DAAC digital.

Către: ”Termoelectrica” S.A.

Servicii de testare a securității sistemului informatic ”Termoelectrica” S.A.

Digitally signed by Sîrbu Ion
Date: 2023.08.28 14:12:55 EEST
Reason: MoldSign Signature
Location: Moldova

Semnat:_______________

Numele, Prenumele: Sirbu Ion

În calitate de: Director

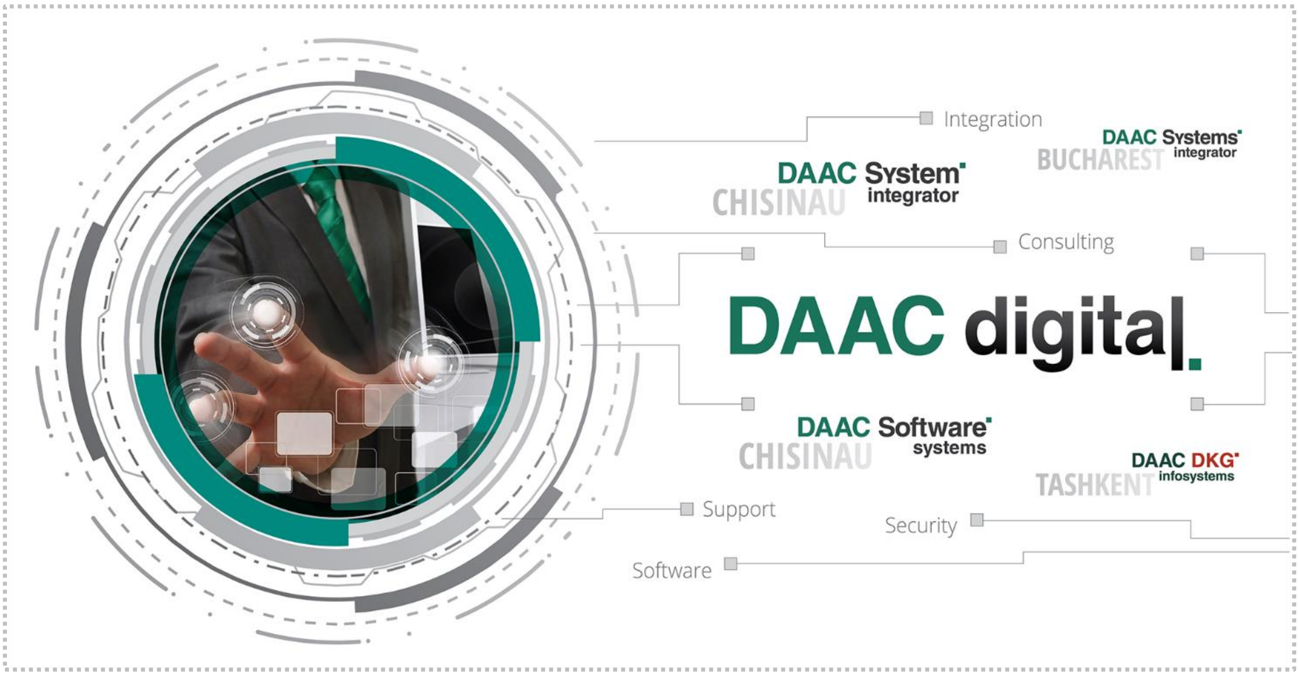
Ofertantul: DAAC Software Systems S.R.L.

Adresa: mun.Chisinau str.Calea Iesilor 10

Data: 29.08.2023

INFORMAȚII GENERALE

Companiile care aparțin grupului DAAC digital creează și implementează soluții inovatoare pentru sprijinirea digitală a dezvoltării informaționale a societății, statului și afacerilor. Companiile activează în Chișinău (Moldova), Tașkent (Uzbekistan) și București (România).



RESURSE ȘI EXPERIENȚĂ

Potențialul DAAC digital face posibilă implementarea unor soluții complexe din punct de vedere tehnologic și la scară largă pentru diferite sectoare ale economiei.

Portofoliul companiei include produse și servicii pentru consultanță, dezvoltare software, inginerie, securitate a informațiilor, precum și platforme hardware, software de producție proprie și peste 50 de furnizori internaționali.

200 ANGAJAȚI IT
ÎN TREI ȚĂRI

700+ CERTIFICARI
INTERNAȚIONALE

DEZVOLTĂRI TEHNOLOGICE ȘI
A PRODUSELOR PROPRII

CONCEPȚIE A LUCRĂRILOR

DAAC Software System SRL acceptă cerințele SA Termoelectrica (denumită în continuare Beneficiar) pentru a furniza diferite tipuri de evaluări de securitate, cum ar fi identificarea aplicațiilor vulnerabile și cu risc ridicat din rețea, inclusiv a celor expuse în Internet, și evaluarea vulnerabilității Infrastructurii rețelei, inclusiv infrastructura WiFi (fără fir).

DAAC Software System SRL în cooperare cu CT Defense SRL, Romania (denumită în continuare Executor) prezintă o experiență vastă și relevantă care este solicitată pentru a livra evaluări calificate de securitate TI. Avem o experiență semnificativă în Republica Moldova, în regiune, precum și în Europa și Asia, cu companii precum BNP Paribas (FR), Euronext (UE), Saltege (BG), Premialab (FR), Emirates NBD Bank (UAE), ADIB Bank (UAE) , Du (UAE), Autoritatea de Reglementare a Telecomunicațiilor (UAE), incl. Banca Mashreq. Am furnizat acestor entități servicii de înaltă calitate prin intermediul portofoliului de securitate TI. De asemenea, vom implementa lecții însușite din alte industrii de servicii de performanță, cu risc ridicat, pe care le-am executat, cum ar fi din domeniul industrial (petrol, gaze și aviația). Aceste proiecte ne-au permis să îmbunătățim și să extindem atât ofertele tehnice, cât și setul de abilități de management de proiect. Acest lucru permite Executorului să îmbunătățească continuu furnizările de servicii, să construiască un istoric consistent și să acumuleze cunoștințe de lucru despre operațiunile din regiune.

Deținem experiență în a face față provocărilor, riscurilor și problemelor tipice care apar atunci când lucrăm cu clienți precum SA Termoelectrica. Această familiaritate cu mediul de operare ne permite să abordăm rapid riscurile și să identificăm probleme specifice, precum și să prezentăm soluții la probleme pe măsură ce apar (și să ne bazăm pe experiențele anterioare). Echipa de management, precum și conducerea noastră se angajează să creeze un parteneriat de durată cu Beneficiarul prin selectarea de manageri de proiect în care suntem convinși că pot oferi servicii de calitate în care SA Termoelectrica poate avea încredere. În cele din urmă, suntem convinși că membrii echipei noastre reprezintă cel mai mare atu al nostru prin dezvoltarea unei echipe care este concentrată pe soluții, puternică din punct de vedere tehnic și cu experiență în lucru la unele dintre cele mai complexe proiecte de securitate din regiune.

În baza informațiilor deținute, Executorul întelege că SA Termoelectrica caută un furnizor de Consultanță în Securitate Informatică cu experiență necesară și relevantă în furnizarea de Servicii de Securitate, în diferite faze. Suntem încântați să depunem oferta pentru serviciile de securitate solicitate, așa cum este descris în acest document. Executantul depune această ofertă care include o abordare detaliată și scopul de activitate, iar în etapa ulterioară acest domeniu de aplicare și oferta se pot modifica conform cerinţelor înaintate.

SPECIFICAȚII TEHNICE

Anexa nr. 22
la Documentația standard nr. 115 din 15.09.2021

Numărul procedurii de achiziţie **21089329/ ocds-b3wdp1-MD-1692622074486**
Obiectul achiziţiei: **Servicii de testare a securității sistemului informatic TERMOELECTRICA S.A**

Denumirea serviciilor/bunurilor	**Denumirea modelului serviciului/bunului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	2	3	4	5	6	7
Lotul 1. Servicii de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA						
1. *Servicii de testare a securității și evaluare a vulnerabilităților informatice în cadrul Sistemului Informatic al Termoelectrica SA*				1. **Scopul serviciilor:** • Identificarea riscurilor asociate prin prisma prevederilor standardului SM EN ISO/IEC 27001; • Identificarea aplicațiilor vulnerabile și de risc sporit în rețea, inclusiv cele expuse in internet; • Evaluarea vulnerabilității infrastructurii de rețea inclusiv infrastructura wireless; • Elaborarea recomandărilor și planului de remediere cu măsurile tehnice și operaționale pentru eliminarea/minimizarea riscurilor identificate și evaluate ca cele critice. 2. **Obiecte de testare:** Principalele obiecte ale testării sunt: • Infrastructura de rețea (inclusiv echipamente active, routere, comutatoare). • Servere și gazde, inclusiv sisteme de operare și servicii. • Aplicație software utilizată în sistem. • Protocoale de comunicație și servicii de rețea.	**1.** Scopul serviciilor: Detalii privind realizarea scopului serviciilor sunt prezentate în secțiunea „Scopul serviciilor”. **2.** Obiecte de testare: Vor fi testate următoarele obiecte: • Infrastructura de rețea (inclusiv echipamente active, routere, comutatoare). • Servere și gazde, inclusiv sisteme de operare și servicii. • Aplicație software utilizată în sistem. • Protocoale de comunicație și servicii de rețea.	Fazele proiectului și activitățile efectuate vor fi aliniate la cele mai bune practici și standarde internaționale, descrise în capitol I. „Project Management and Services Methodology”

