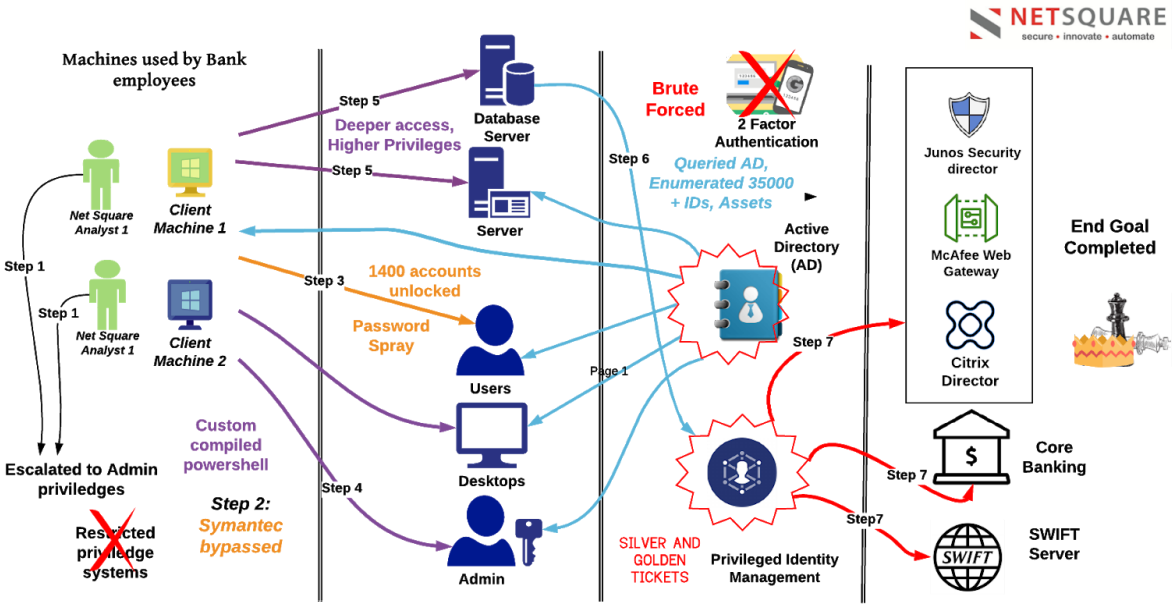
NETSQUARE
secure • innovate • automate

“5 days in a Bank”

As a CISO, you are no stranger to the question: “How effective is my Blue Team in discovering and responding to real time attacks?”

A case study of a Red Team exercise conducted on Net Square's banking customers revealed vital answers, not all of them being technical. Read on.



5 Days in Bank

THE SCENARIO

Net Square’s Red Team became “employees of the Bank” with 2 standard issue desktops loaded with the Bank’s baseline configuration. No administrator privileges or any network information was provided.

HOW IT ALL WENT DOWN

DAY 1	The first attack was obtaining Local Administrator privileges on the desktops, by reconfiguring the BIOS and booting off a USB pen drive.
DAY 2	Powershell restrictions enforced by Symantec and GPO policies were overcome by directly invoking .NET components using custom compiled code. Powershell was used to enumerate 35000+ accounts from Active Directory and took over 1400 users using a "password spray".

DAY 3	Lateral movement across the compromised user desktops yielded several critical assets - IP addresses of internal servers, connection shortcuts, credentials stored in text files, etc.
DAY 4	Privileged Identity Management (PIM) gateway compromised by brute forcing Google Authenticator 2FA tokens, owing to improper integration in the PIM product.
DAY 5	ENDGAME: Administrative/Super User access was obtained on ➢ Core Banking system. ➢ Citrix Director. ➢ McAfee Web Gateway. ➢ Junos Space Security Director. ➢ Underlying OS of SWIFT Server Golden and Silver tickets generated on AD with Read Only Domain Controls

INSIGHTS

- Attacks succeed because of a reactive approach to defense. "Defense doesn't mean Risk Reduction" as our CEO Saumil Shah says in his Blackhat 2017 Keynote [WATCH HERE]
- IT Security has never addressed the "human factor" when strategizing defense. Saumil emphasises "It's time to rethink user hardening efforts not from a one-size-fits-all perspective" - a different way of thinking about processes and policies.
- Bespoke applications are prone to having implementation and integration errors, as they are rarely subject to real world attack testing.
- It is vital to ensure a timely response from your organisation's Blue Team when faced with a real world attack scenario.

CATCH ME IF YOU CAN!

- A high volume of failed login attempts against the AD should have been detected and stopped by the Blue Team.
- Canary tokens (soft tokens) scattered around users' desktops and folders generate alerts when opened by attackers snooping around while moving laterally.
- A million login requests within 120 seconds were generated to brute force Google Authenticator, which should have been immediately alerted by the network monitoring team.

THE CISO STRENGTH TEST

Saumil concludes his keynote with a single thought:*"You should be doing something new every week. Try to bring one change at a time, measure whether the change is effective. This will improve user maturity to improve proactiveness in defense."*

NET SQUARE IS HERE TO HELP

Net Square's Red Team engagements helped reveal previously unseen gaps in all key aspects of our customers' defense strategy - people, process and technology, in that order.

A quick 25 minutes call with our security experts can give you great insights about how we can perform a **proof of concept Red Team engagement** for you. CLICK HERE to schedule a call at your convenience.

Thank you for reviewing the case study and we look forward to serving you.

Contact us on,
Net Square Solutions Pvt. Ltd.
1, Sanjivbaug, Paldi, Ahmedabad 380007 Gujarat

Contact person:
Prerna Nikam (prerna@net-square.com) - Cell no. +91 7977890081 or
Haresh Vanju (haresh@net-square.com) - Cell no. +91 9930950045

