NetSentries
SMART SECURITY~DELIVERED

AA

NetSentries Adversarial Attack
Simulation Exercise for FINSERV
For Banng Red/Purple Teaming

BANKING RED TEAMING

BANKING PURPLE TEAMING

OSINT & DARKWEB MINING

DEFENSIVE SECURITY ENABLEMENT

CSOC ENABLEMENT

ADVERSARY SIMULATION

4%
SURFACE WEB
access via search engines, URLs and content
90%
DEEP WEB
mostly excluded from search engine index
DARK WEB
6%
access only via special browsers (e.g. TOR)
SAFE LOCKER
BANK ACCOUNT
MONEY
BANK CARD
BANK CAR
BANK
MONEY CASE
EXCHANGE RATES
WAITING ROOM
AUTOMATED TELLER MACHINE
BANK OFFICE
ERROR
LOGIN
PASSWORD
HACKER

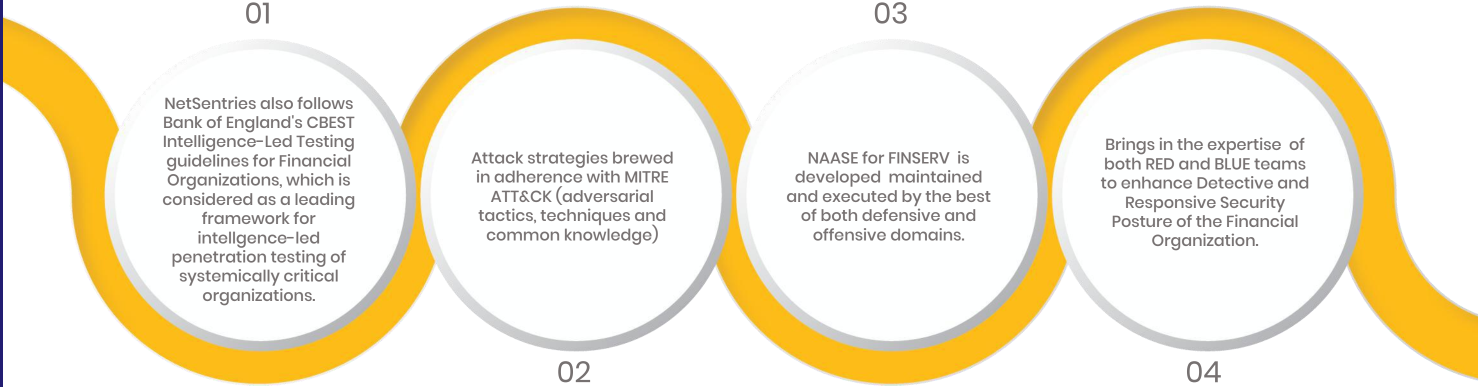
NAASE

NetSentries Adversarial Attack Simulaction Exercise for FINSERV

WHY NAASE FOR BANKING RED/ PURPLE TEAMING

NAASE - NetSentries Adversarial Attack Simulation Exercise fo FINSERV is the only program encapsulating the best practices of Bank of Singapore's Red / Purple team guidelines, Bank of England's CBEST and MITRE ATT&CK.

Red / Purple Team / Adversarial Attack Simulation exercises are developed in conformance with Guidelines for the Financial Industry by Association of Banks in Singapore (ABS)



01

NetSentries also follows Bank of England's CBEST Intelligence-Led Testing guidelines for Financial Organizations, which is considered as a leading framework for intellgence-led penetration testing of systemically critical organizations.

02

Attack strategies brewed in adherence with MITRE ATT&CK (adversarial tactics, techniques and common knowledge)

03

NAASE for FINSERV is developed maintained and executed by the best of both defensive and offensive domains.

04

Brings in the expertise of both RED and BLUE teams to enhance Detective and Responsive Security Posture of the Financial Organization.

FINANCIAL ORGANIZATION OSINT AND DARK WEB ENUMERATION

- During Open-source intelligence (OSINT) and Darkweb enumeration NetSentries will collect data about the target organization from publicly available sources to be used in an intelligence context for further phases.
- NetSentries finds, collects and analyze relevant datasets publicly available about your organization that can be used by adversaries for planning fraud or cyber attacks.
- The collected datasets are risk scored and correlated with each other for identifying possible unknown threat vectors.
- The business risk scoring helps organizations to take necessary preventive proactive actions.
- NetSentries also offers effectiveness review of organizations brand monitoring service as an optional add on.