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				• Aplicații web. 3. **Metode de testare:** Pentru atingerea obiectivelor stabilite se vor aplica cel puțin următoarele metode de testare a securității cibernetice: • Analiză externă (mediul informațional al sistemului, zonele de domeniu etc.). • Scanarea pentru vulnerabilități. • Testare de penetrare - folosind instrumente și metode specializate (vezi punctul 7). Vor fi utilizate cel puțin 2 tipuri de teste: - Testele automate – vor identifica erori de programare în aplicațiile utilizate şi vor fi efectuate cu ajutorul unor aplicații specializate precum instrumentele de scanare a vulnerabilităților, a aplicațiilor web și a codului, instrumente de testare și identificare a eventualelor erori de programare din aplicații în vederea exploatării lor. - Testele manuale – vor analiza aspectele ale aplicațiilor care necesită intuiția umană, identificând-se erori logice de programare, și vor analiza și confirma sau infirma rezultatele testelor automate. • Analiza codului (dacă este necesar). • Inginerie socială (verificarea nivelului de conștientizare a personalului cu privire la securitate).	• Aplicații web. **3.** Metode de testare: Metodele utilizate pentru testare a securității cibernetice sunt prezentate în următoarele secțiuni: I. “Project Management and Services Methodology”: • General approach; • Vulnerability assessment/penetration test; • External Penetration Testing; • Escalating privileges; • Penetrating the network/exploit the weaknesses; • Application layer attacks; • Network/infrastructure attacks; • Exploitation attack scenarios; • Application layer attacks. II. Internal Network Security Assessment methodology (Active Directory Flag capture): • Initial access; • Execution; • Persistance; • Privilege Escalation; • Defense evasion; • Credential access; • Discovery; • Lateral Movement; • Collection, Command and Control; • Exfiltration and Impact III. Application Penetration Testing: • Injection; • Briken authentication; • Sensitive data exposure; • XML External entities; • Broken access Control; • Security Misconfiguration;	

www.integrator.md

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				4. **Lista vulnerabilităților și aspectelor de securitate pentru a fi testate:** • Deficiențe în configurarea echipamentelor de rețea. • Deschiderea de porturi și servicii disponibile în rețeaua externă. • Puncte slabe în autentificare și control al accesului. • Vulnerabilitatea aplicațiilor web • Posibile vulnerabilități de securitate fizică. 5. **Planul de testare:**	• Cross-site scripting; • Insecure decentralization; • Using components with known vulnerabilities; • Insufficient Logging & Monitoring. Analiza codului (dacă fa fi necesar). Inginerie socială: Va fi verificat nivelul de conștientizare a personalului cu privire la respectarea cerințelor de Securitate prin următoarele activități: • identificarea personalului din cadrul organizației expuși riscului prin accesarea informațiilor din Internet/rețelele sociale, implicând conturile oficiale ale organizației; • simularea atacurilor de phishing ; • verificarea Active Directory la prezența mai multor vulnerabilități legate de parole; • identificarea parolelor neconforme și vechi salvate în browserele Chrome, Firefox și Edge; • Verificarea utilizării parolelor compromise, disponibile public asociate domeniului dvs. **4.** Lista vulnerabilităților și aspectele de securitate vor fi testate în conformitate cu informațiile, specificate in secțiunile: I. Project Management and Services Methodology II. Internal Network Security Assessment methodology (Active Directory Flag capture) III. Application Penetration Testing IV.Inginerie socială (este detailată anterior în secțiunea 3.Metode de testare) **5.** Planul de testare este prezentat în secțiunea IV.“Project time line”	

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				Va conține minim următoarele faze: ➢ **Faza de colectare a informațiilor:** • Identificarea scopurilor de testare și formarea unei ipoteze de lucru. • Colectarea de informații despre sistem (domeni IP, domenii, informații despre personal etc.). ➢ **Faza de scanare și de detectare a vulnerabilităților:** • Utilizarea scanerelor de vulnerabilitate pentru a găsi porturi și servicii deschise. • Utilizarea instrumentelor specializate pentru detectarea vulnerabilităților. ➢ **Analiza vulnerabilității si faza de exploatare:** • Încercările de a exploata vulnerabilitățile găsite pentru a obține acces neautorizat. • Analiza rezultatelor încercărilor de exploatare. ➢ **Faza de analiză a securității aplicației web:** • Verificarea aplicațiilor web pentru vulnerabilități precum SQL injection, XSS etc. ➢ **Faza de analiză Testarea securității sistemului de e-mail:** • Verificarea vulnerabilităților precum refuzul serviciului (DoS) sau injectarea de cod rău intenționat. • Autentificarea utilizatorului și verificări de autorizare pentru a preveni accesul neautorizat. • Testarea posibilității de interceptare a datelor și analiza traficului pentru a asigura protecția datelor.	Fazele și metodologia efectuată sunt prezentate detailat în secțiunea I.“Project Management and Services Methodology”	

www.integrator.md

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				- Verificarea posibilității de acces la distanță la căsuța poștală prin protocoalele POP3, IMAP, SMTP. **6. Lista instrumentelor pentru efectuarea testelor de penetrare:** *Notă: Lista instrumentelor nu este obligatorie, specificate în termenii de referință și pot fi utilizate altele alternative, care depind de obiectivele specifice ale testării și de caracteristicile obiectelor. Utilizarea fiecărui instrument, trebuie să fie coordonată în prealabil cu proprietarul sistemului/aplicației/rețelei.* **6.1. Scanere de vulnerabilitate:** - **Nmap:** Pentru a scana rețeaua pentru gazde active și porturi deschise. - **OpenVAS:** Pentru a detecta vulnerabilități cunoscute în serviciile de rețea. - **Nessus:** Pentru detectarea vulnerabilităților și analiza securității rețelei. **6.2. Instrumente de analiză a aplicațiilor web:** - **Burp Suite**: Pentru analiza securității aplicațiilor web, interceptarea și modificarea traficului. - **OWASP ZAP:** Un instrument gratuit pentru descoperirea vulnerabilităților în aplicațiile web. - **Sqlmap:** Pentru a automatiza detectarea și exploatarea injecțiilor SQL. **6.3. Instrumente pentru testarea vulnerabilităților rețelei:**	**6.** Lista instrumentelor pentru efectuarea testelor de penetrare sunt detailate în secțiunea VIII"Lista instrumentelor/platformelor utilizate"	

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				• **Metasploit Framework**: Pentru a verifica vulnerabilitățile rețelei și pentru a exploata vulnerabilitățile. • **Wireshark:** Pentru a analiza traficul de rețea și a identifica vulnerabilitățile. **6.4. Instrumente de analiză a securității codului:** • **FindBugs**: Pentru a găsi vulnerabilități în codul Java. • **Bandit:** Pentru a scana codul Python pentru vulnerabilități. **6.5. Instrumente pentru analiza rețelelor wireless:** • Aircrack-ng: Pentru analiza securității rețelei wireless și cracarea WPA/WPA2 PSK. **7. Restricții** Restricții care pot afecta testarea, cum ar fi: • Fără testare în timpul programului de lucru. • Interzicerea utilizării anumitor instrumente sau metode. **8. Rezultate așteptate:** • Raport asupra testării efectuate cu o descriere detaliată a vulnerabilităților, riscurilor identificate și recomandări pentru eliminarea acestora.	7. **Restricții** Testarea activă care poate impacta funcționalitatea rețelei va fi executată în afara orelor, agreat cu clientul, ramânând pentru echipa tehnică să efectueze testele non intrusive în restul timpului astfel încât să fie asigurat 0 downtime. Acest mod de lucru este urmat în alte cazuri similare, astfel ca să nu încurce buna desfășurare a proiectului. Vor fi utilizate doar instrumente ce sunt prezentate în secțiunea VIII.“Lista instrumentelor/platformelor utilizate” **8. Rezultate așteptate:** Informații privind rezultatele așteptate sunt detaliate in secțiunile: • VI. Threat Classification and Reporting; • VII. Project deliverables	

www.integrator.md

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				• Evaluarea eficacității mijloacelor existente de protecție și de detectare a incidentelor. • Descrierea detaliată a încercărilor reușite și nereușite de a exploata vulnerabilitățile. Raportul de evaluare va conține cel puțin următoarele capitole: - Sumar executiv - Obiectivele și scopul evaluării - Prezentarea metodologiei utilizate în cadrul testării - Descrierea contextului în care s-a desfășurat testarea - Detalii despre rețeaua și sistemele evaluate - Prezentarea individuala a vulnerabilităților descoperite: ○ descrierea vulnerabilității ○ catalogarea vulnerabilității ○ descrierea tehnică ○ analiza severității și probabilității ○ calcularea riscului ○ contramăsuri recomandate pentru mediere - Anexe cu lista testelor de securitate efectuate. **9. Condiții de testare:** • Testarea trebuie efectuată într-un mediu de testare dedicat pentru a evita impactul negativ asupra sistemului de producție.	**9. Condiții de testare**: Testarea activă care poate impacta funcționalitatea rețelei va fi facută în afara orelor, agreeat cu clientul, ramânând pentru echipa tehnică să efectueze testele non intrusive în restul timpului astfel încât să fie	

www.integrator.md

Denumirea serviciilor/bunurilor	Denumirea modelului serviciului/bunului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
				• înainte de testare trebuie sa fie aprobat de beneficiar programul de testare. Testarea nu ar trebui să degradeze performanța sistemului sau să compromită disponibilitatea sistemului.	asigurat 0 downtime. Acest mod de lucru este urmat în alte cazuri similare, astfel ca să nu încurce buna desfășurare a proiectului.	

