administratively disabled.

Upon further enumeration, we also found that this server had IBM endpoint manager installed. IBM endpoint manager is used by administrators to remotely control, copy files and manage remote hosts. We investigated the configuration of the IBM endpoint manager and found that there was a significant misconfiguration. If we started the IBM endpoint manager and requested access for our own host, it would give us the following options to remotely control our own host: monitor, manage and control. We selected the 'manage' option and found that it gave us full privileges to write to C:\Windows\System32 directory. To test our privileges, we successfully copied psexec.exe.



Now we started enumerating different services to check what we could overwrite. We had to be very specific with our selection. We could not overwrite a service that was running and we did not have any privileges to stop a running service. It meant that we would have to find a service which wasn't running, and was configured to run on boot. Once done we could then reboot the server so that our custom service was executed. We realized we had to be a little more creative than we initially imagined.

Upon further enumeration, we found a service which we anticipated no one was concerned about – McAfee Agent Backwards Compatibility Service. Now we had to find a way to copy a service executable to the remote machine which did not have internet access.

We quickly wrote a service file in C which ran cmd.exe as an administrator on boot and presented us with a cmd.exe console. We knew that we could not copy our file to the remote machine. With a quick hack, we wrote a python script on our local machine which read our local service file and emulated keystrokes to write the hex bytes of this file on to the remote machine.

Our idea was to convert the hex data to exe using powershell on the remote host once the hex bytes were fully written to the remote host in a text file. We left it overnight since writing a 100kb file can take up a large amount of time using keystrokes. We also made contact with our nominated client liaison for the Red Team project for permission to reboot the server.

 **INDUSTRY EXPERTISE**

Our consultants with shipping industry specific expertise were engaged for this assessment. It helps if the consultants know a typical environment for the client sector. Our consultants are experienced with critical infrastructure sectors – including energy, healthcare, and telecommunication providers.

 **REPORTS**

Detailed, concise reports with actionable recommendations were delivered at the end of the engagement to aid in remediating identified issues post-engagement.

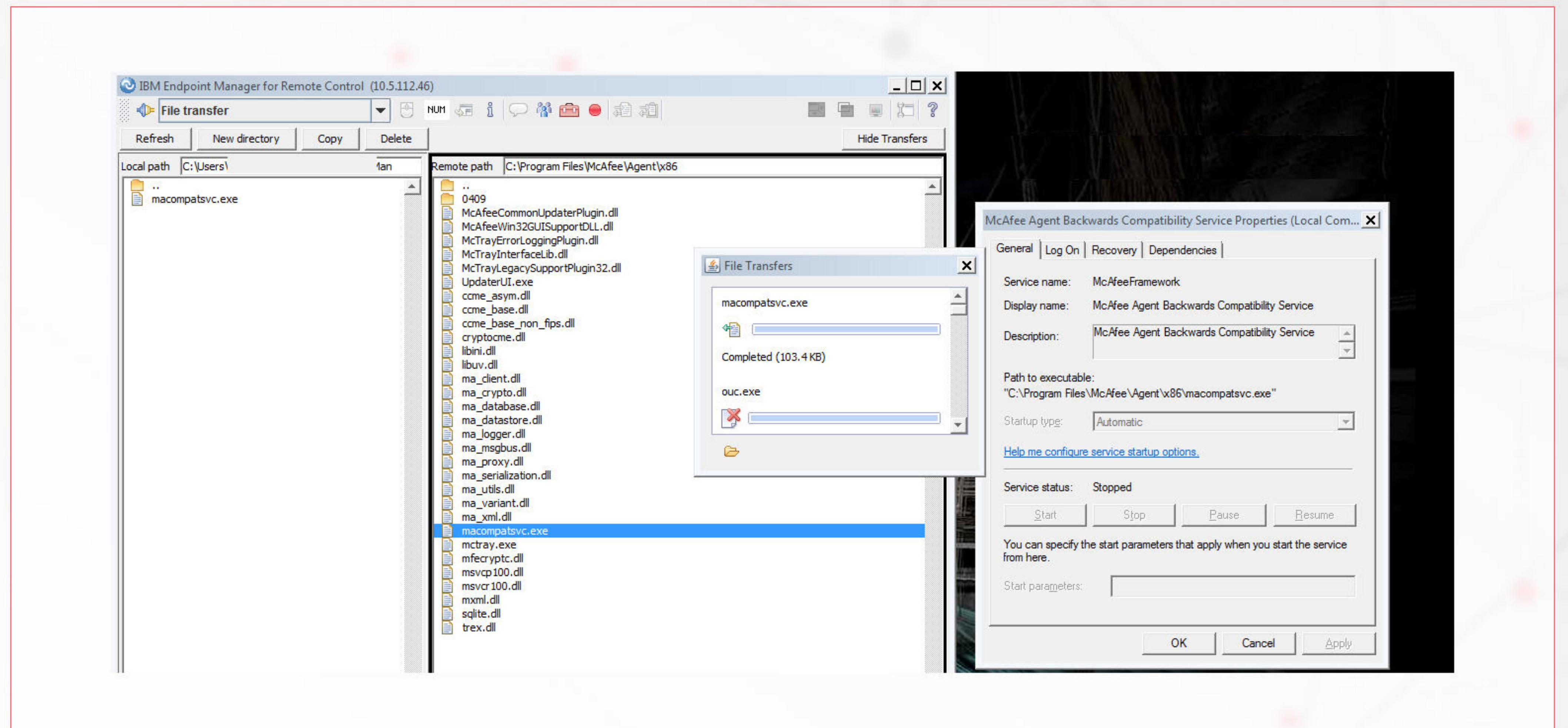
DAY 4.