COMMON DARKWEB DATASETS ENUMERATED

NetSentries Red Team will scour the Darkweb to identify possible latest hacker tools and tactics that can be used against the targeted organization. All active searchable Darkweb market channels will be surfed for existence of any kind of sensitive data like:

- Leaked ATM/Credit cards
- Stolen Bank accounts
- Sophisticated hardware hacking tools
- Rogue mobile applications mimicking on market products
- Infrastructure, Web app, mobile version related exploits in Dark Web (0day exploits)
- Accessibility of corporate web application with low latency anonymity browsers

- Intranet portals/ websites accessible from the internet
- Legacy systems used by the organization
- Corporate Email Addresses
- Backlinks to Corporate Domain
- Backlinks to Corporate Domain
- Disaster Recovery Locations
- Corporate Domain Name
- Brand Discussions
- Data center locations
- Geospatial information (e.g.,maps and commercial imagery products)

- Organizational public IP Addresses and devices
- Sensitive files / documents
- Known security solutions used
- Organization related Image / Video / Docs
- Organization related Image / Video / Docs
- Technology used
- VPN gateways and other perimeter devices
- VPN gateways and other perimeter devices
- Organizational Instant Messaging Channels
- Operating systems used
- Traditional mass media (e.g., television, radio, newspapers, books, magazines)

- Time Zone of operation work hours
- Organizational Social Network Accounts/ Social media profiles with organisation data
- Locations and Branches
- Compliance Standards followed
- Organizational Forums / Blogs / IRC
- Partner organization
- People Related- to Organization and Corporate Usernames
- Archives Related to Organization
- Organisational data in public Code repositories

- Archives Related to organization
- Investors in the organization
- Corporate VOIP infrastructure (exposed to the internet)
- Tools Used by the organization
- Investments by the organization
- File upload options (option for pubic to share info with bank)
- Mobile Applications owned and used by organization
- Autonomous systems BGP

COMMON OSINT DATASETS ENUMERATED

BANKING RED TEAMING

BANKING EXTERNAL RED TEAMING AND SPEAR PHISHING WITH CLEANET/DARKWEB ENUMERATION

01	02	03	04	05	06
OSINT and DARKWEB enumeration to collect datasets related to organization that can be used for adversarial actions.	Extreme Blackbox Penetration Testing all E banking and Mobile banking Channels with available public and Dark web exploits including zero days.	Advanced Spear phishing with custom evasive exploits and specially created landing pages.	Whaling, smishing and social engineering clubbed attacks.	Advanced post exploitation actions like persistency, lateral movement, data exfiltration and password dumping.	Access to phishing framework for Blue Team/SOC training.

BANKING INFRASTRUCTURE INTERNAL RED TEAMING BANKING OSINT AND DARK WEB ENUMERATION

Verify the effectiveness of logical and physical security controls related to People, Process and Technology like a determined insider attacker with:

- Network security control manipulation
- End point security control bypass
- Internal Security Gateways Control bypass
- Advanced Active Directory Information Gathering, Enumeration and Reconnaissance
- SQL Server Trust Abusing
- Kerberos and WMI attacks
- Privilege escalation
- Pivoting
- Advanced Lateral Movement (WMI, PS Remoting, DCOM, etc.)
- Critical Infrastructure OS Control Validation
- Internal aapplication Manual exploitation
- Advanced Persistence / Backdooring
- Data Exfiltration bypassing corporate security controls
- Enterprise Wireless Cracking