Semnat:_______________

Numele, Prenumele: Sirbu Ion

În calitate de: Director

Ofertantul: DAAC Software Systems S.R.L.

Adresa: mun.Chisinau str.Calea Iesilor 10

SCOPUL SERVICIILOR

Scope Description

Executor will perform different types of assessments, in different cycles. The type of assessments will be discussed and agreed upon (as part of the timelines) with the client, before initiating the engagement.

Executor proposes to conduct Security Services divided into phases as described below:

A. External Network Security Assessment (Black-box and Gray-box)

Covers the following:

- Reconnaissance and discover infrastructure.
- Security audit of published web applications.
- Performing exploitation services in safe-mode
- Documentation on how each reported vulnerability can be exploited.
- Provide Black-box testing outcomes in report. Including in the report, the recommended remediation of each vulnerability found.
- Black Box and Gray Box approaches
- Vulnerability Assessment and Penetration Testing on the external Infrastructure
- IP security testing
- Retesting in the scope of work
- Multiple reports: gray box and Black box, Technical, Retest, Management, Final report

Reconnaissance and Asset Discovery

- Discovery of IP addresses belonging to Customer
- Discovery of Domains and Subdomains including CIDR ranges belonging to Customer
- Updating the External IP Scoping Sheet
- Confirm assets with CustomerTeam and report activities

Vulnerability Assessment and Penetration Testing for exposed assets

- Vulnerability Assessment and Penetration Testing on Customer exposed external facing assets
    - o Subdomains
    - o IP addresses
    - o Domains
- Reporting

Application Security Testing for Customer's IT Applications

- Penetration Testing activities, based on OWASP methodology, NIST, and PTES approach, cover the level of security– ASVS checks included, for the following:
    - o Authenticated and Unauthenticated testing

- Reporting real-time, on High-severity alerts/findings, final reports – for each application
- Re-testing in the scope of work

B. Internal Network Security Assessment (Black-box and Gray-box)

Covers the following:

- Black Box and Gray Box approaches
- Reconnaissance and Discover Customer's infrastructure
- Security audit of internal web applications.
- Performing exploitation services in safe-mode
- Active Directory assessment
- Scenario-based assessments
- Testing from different networks
- WIFI Security Assessment
- Network-specific testing based on PTES methodology and NIST framework
- Retesting in the scope of work
- Multiple reports: gray box and Black box, Technical, Retest, Management, Final report

Penetration Testing for the Internal Network Infrastructure

- Vulnerability Assessment and Penetration Testing on Customer's for the Internal Infrastructure
    - o Segmentation testing
    - o Scenario-based assessments
    - o Testing from different networks
    - o Network-specific testing based on PTES methodology and NIST framework
- Retesting in the scope of work
- Reporting

Social Engineering by real Phishing Attack simulation

- Determine the vulnerability level of Customers network by giving an indication of how many users may be susceptible to an email-born social engineering attack.
- The results of the test include the number of users who failed the test divided by the number of users to whom the test was delivered.

Out of scope

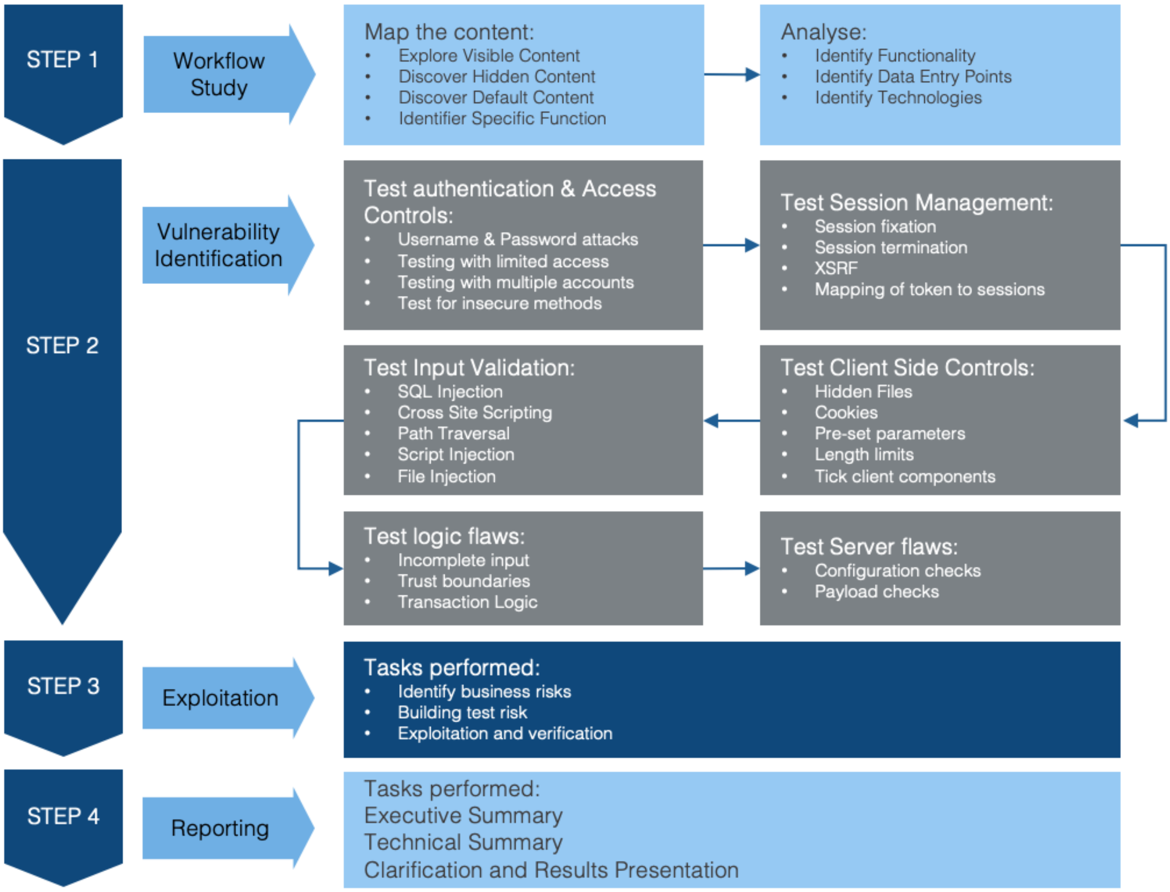
- Source Code and Configuration Reviews

I. PROJECT MANAGEMENT AND SERVICES METHODOLOGY

This chapter presents methodologies for different cyber-security services. The final project execution approach might be adjusted depending on actual scope, dependencies, and specific requirements or constraints given by Customer during the kick-off of a particular engagement.

1. GENERAL APPROACH

In order to meet all requirements requested by Customer every activity we divide into the following main steps:



The steps are aligned to the in-depth security concepts and are focused on process and technical security controls and their implementation in the various phases of the project delivery. The results provided for each activity will include detailed and comprehensive assessments of Customer's security posture, expansive recommendations, and tools and knowledge to facilitate continuous improvements. For each activity, Customer will nominate relevant employees to ensure smooth knowledge transfer and prerequisites preparation.

The project phases and activities performed will also be aligned with international best practices and standards such as:

- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- Open Web Application Security Project (OWASP) Testing Guide
- The National Institute of Standards and Technology (NIST)
- PCI Data Security Standard Penetration Testing Guidance (PCI DSS)
- The Intelligence Lifecycle & F3EAD Cycle (Threat Intelligence)
- OWASP Mobile Security Testing Guide (MSTG)

- Penetration Testing Framework for IoT (PTFIoT)
- PCI DSS ATM Security Guidelines
- CIS Cloud Foundations Benchmark Standard
- OWASP Code Review Guide
- Threat Intelligence Based Ethical Red Teaming Framework (TIBER-EU)
- Application Security and Development Security Technical Implementation Guide
- Social Engineering Attack Framework and Toolkit (SET)
- Digital Forensics Framework (DFF)
- Incident Response Framework (NIST)
- Secure Controls Framework (SCF)
- CREST Penetration Testing Guide
- CSA STAR Self-Assessment / CAIQ
- CIS Secure Platforms Benchmarks (CIS Security)
- Application Security Verification Standard (ASVS)

2. VULNERABILITY ASSESSMENT/PENETRATION TEST

Our vulnerability assessment/penetration test (VA/PT) service is designed to provide a comprehensive overview of technical security issues throughout your environment. Our services are aligned to the requirements set forth in standards and initiatives such as ISO/IEC 27001, COBIT 5, the ISF Standard of Good Practice, Open-Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), National Institute of Standards and Technology Special Publication 800-115, the Information Systems Security Assessment Framework (ISSAF), and Penetration Testing Execution Standard (PTES). We can also provide a comparative gap analysis against relevant standards such as PCI/DSS, NERC, HIPAA, or other regulatory requirements as may be specified in the project scope.