THE RECKONING

We saw that our file was successfully written to the remote host and converted the hex bytes in the text file to executable to powershell. We decided to keep the same name as that of the McAfee service executable – **maccompatsvc.exe**.

Once we had copied the executable, we rebooted the server and successfully escalated our privilege to Administrator.

From here things looked easy. We could now enable the proxy server on our Internet Explorer and gain access to the internet.



We used a custom tool to dump the memory of Isass.exe using the PSCaptureSnapshot technique and uploaded the dump file to an AWS bucket since we knew that the organization used AWS from our initial recon. We then extracted the credentials from the dump file and found cleartext server administrator's credentials since wdigest was enabled on the server.

We directly jumped on to the Domain Controller (DC) using RDP from this server and were able to gain Administrative privileges on the DC. After gaining administrative privileges, we enumerated the User Groups and found the Developers groups. We used Dcsync to extract the NTLM hashes of the developers just in case we needed them for lateral movement.

We threw all the hashes to our cracking rig and went back to hunt for more information since our final aim was to gain access to their internal database. We needed to perform some silent reconnaissance to identify the roles of several developers.

DAY 4.

Active Directory does not disappoint when gathering User Role Names. As it was already after hours, we decided it might be the best time to login to the lead developers hosts to gather the database information.

We logged in using RDP to find their Outlook and Microsoft Teams sessions already running. We enumerated Outlook but didn't find anything important. We enumerated several applications, and in the end we found multiple unmounted drives using 'net view' command. We mounted these drives by directly navigating the path, and found a thick client application on one of the drives. Upon running this application, it requested Active Directory Credentials and we used the developer's credentials to login to the database.

RESULT!

Finally, we had reached the main goal of the assessment. It took a total of 4 days of persistent hard work, logic and a lot of creativity to finally breach a high level conglomerate.

Perhaps the best part of the whole assessment was that we didn't need to use our command and control centre since we had already backdoored the Citrix Gateway and we didn't use a single exploit or a hardcore phishing campaign where one single click of the user, plus a few misconfigurations led to the breach of the whole organization.

RECOMMENDATIONS

Penetration Testing Assessments are no substitute for Red Team Testing, they simply will not deliver the insights required to defend against real adversaries. This assignment again highlighted the need to:

1. Educate users by running at least one phishing awareness campaign per quarter and be ready for creative and realistic campaigns targeting your teams directly.
2. Educate users about having multi factor authentication and strong password complexity. The LMNTRIX team was able to easily crack the password with an in-house dictionary of keywords for a user account since the account password was constructed from commonly used keywords.
3. Continuously monitor critical networks and servers for random reboots and suspicious activities. As threat actors become more emboldened they move faster to capture the flag, and early detection and response of suspicious activity may be the difference between a compromised network and significant loss or damage.

ABOUT LMNTRIX ACTIVE OFFENSE

LMNTRIX Active Offense proactively evaluates your organization's ability to effectively prevent, detect, and respond to cyber threats before they disrupt business and become headline breaches. Receive pragmatic recommendations to improve processes, technologies and overall security posture.

To learn more, visit lmntrix.com.

LMNTRIX is the leader in intelligence led security-as-a-service. Working as a seamless, scalable extension of customer security operations, LMNTRIX offers a single MDR solution called Active Defense that blends our cyber defense platform called LMNTRX XDR with innovative security technology stack, nation-state grade threat intelligence and world-renowned Cyber Defense Centers. With this approach, LMNTRIX eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyberattacks.

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, UEBA and Deception Everywhere with completely automated attack validation, investigation, containment and remediation on a single, intuitive platform. Backed by a 24/7 Managed Detection and Response service – at no extra cost – LMNTRIX provides comprehensive protection of the environment for even the smallest security teams. It is a single investigative platform for insights into threats on enterprise, cloud, hybrid, and industrial control systems (ICS) networks. The LMNTRIX XDR delivers unique advantages over current network security solutions. It is a holistic and multi-vector platform with unlimited retention window of full-fidelity network traffic, innovative security visualizations, and the ease and cost-savings of an on-demand deployment model.

LMNTRIX, Inc.
333 City Blvd West, 18th
Floor, Suite 1805 Orange,
CA 92868 USA
+1.888.958.4555
info@lmntrix.com
lmntrix.com