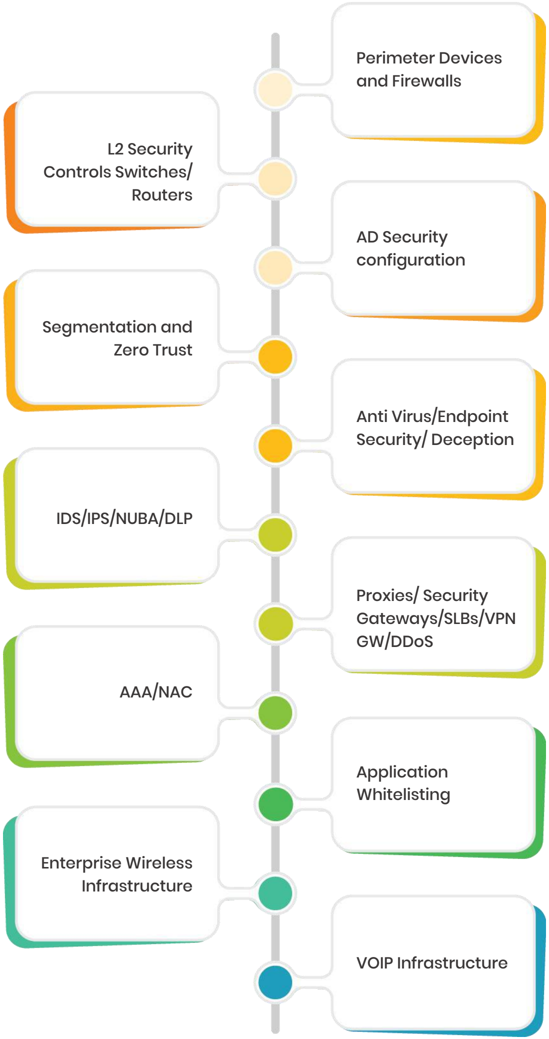
BANKING PURPLE TEAMING

As part of Purple Teaming NetSentries Team evaluates the effectiveness and proper implementation of thefollowing technologies :

NetSentries red team conducts objectives-based assessments that mimic known and quantifiable threat actors.

Banks blue team /SOC educate themselves around └ the Techniques, Tactics and Procedures, and build └ and configure their detection and response capability in-line with these known approaches.

Banks benefit from much more tailored, real-world assurance.



Perimeter Devices and Firewalls

L2 Security Controls Switches/ Routers

AD Security configuration

Segmentation and Zero Trust

Anti Virus/Endpoint Security/ Deception

IDS/IPS/NUBA/DLP

Proxies/ Security Gateways/SLBs/VPN GW/DDoS

AAA/NAC

Application Whitelisting

Enterprise Wireless Infrastructure

VOIP Infrastructure

REMEDIATION ENABLEMENT

DEFENSIVE SECURITY ADVISORY

- Remediation Recommendations for all failed defensive security controls
- Roadmap for remediation with prioritization of issues to be addressed
- Advisory for compensatory controls where immediate fix is not possible
- Guidance on virtual patching if required
- Selective patching recommendations for minimal business impact

CSOC INCIDENT DETECTION ENABLEMENT

- Strategic Planning Support for remediation of failed incident detection
- Generic recommendations on type of device logging to be enabled and rate limiting
- Recommendations on use cases for addressing detection failures reported

ADVANCED CSOC INCIDENT DETECTION ENABLEMENT

- Support for Log baselining, Events of Interest Definition, Selective Log Forwarding Recommendations, Use case/Correlation rule definitions ,monitoring dashboard development recommendations, Compliance monitoring and failed security control monitoring strategy definitions etc. to improve the Detection and Response Posture

EXECUTION PHASES

PHASE 0	PHASE 1	PHASE 2	PHASE 3
Scoping and Enumeration (DarkWeb and Clearnet, if external, RTPT is in scope)	Adversarial Simulations, control validations and remediation recommendation	Remediation Enablement	Effectiveness Validation

REMEDIATION ENABLEMENT

SMART SECURITY - DELIVERED

NetSentries Technologies a specialized Banking and FINTECH Cyber Threat Management Services company headquartered in Dubai, UAE with offshore service and Development centers in Bangalore and Cochin India.

75+ experienced consultants in various Information Security domains Providing Services to 40+ banks in the Middle East and Rest of Asia Presence and Partners across the Globe.

- Cyber Threat Management SAT
- GRC Enablement
- SOC Assessments & Threat Simulations
- IOT/ICS/SCADA Security
- Cyber Security Consulting
- Control Validations
- Cyber Security Staff Augmentation

We carry out extensive research and development on Cyber Threat Management with specific focus on the Banking & Finance Industry requirements.

CONTACT US

NetSentries Technologies FZCO,Techno Hub 2, Dtec, Dubai Silicon Oasis, P.O. Box: 644945 Dubai, United Arab Emirates

sales@netsentries.com

www.netsentries.com

+971 55 739 1463