The assessment will be conducted from an external perspective. Using industry-standard scanning tools as well as manual discovery techniques, our team will interact with and assess the security of each device in your network, in accordance with the scope of work. Each device will be assessed to determine the services that it offers, the versions of the associated software and hardware, the security configuration of the device, and the resulting security posture of the device.

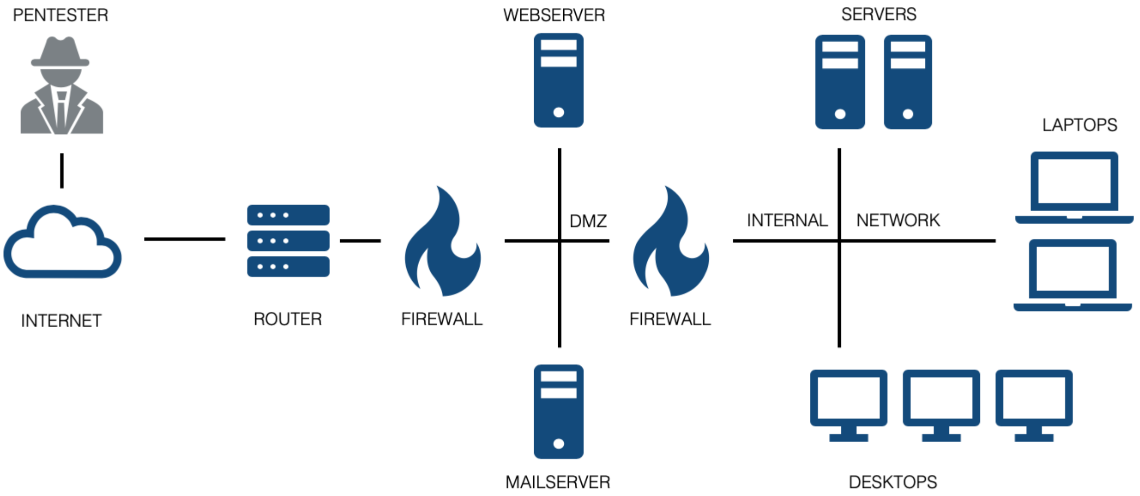
Examples of the types of testing that may be performed during this phase include but are certainly not limited to:

- Network mapping and enumeration
- Port scanning
- Vulnerability scanning
- Local area network manipulation attempts
- IP address spoofing
- Vulnerability validation
- Authentication attacks
- Network monitoring

After initial vulnerability scans and associated tests are conducted, our engineers will analyze the results and perform additional manual testing. These additional tests are designed to verify initial findings, understand the potential business impact of the technical findings, and explore ways in which an attacker could potentially exploit the identified vulnerabilities, either directly or by combining a series of exploits into an attack chain, which can result in further penetration into the network and risk the business.

3. External penetration testing

The goal of the Penetration Testing activities is to assess the security of Customer`s external IT infrastructure and Web Applications that are in scope (and not only), by simulating hacking attacks:



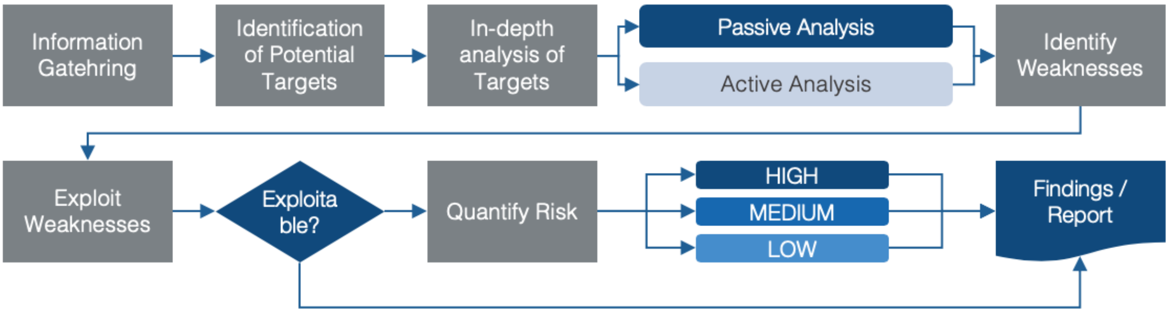
Attacks can usually be approached from different perspectives. Typical examples of such are:

- An external attacker that has no prior knowledge or access to the application/infrastructure.
- An external attacker that has limited access. E.g. a customer using your web application or a disgruntled employee
- An internal attacker. e.g., an employee.

The security assessment to be performed is a Penetration test. This means that the focus will be to attempt to penetrate OTP Bank's networks from every aspect rather than drawing up a list of low/medium vulnerabilities found on each machine.

Under no circumstances will there be an attack against any other system than those belonging to Customer, and no possibly destructive tests will be performed without prior authorization, this includes DoS (Denial of Service), DDoS (Distributed Denial of Service), and compromise of production servers.

The diagram that follows outlines the external penetration testing methodology to be followed by security engineers.



As part of external penetration test the following tasks are performed:

- Information Gathering and Network Mapping

The purpose of this first stage of the tests is to get a clear picture of the network, the types of systems, and the services running on the different systems.

Following tests will be performed:

- Find publicly available information about the network on the Internet. This includes querying the WHOIS databases, search engines, news groups and mailing lists archives, etc.
- Portscan all IP addresses in the network (UDP/TCP) to determine which systems are alive, what services are running, and the types of operating systems.
- Use network-mapping tools to determine the structure of the network.
- Use banner-grabbing techniques to determine the type and version of the services running.
- Query DNS servers for information gathering purposes (attempt zone transfers, DNS scans, etc.).
- Identification of potential targets
- In-depth analysis of targets
- Identification of weaknesses

During this stage, the different found services will be tested against known vulnerabilities and other security related problems.

Where applicable, brute-forcing techniques will be used to test for weak passwords. It is impossible to provide test outlines for all different services that may exist on the systems in your network.

Our team has years of experience in performing security audits. This gives you the assurance that our engineers possess the know-how needed to successfully complete such audits.

All our staff has vast experience in managing and auditing the majority of popular Operating Systems and Services: UNIX, Windows, Web servers/applications, mail servers, database servers, etc.

3.1 ESCALATING PRIVILEGES

In a lot of cases, an exploited vulnerability gives the attacker only limited access to the system. By exploiting another local vulnerability on the system, it may be possible to further compromise the system and get full access. This is usually Administrator or SYSTEM access for Win32 or root access for *nix systems.

Once an attacker gets full access, tools and utilities can be installed on the systems, which allow to further penetrate the network.

Please note that DAAC Digital engineers keep full track of all changes that are made to any system and tools installed and these changes are undone as soon and to the extent possible.

3.2 PENETRATING THE NETWORK/EXPLOIT THE WEAKNESSES

Once one of the systems in a network has been compromised a number of new possibilities become available to attack other systems and dig further into the network.

Because of the fact that the compromised system is installed on some ‘internal’ network segment, different (or no) firewall rules will be applicable. This means that probably more systems and services will be visible to the attacker.

When NAT/PAT is used, the attacker can now connect to IP addresses that are not routed to the Internet.

The attacker can use packet sniffers on the compromised system(s) to gather information, passwords, etc. that will help to attack other systems.

In a lot of cases, administrators use the same accounts and passwords on different systems. Passwords that are cracked on the compromised system may work on others.

Attacks can be used that are only possible on a local network segment or that are using other protocols than IP.

4. Application layer attacks

These activities will be dependent on the applications discovered on the infrastructure. This information should be provided beforehand to focused on the approach on the specific applications, which will be assessed for network reachability and then subject to application layer attacks and assessment. These are not restricted to the following:

4.1 ACTIVE PROGRAM SCRIPTING EXPLOITS

This activity will utilise injection of malicious scripts into the targeted infrastructure in order to determine the capability of the security infrastructure in detecting and preventing these unwanted traffic penetrating into the network. These malicious scripts can be of several scripting language such as Java, Javascript, ActiveX or VBS which will be injected into the targeted systems/hosts. Scripting exploits generators such as Metasploit and WebScarab will be utilised to generate and launch these traffics into the targeted network. These activities will determine the application layer inspection capability of the current IDS/IPS.

4.2 MALICIOUS PROGRAMS ATTACKS

These include programs such as Trojan Horses, Worms, Viruses and Backdoors which will be injected into the network to check the capability of the security infrastructure (firewalls, IDS, IPS) in detecting and preventing these malicious programs. Common programs such as Trojans (Trinoo, BackOrifice), Exploit worms (Zotob, Sasser) among others will be tested for detection and prevention.

It is important to mention that no malicious programs or scripts will be deployed on any production system environment. The scenario will utilise a dedicated target host(s) deployed within a specific network wherein it will launch or receive the attacks from another source outside the network of concern. This is much like a client-server approach to launch the scripts and malicious programs.

The security infrastructure particularly the firewalls, IDS, and IPS will be tested for their capability in detecting and mitigating these attacks into the network. This will check if the security infrastructure is currently up to date in its detection capabilities such as signature matching and so forth.

5. Network/infrastructure attacks

These attacks are focused on the manipulation of the TCP/IP protocol in order to craft packets into the infrastructure in order to conduct security assessment on the network.

- Port Scanning – This will be used to detect running services exposed on the targeted hosts and devices. Port scanners (particularly nmap) will be utilised for this activity targeted to the network ranges provided. It will utilise most type of scans including TCP scanning (i.e. Full-TCP, Half-Open, RST, NULL scans), UDP scanning and so forth (ACK scan, FIN scan). Similar to the ICMP sweeps, these packets will be generated from strategic location specifically from the User VLAN and the external interfaces particularly facing the Internet and will target the IPS Infrastructure. These activities will also focus in the detection capability of the IDS and IPS in detecting and deterring service discovery and enumeration which are important for any attacks gathering information about vulnerable services on the targeted network. Packets variation will include fragmented packets as well as IDLE scans to minimise detection
- IP Spoofing – This activity will focus on the resilience of the network infrastructure in handling spoofed packets pretending to be other systems/hosts. Specific systems and

networks will be subjected to IP spoofing to determine if the spoofed IP address can pass through the network and through the security devices. These activities will focus in the proper network protection of the infrastructure (i.e. router and switches) in handling spoofed packets as well as the security devices (firewalls, IDS, IPS) in detecting these anomalous packets. Generated packets will utilise spoofed address belonging within the IP address range allocated to the target network. These will be generated from the User VLANs and the other external interfaces particularly facing the Internet. In addition, the network will be tested for basic ingress filtering utilising address space from the reserved IP address space. Information about the network infrastructure is important in order to launch effective spoofing attacks to determine how the network/security devices prevent these unwanted packets.

- Most of the activities are utilised for network reconnaissance whose information gathered will be utilised to launching succeeding attacks. These other succeeding attacks will focus on the previous gathered information from the targeted environment and exploit these services.

6. Exploitation attack scenarios

These are scenarios more focused in determining the posture of the security infrastructure (Firewalls, IDS, IPS) to detect attacks in several situations. For these activities to be conducted, it is required to have a least a dedicated host(s) deployed in the same network segment within the critical systems. This would require physical network access, VLAN membership as well as allocated IP address within the same network segment.

Strategic locations on the network will be identified to determine the most effective ways in conducting these activities. These activities will focus in the determining the current mechanism in place protecting sensitive information passing through the network. These attacks include different scenarios from intercepting the traffic flow between systems, manipulating the traffic and injecting altered information into the network. Aside from these, scenarios include bypassing access controls within targeted networks by utilizing exploitation of trust relationship as well as utilizing port redirection and covert channels.

These attacks are not focused in the determining the security of the targeted host but on the resilience of the network in protecting against such attacks if ever one the hosts are compromised.

- IP Sniffing – These will focus in the interception of data propagating into the network infrastructure particularly where transaction occurs between critical and sensitive systems. This is done by installing dedicated host(s) with interfaces in promiscuous mode in order to passively collect traffic in strategic locations across the network of interest. Common tools such as tcpdump and wireshark can perform these activities. A combination of Layer 2 header manipulation (i.e. MAC address spoofing) will be utilised in order to intercept and hijack specific traffic of interest especially communications between sensitive systems. These activities will also focus in determining the security of the switching infrastructure in preventing such attacks from occurring across the infrastructure.

- Traffic/Data Manipulation – Aside from sniffing the traffic across the infrastructure, the packets captured in transit will be manipulated and its payload altered based on the information gathered and analysed. These will utilise a combination of data manipulation techniques depending on the capture traffic from Web Traffic (HTTP/HTTPS), Email Traffic (SMTP/POP/IMAP), DNS, Remote Authentication (Telnet, SSH) and even Database transactions (Oracle, SQL). These activities will be focused on the capabilities of the security infrastructure (firewalls, IDS, IPS) in detecting and preventing these attacks. Utilising the collection of tools from dsniff and packet injectors particularly hping, scapy and packit, captured data traffic can be intercepted, manipulated and injected back into the network. The main focus of these tests is to determine the capability of the security infrastructure in detecting and preventing these traffic manipulation scenarios.

- Trust Exploitation – These activities will focus in exploiting the inherent trusted relationship between systems and network segments in the infrastructure. These will utilise several variations in order to exploit these such as IP spoofing, Sequence Number prediction, and crafted payload attacking R-services, NIS, and so forth. Packet crafting tools will be utilised to launch these packets such as hping and scapy. It is important to gain proper understanding of the current infrastructure in order to effectively exploit these trusted relationships. These activities will focus on the resilience of the network in deterring such exploitation. It will also determine if the current security configuration of the firewalls are able to ensure the communication flows only in the proper direction on the proper service.
- Port Redirection – These activities will focus on bypassing security controls on network. Tools such as HTTPTunnel and NetCat will be utilised for the port redirection attacks. These activities will target specific locations in the network to conduct port redirection attacks. However, these activities require physical access on the network of interest in order to launch these attacks. This can be conducted by using dedicated hosts listening or if possible, install port redirection tools in one of the systems to test these attacks. These activities will test the configuration of security devices (firewalls, IDS, IPS) in detecting and preventing these unwanted traffics to/from the network.

It is important to consider that these attack scenarios will require the information from the previous activities conducted over the network infrastructure. Moreover, it will be important to remember that production systems currently in place in the network will not be subjected to deployment any tools or programs without proper authorization. This will ensure non-disruption of network services current in production. Particular services that will be targeted for these activities are Web (HTTP/HTTPs) traffic session, Telnet (SSH) remote access, email (SMTP/POP/IMAP) traffic and FTP transaction.

Most of the scenarios will simulate the attacks by utilizing a client-server situation wherein from dedicated host(s) deployed within the network of interest and other host(s) are deployed externally.

For these attacks scenarios to be effectively conducted, usually a physical network access is required to launch these tests.

7. Application layer attacks

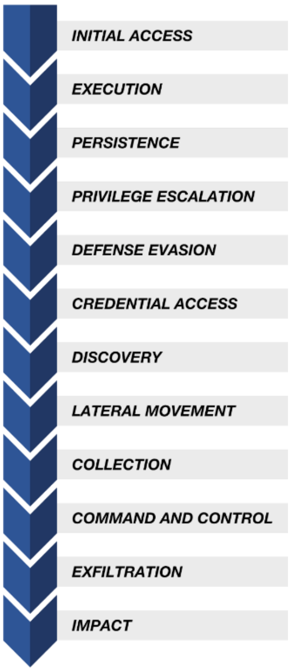
These activities will be dependent on the applications discovered on the infrastructure. This information should be provided beforehand to focused on the approach on the specific applications, which will be assessed for network reachability and then subject to application layer attacks and assessment. These are not restricted to the following:

- Active Program Scripting Exploits – This activity will utilise injection of malicious scripts into the targeted infrastructure in order to determine the capability of the security infrastructure in detecting and preventing these unwanted traffic penetrating into the network. These malicious scripts can be of several scripting language such as Java, Javascript, ActiveX or VBS which will be injected into the targeted systems/hosts. Scripting exploits generators such as Metasploit and WebScarab will be utilised to generate and launch these traffics into the targeted network. These activities will determine the application layer inspection capability of the current IDS/IPS.
- Malicious Programs attacks – These include programs such as Trojan Horses, Worms, Viruses and Backdoors which will be injected into the network to check the capability of the security

infrastructure (firewalls, IDS, IPS) in detecting and preventing these malicious programs. Common programs such as Trojans (Trinoo, BackOrifice), Exploit worms (Zotob, Sasser) among others will be tested for detection and prevention.

It is important to mention that no malicious programs or scripts will be deployed on any production system environment. The scenario will utilise a dedicated target host(s) deployed within a specific network wherein it will launch or receive the attacks from another source outside the network of concern. This is much like a client-server approach to launch the scripts and malicious programs. The security infrastructure particularly the firewalls, IDS, and IPS will be tested for their capability in detecting and mitigating these attacks into the network. This will check if the security infrastructure is currently up to date in its detection capabilities such as signature matching and so forth.

II. INTERNAL NETWORK SECURITY ASSESSMENT METHODOLOGY (ACTIVE DIRECTORY FLAG CAPTURE)



In this chapter is the Internal Network Assessment that Executor is providing, is an active form of security assessment where our team of offensive cyber security experts seeks to exploit vulnerabilities within your organization starting from the endpoint (technical, organizational, or other) to achieve the proposed objective. We then leverage the initial foothold for lateral movement, penetrate further into the environment to increase influence or control, and provide an understanding of the risks and potential impact to the organization if similar actions were to be taken by a cyber threat actor. While any penetration test does carry some associated risk, the value to the organization far exceeds any potential downside. We align our methodology with the tenets of several penetration testing standards including the Open Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), NIST Technical Guide to Information Security Testing and Assessment (Special Publication 800-115), and Open Web Application Security Project (OWASP) Testing Guide. Finally, we map our testing to the tactics and techniques presented in the MITRE ATT&CK (Attacker Tools, Techniques, and Common Knowledge) Enterprise Matrix to help define the techniques used and highlight areas of concern using an established lexicon. The steps that we take during the penetration testing phase will be limited in strict conformity to agreed-upon rules of engagement scope of work. The following is a list of possible tactics that may be used, should they be included in the agreed-upon scope.

1. INITIAL ACCESS

There are many techniques that can be used to obtain initial access, or compromise, a computer network or other information system. Client-side attacks remain a current favorite of real-world threat actors. These include drive-by downloads, where a user is lured to a malicious website which then seeks to compromise the system through execution or download of malware, as well as phishing and spear phishing attacks, where users are sent communications by email, social media, or other communications channels leveraging a social engineering ruse to trick the user into taking actions beneficial to the attacker. Credentials obtained through social engineering, password guessing, password spraying, and credential stuffing attacks (where credentials compromised from one organization are reused in an attempt to access another organization) can also be used to achieve an initial foothold through remotely accessible systems.

Public-facing IT resources may be directly attacked from the Internet, or through partner networks, to exploit technical vulnerabilities that may be exposed. Unpatched services and similar technical vulnerabilities provide easy footholds and targets of opportunity for a wide range of threat actors. Similarly, remote access services offered by your organization to remote employees' branch offices may also be directly attacked if misconfigured or otherwise improperly secured.

Physical security attacks may also be used to facilitate initial access through the use of hardware injectables, remotely accessible devices that can be used to provide an initial foothold inside an environment; facilitate reconnaissance of an internal environment; or steal network traffic, authentication credentials, or other information. Removable media, weaponized to achieve installation of malicious software, might also be used in conjunction with social engineering ruses to effectively achieve an initial foothold inside your organization. Physical access to systems can also be used to defeat operating system access controls providing direct access to store data.

Access to an organization's information resources may also be achieved by leveraging third-party devices which may be trusted by the target organization. Examples include supply chain attacks to inject malicious code or otherwise leverage a supplier relationship to provide a tactical advantage that results in initial access. Trusted organizational relationships, such as partners or customers, also provide an opportunity for an attacker to leverage a position of compromise in an external organization to achieve an initial compromise of your organization. This would include devices trusted by your employees and allowed access to your organization's internal resources through a bring your own device (BYOD) program.

Many of the techniques available to real-world adversaries are not available to our ethical penetration testing teams. Bribing or blackmailing employees of your organization to install hardware or software injects, compromising third-party sites and leveraging their position to further penetrate your protected systems, and leveraging personal relationships with members of your organization to obtain a position of advantage are all commonly used techniques that are outside of the scope of any ethical penetration test. To simulate these types of activities, we may agree to include an "assumed compromise assessment," where an initial foothold on a standard client machine inside of your organization is provided and subsequent lateral movement capabilities are assessed, in the scope of work.

2. EXECUTION

This pervasive technique refers to an attacker executing malicious code on your systems. It can be used as part of initial access or in support of almost every other adversary tactic. Our team will attempt to achieve execution in a multitude of different ways including but not limited to:

- Exploitation of vulnerable services, including through overflow or other unpatched vulnerabilities or misconfiguration issues
- Command interpreters including cmd.exe, PowerShell, Microsoft Connection Manger Profile Installer, bash or other *nix shells, or other means
- Execution of malicious executables, scripts (including embedded macros), compiled HTML files, HTML applications, and others by users or automated processes
- Component Object Model (COM) and Distributed COM (DCOM) attacks, Windows Management Instrumentation, Windows Remote Management, Remote Desktop Protocol, ssh and similar remote access protocols
- Scheduled tasks, cron jobs, and similar automation system attacks
- Auto Start Extensibility Point manipulation including but not limited to Registry keys, startup items, atbroker, services, and similar automated processes
- Path manipulation, DLL hijacking, and library manipulation attacks

The specific techniques used will depend upon the attack surface, the rules of engagement (stealth or exhaustive testing) and the likelihood of success of one technique compared to others. The execution tactic will be utilized throughout the penetration testing process in support of other tactics listed.

3. PERSISTENCE

There are myriad techniques that can be used to achieve tactic of persistence (MITRE ATT&CK categorizes over 60). This tactic seeks to achieve ongoing access to systems, often outside of standard authentication mechanisms, to ensure attacker access. From a penetration testing perspective, persistence will largely be achieved in order to demonstrate the ability of an attacker to maintain a foothold inside of your environment for an extended period. However, in accordance with our scope of work, our persistence mechanisms will be thoroughly documented and removed prior to the end of the project. We also will not use any persistence mechanisms that represent an increased exposure to your organization. Unless a long-term, adversary emulation or purple team exercise is authorized, our persistence mechanisms will only be installed briefly during the penetration testing period.

4. Privilege escalation

Once an initial foothold is achieved, an adversary frequently attempts to escalate privileges to increase their influence on the impacted system and obtain credentials to assist in lateral to other systems. There are a multitude of techniques that can be used to elevate privileges (MITRE ATT&CK categorizes over 30), and our penetration testing team will attempt to as many as are appropriate for the scope of the engagement.

One of the most commonly employed methods to escalate privilege is theft of user credentials, often from memory of running systems using tools such as Mimikatz. Password hashes or Kerberos tickets can be stolen from the Local Security Authority Subsystem process and passed to other systems to achieve lateral movement with the stolen credentials. Since privileged credentials may be restricted by user access control (UAC), UAC bypasses are another frequently utilized technique. Other sources of credential theft include domain cash credentials, local security account manager hives, Active Directory, and secure user databases, and even plaintext passwords found on endpoint systems.

There are a variety of other ways to escalate privileges on the local system. Vulnerabilities in operating systems may permit local privilege escalation exploits; hijacking, hooking, and injection of DLLs all offer opportunities for privilege escalation; *nix and macOS dynamic libraries and Windows application shims can similarly be hijacked to achieve privilege escalation; poorly configured services can be manipulated to run malicious code; modification of setuid bits, setgid bits, or user ID numbers can be used to elevate permissions; modification of group membership including global security groups and sudoers group, as well as command injection and web shell attacks have all been used to elevate privileges by adversaries. These and other techniques may be utilized by our penetration testing team (in accordance with the scope of work) to assess your preventive and detective controls against these common attack vectors.

5. Defense evasion

To maintain a persistent presence and achieve their actions on objectives, modern adversaries expend significant effort evading the preventive and detective controls in your environment. The MITRE ATT&CK Enterprise matrix lists over 70 specific techniques for this tactic.

One of the most commonly used techniques is to hide in plain sight, using protocols, process names, and tools that already exist within the environment. This "living off the land" approach reduces the adversary's dependence on malware which can be detected in places the burden of network defenders to discern abnormal, malicious activity from normal system behavior. Attackers will seek to conceal their presence on individual systems using process names that blend in with normal system activity. Indirect command execution such as using the Program Compatibility Assistant to execute cmd.exe commands or direct access to System.Management.Automation functions to run PowerShell commands, can be used to evade preventive and detective controls. Process hollowing, code caves, environmentally key payloads, and code injection are commonly used techniques to attempt stealthy execution of code. Scripts, including PowerShell, will typically be heavily obfuscated or encoded to defeat signature-based detection and frustrate analysis activities by network defenders. Adversaries will use stolen credentials and remote access technologies already in place to move laterally.

Attackers will use covert channels, encryption, stenography, as well as commonly employed protocols in order to hide their malicious activity on the network. Polymorphism and similar techniques to evade are commonly employed. They will steal, forge, or install certificates to make encrypted network communications appear legitimate. Port knocking techniques may be deployed to conceal open ports, and hidden windows may be employed to conceal activity from end-users. Attackers will establish command-and-control channels using infrequent, and often inconsistent outbound beacons to make detection of their activity more difficult.

Our penetration testing team has years of experience in conducting adversary operations in a covert manner. We will thoroughly test your preventive and detective controls against a wide range of defense evasion techniques in accordance with scope of work. If desired and included in the scope of work, these techniques can further be refined in a white box manner to test for common vulnerabilities or weaknesses in specific preventive or detective controls in use in your environment.

6. Credential access

Adversaries understand that by using valid credentials to access other systems or elevate permissions, their activity is less likely to be detected, since it blends in with normal network behavior. Credentials can be obtained in many ways. As discussed previously in this document, credentials can be stolen from memory or otherwise taken from a running system. They can be gathered through social engineering attacks, such as fishing and watering hole attacks, captured using tools such as keystroke loggers, or intercepted through local area network attacks manipulation protocols such as LLMNR and SMB. Attacks against Active Directory domains including Kerberoasting, pass the ticket, overpass the hash, golden tickets, silver tickets, skeleton key attack, AD replication attacks and more are very common amongst events adversaries. Valid credentials can even be found in log files or configuration files. Theft of private keys brother certificates used in access control is also an attractive technique for attackers. Our team will perform many of these types of attacks in order to test your networks vulnerabilities, as well as your preventive and detective controls.

7. Discovery

An important adversary tactic, which is overlooked by many penetration tests, is the need for attackers to understand the victim environment in order to locate data of interest. Attackers do not know in advance where valuable assets may be located within your environment, and the actions they take in order to locate such data is often an important stage of the attack during which network defenders to detect respond to the malicious activities. Network mapping, account discovery, cloud service discovery, hunting for files of interest through keyword searches or other mechanisms, sniffing traffic, analysis of virtual environments, and connecting to remote systems offer many opportunities for defenders to detect and respond to malicious behavior within a network. All too often, traditional penetration tests do not perform this critically important tactic, instead simply obtaining privileged access to a system, marking a system is compromised, and moving on to other devices. This lack of realistic adversary behavior often leads to an incomplete understanding of business risk and incomplete testing of defensive controls. Our team will conduct realistic discovery in order to accurately provide you with an understanding of your network security posture.

8. Lateral movement

Often viewed as the main battleground between attackers and defenders, the lateral movement phase of an attack provides defenders with a wealth of opportunities to detect respond to the adversary. Our team will use a variety of different techniques to achieve lateral movement in order to test not only your preventive and detective controls but also your susceptibility to a variety of commonly encountered techniques. Techniques include but are not limited to: reuse of valid credentials for pass the hash, pass the ticket, and similar attacks. Valid credentials will also be leveraged for remote access to services such as RDP, ssh, VPNs, network shares, PowerShell, wmic, etc. In addition to credential reuse, our team employee remote exploitation, abuse of COM objects, scheduled tasks, file copy services, and other techniques is appropriate to your environment to provide a realistic assessment of your controls.

9. COLLECTION, COMMAND AND CONTROL

Once an adversary has established a presence within your environment, they need to be able to achieve operational effectiveness. This requires having a mechanism to control remote systems, collect and collate information within your environment of interest to the adversary, and stage data for later exfiltration while attempting to avoid detection. Collection of data may include techniques including use of screen captures, keystroke loggers, hijacking of microphones and cameras embedded within electronic devices, capturing of network traffic, theft of logical files, and other techniques.

Command-and-control (C2) is necessary to allow the adversary to interact with and control systems in your environment, as well as maintain the resources they need outside of your environment to facilitate the attack. Frequently encountered methods include outbound beacons with varying connection intervals, web shells for inbound communication, use of proxies and tunneling devices, custom-designed protocols, abnormal utilization of protocols and ports, utilization of high-traffic network protocols including HTTP and HTTPS, covert channels, stenography, port knocking, encryption, and many of the techniques. Our team will utilize realistic C2 channels to attempt to evade your preventive and detective controls and give you an assessment of their effectiveness.

10. Exfiltration and impact

Referred to as “Actions on Objectives” in some attack chain models, this is where the attacker is able to achieve their ultimate objective against your organization. Whether this is exfiltration of data from your environment, manipulation of data within your environment, or disruptive attacks against you, the attacker is a variety of techniques that can be used here. Some of these types of activities or destructive and would therefore need to be simulated only in careful coordination with your network defenders. Others, such as data exfiltration, can be performed in a controlled manner to ensure no compromise of the confidentiality, integrity and availability of information during the testing process. As appropriate to the scope of the engagement, we can work your environment to test your readiness to respond to destructive attacks such as ransomware, which involve the need for rapid detection and immediate action immediate action to successfully mitigate their destructive intent.

This final phase of this attack process is unfortunately were all too many incidents are discovered. Our team’s goal will be to work with yours to identify not only vulnerabilities within your environment, but also to identify opportunities for improvement in your preventive and detective controls to increase your ability to detect adversary behavior, decreased the dwell time of an attacker, and improve your overall security posture.

III. APPLICATION PENETRATION TESTING

During this phase, a security expert from will aim to identify additional potential weaknesses in the identified web/stand-alone applications. Based on the review, our experts will provide recommendations where required to allow our customers to quickly and cost-effectively raise the level of security. In order to usefully test the application from a crystal box point of attack, we will require minimum of two valid user names and passwords on any dynamic web applications to allow for thorough testing from every aspect.

The general methodology is outlined below. Some customizations of the methodology may be done, based on the type of application being tested.

The early stage of that phase includes the understanding of the business logic of the application. After the business logic has been determined, various tests will be performed to determine the 'relationship' between the different scripts that make up the application and identify possible ways to manipulate the logic of the application, e.g. by bypassing certain scripts that would do necessary security checks. The security tests to be performed will be based on the OWASP Application Security Verification Standard, which includes but is not limited to the following areas of testing.

1. Injection

During this phase, experts will perform various tests to identify whether there are any injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

2. Broken authentication

During this phase, the application functions related to authentication. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

3. Sensitive data exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

4. XML external entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

5. Broken access control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

6. Security misconfiguration

During this phase, experts will review the secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained, as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.

7. Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

8. Insecure deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

9. Using components with known vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

10. Insufficient logging & monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Executant Security’s ASA includes, but is not limited to, the identification of the following risks:

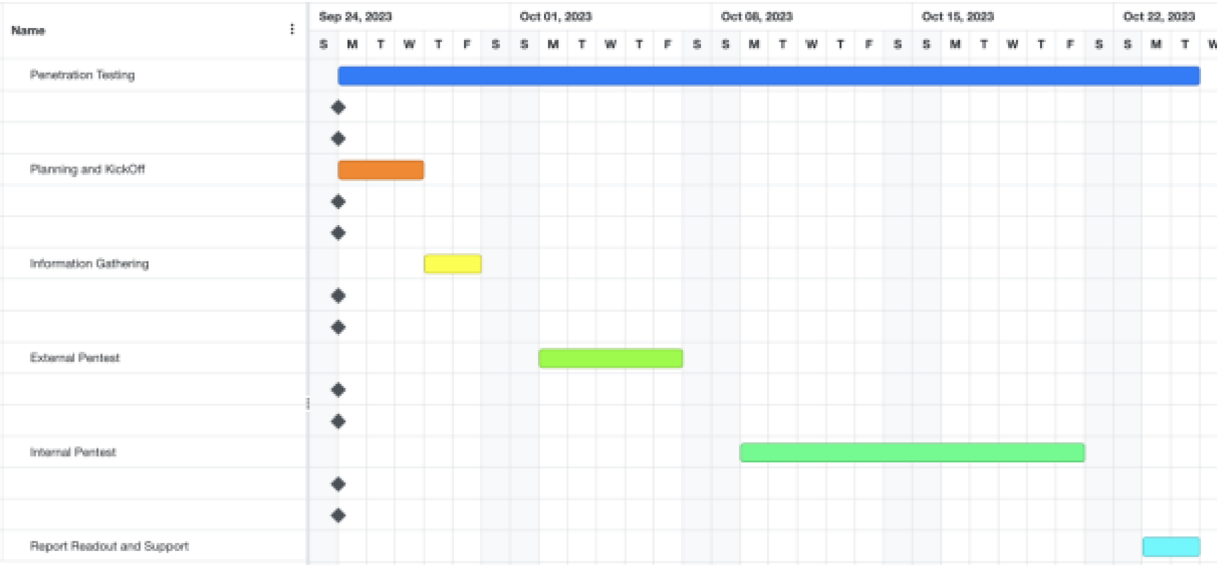
Application Profiling and Information Disclosure	Platform and Third-Party Misconfiguration	Cookie and Session Handling
▪ Default Banners ▪ Unhandled Error Conditions ▪ Application Binary Information Leakage ▪ Extraneous Content in Web Backend ▪ Source Code Disclosure ▪ Unintended Data Leakage ▪ Content Expiration and Cache Control ▪ Insecure Data Storage ▪ Account Enumeration ▪ Backup/Archive Content	▪ Default Administrative Credentials ▪ Default Content and Scripts ▪ Web Server Vulnerabilities ▪ Weak SSL Implementation ▪ Flawed Use of Cryptography	▪ Session Fixation/Hijacking ▪ Set-Cookie Weaknesses ▪ Sensitive Information Disclosure ▪ Cookie Poisoning ▪ Multiple Simultaneous Login Allowed ▪ Session Timeout ▪ Explicit/Implicit Logout Failures ▪ Persistent Sessions ▪ Custom Session Management

Application Profiling and Information Disclosure	Platform and Third-Party Misconfiguration	Cookie and Session Handling
Command Injection Flaws	**Logic Flaws**	**Client-Side Flaws**
▪ SQL Injection ▪ XXE, XPath, and XML Injection ▪ OS Command Injection ▪ Server Script Injection/Upload ▪ Cross-Site Scripting (XSS) ▪ Buffer Overflow	▪ Privilege Escalation ▪ Sensitive Information Disclosure ▪ Data Mining/Inference ▪ Functional Bugs ▪ Application-Specific Control Failures ▪ Weak Data Validation ▪ Race Conditions	▪ Exposure of Sensitive Business Logic ▪ Reliance on Client-Side Validation ▪ AJAX/Web Service Flaws ▪ Interprocess Communication Weaknesses ▪ Client-side Injection
Authentication and Authorization		
▪ Unauthenticated Sensitive Content ▪ Poor Separation of Privilege ▪ Brute-Force Login ▪ Weak Password, Passcode, or PIN Policy ▪ Account Lockout/Denial of Service ▪ SSO Weaknesses ▪ Security Question Weaknesses ▪ Client-side Credential Storage ▪ Anti-automation Flaws		

Executant's security experts perform extensive manual testing, which comprises a significant majority of the testing effort. During this portion of the testing, the our consultant executes the application, and analyzes the communication, functions, and the data the application sends and receives. The security Team tests complex interactions, workflows, and business logic. Additionally, the Team manually evaluates areas of the application and specific vulnerabilities that automated tools either have difficulty with or are unable to identify.

IV. PROJECT TIMELINE

The final schedule will be agreed upon during the project initiation. During the execution phase, the project plan might be adjusted to adapt the situation and respond to identified issues. At this stage, it is not possible to build a detailed project plan since the actual duration will depend on test readiness on the TERMOELECTRICA S.A. side.



Executor offers services to be mobilized within a minimum period of 20-25 business days from official commencement. However, maintaining continuous communication between the teams and early information sharing about plans for individual components can significantly reduce the lead time for the resource's availability.

V. ASSUMPTIONS AND EXCLUSIONS

- All prerequisites will be defined by Executor before starting the assessment. TERMOELECTRICA S.A. will be responsible for fulfilling all prerequisites according to the defined schedule.
- Any documents, network diagrams, configuration files, user accounts, etc. have to be provided before the start of the tasks where these documents/information are needed. Executor will provide a secure way of exchanging sensitive information.
- Executor will provide remediation and/or recommendations but will not be responsible for fixing/mitigating gaps and vulnerabilities.
- Appropriate backups of applications, databases, etc. should be taken by TERMOELECTRICA S.A. before the start of the penetration tests.
- Each activity included within the proposal will be time-based and whenever is needed, the security team from Executor side together with the TERMOELECTRICA S.A.`s team will prioritize the assets and testing scenarios to get the best possible output. The list of IPs in the scope of the tests must be approved by TERMOELECTRICA S.A. In the case of network segments, list of excluded IPs must be provided by TERMOELECTRICA S.A.

VI. THREAT CLASSIFICATION AND REPORTING

During our security assessments or penetration testing, when any exploitable vulnerability is discovered, further research is conducted on that vulnerability to identify its level of severity. For example, a remote exploit which can provide a root or super-user session on the targeted server is classified as a high risk finding; whereas information disclosure regarding an internal hostname would be classified as a low risk finding. The risk is calculated according to the following criteria:

1. IMPACT

The security impact on your web application in the event of an exploitation of this vulnerability by an attacker. This criterion indicates the benefit of the attack to the attacker.

2. Ease of exploitation

The level of difficulty for an attacker to exploit this problem. Difficulty could increase due to technical complexity, the need for prior knowledge of the network, or other factors. This criterion indicates the cost in time and resources of the attack for the attacker.

3. Popularity and ease of identification of the vulnerability

This criterion factors in the public availability of information and tools to detect the vulnerability. Problems that are exploited by Internet worms or that have easy to use exploit code available on the Internet, for example, would get a higher rating. This criterion indicates the probability of an attack.

The risk is classified as follows:

Risk Classification	Characteristics
Critical Risk	Vulnerabilities in this category usually have the following characteristics: Exploitation of the vulnerability results in root/administrator-level access to the system; The information required in order to exploit the vulnerability, such as example code, is widely available to attackers; Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victim systems, and does not need to persuade a target user, for example via social engineering, into performing any special functions.
High Risk	Vulnerabilities that score in the high range usually have the following characteristics: The vulnerability is difficult to exploit; Exploitation does not result in elevated privileges, but may grant unintended access to data; Exploitation does not result in a significant data loss.
Medium Risk	Vulnerabilities that score in the medium range usually have the following characteristics: Denial of service vulnerabilities that are difficult to set up; Exploits that require an attacker to reside on the same local network as the victim; Vulnerabilities that affect only nonstandard configurations or obscure applications; Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics; Vulnerabilities where exploitation provides only very limited access.
Low Risk	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access.
Informational	These are not vulnerabilities, but additional information gleaned from the target during vulnerability testing.

VII. PROJECT DELIVERABLES

At the conclusion of each phase, Executor will provide written documentation of the approach, findings and recommendations associated with the project. The documentation will consist of the following:

1. Detailed technical reports

The reports will be clear enough for Customer Security Team or any other skilled security tester to re-perform the test scenario. All bulk data (like Vulnerability scan results) will be put in MS Excel format. The main document will include:

- The methodology employed
- Tools used (if applicable)
- Positive security aspects identified (if applicable)
- Detailed technical vulnerability findings
- Supporting evidences, screenshots or POCs (if applicable)
- Executive and Management Summary
- Methodology section
- Individual Risk rating based on Inherent and Residual Risk
- An assignment of a risk rating for each vulnerability
- Proposed remediation steps
- Any other recommendations and conclusions of overall security posture (if applicable)

VIII. LISTA INSTRUMENTELOR/PLATFORMELOR UTILIZATE

OpenVas Vulnerability Scanner
Burp Professional
Gobuster, **Dirbuster**, **Filibuster** directory brute-force tools
Nikto web vulnerability Scanner
THC Hydra brute force tool
Nmap, Nmap NSE
Kali distribution
Knowbe4 Phishing attack simulator
KnowBe4 Mailserver Security Assessment

Below is the list of supporting tools and scripts that may be used depending on a specific scenario found and employed across testing cycles (non-exhaustive).

Achilles – A tool designed for testing the security of web applications
ActivePerl – PERL for Windows
ADMft – An FTP brute-force tool
ADMpop – A POP brute-force tool
ADMsmb – An SMB brute-force tool
ADMsnmp – An SNMP brute-force tool
Airsnort – A wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered
Arirang – A powerful webserver security scanner (according to their own description)
Borg – A Free disassembler for Win32 PE files
Browser Password Inspector – identifică parolele neconforme și vechi salvate în browserele Chrome, Firefox și Edge
Brutus – An Windows GUI brute-force tool for FTP, telnet, POP3, SMB, HTTP, etc
Burp Proxy - Burp Proxy is an intercepting proxy server for security testing of web applications.
Cain and Abel – GUI password sniffer for Windows
Chntpw – An image of a (Linux) boot disk that allows changing any password on a Windows NT/2000.
Cisco TFTPServer – A free TFTP Server.
CiscoCFG – Example PERL script that could be used to upload/download config files to/from Cisco routers using SNMP
CiscoCrack – PERL script that unscrambles Cisco level 7 passwords
ciscosnmpdos – Example script to test SNMP DOS vulnerability in Cisco IOS. Payload taken from OULU University SNMP test suite. Using this on a vulnerable router will make it reboot. Use with care!
Cishttpex.pl – Perl script that finds the magic number for the HTTP vulnerability
CmdAsp.asp – An ASP page that allows executing commands on a server
Crack – A password cracker
CrypTool – A Cryptanalysis tool.
cURL – Curl is a tool for transferring files with URL syntax, supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP
DCEtest – This little utility dumps MSRPC endpoint information from Windows systems.
DumpEvt – Dump the event log in a format suitable for importing into a database
DumpReg – Dumps the registry, making it easy to find keys and values containing a string

DumpSec – Dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares

ELSave – ELSave is a tool to save and/or clear a NT event log

Elza – A family of tools for arbitrary HTTP communication with picky web sites for the purpose of penetration testing and information gathering

E-mail Exposure Check Pro - identifică personalul din cadrul organizației dvs. expuși riscului prin accesarea informațiilor din Internet/rețelele sociale, implicand conturile oficiale ale organizației.

Enum – A tool to enumerate, using null and user sessions, Win32 (NT) information

EPDump – A little tool to dump the contents of the endpoint mapper

Ethereal – Ethereal is a free network protocol analyser for UNIX and Windows.

Ettercap – Ettercap is a multipurpose sniffer/interceptor/logger for switched LAN. It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis.

FScan – A command-line port scanner. Supports TCP and UDP

GetAccount – Windows remote user enumerator based on the SID2USER calls

GetPass! – Tools that unscrambles Cisco level 7 passwords

Grinder – Tool that scans a range of IP address to query web servers for a given document

Hackman – Hackman is a freeware hex editor and disassembler

HPing – HPing is a command-line oriented TCP/IP packet assembler/analyser. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

Hyena – Centralised Windows domain management tool. Very useful when auditing 'internal' networks.

ICMPush – ICMPush is a tool that sends ICMP packets fully customised from command line

IDA Pro – Demo (IDA Pro 4.21) and freeware version (ida37fw) of the popular (commercial) disassembler.

IEHistory – The Internet Explorer History Viewer will parse and print the history of URL's visited using the Microsoft Internet Explorer version 3.x, 4.x and 5.x.

IIS5-Koei – Graphical exploit for the IIS5 .printer ISAPI buffer overflow.

IISCat – IIS FPSE bug that allows to view ASP script source code

IISCrack – This ISAPI DLL allows you to gain SYSTEM level access to an IIS 5.0 system.

IISHack – An exploit for a buffer overflow vulnerability in IIS4

Irpas – Internetwork Routing Protocol Attack Suite

Jill – Exploit for the .PRINTER buffer overflow in IIS5

John The Ripper – A password cracker

Joshua – Perl based war dialer

Breached Password Test - verifică dacă utilizatorii dvs. folosesc în prezent parole care se află în baz de date de parole compromise, disponibile public asociate domeniului dvs.

L0phtcrack – NTLM/Lanman password auditing and recovery application (read - cracker)

LANguard network scanner – Port & vulnerability scanner

Legion – This is a Win32 file share scanner

Lsadump – An application to dump the contents of the LSA secrets on a machine, provided you are an Administrator

MingSweeper – A network reconnaissance tool capable of performing Ping sweeps, Reverse DNS sweeps, TCP and UDP port scans, OS identification and application identification

msadc – The famous exploit for th2e RDS vulnerability in IIS4

Msn666 – MSN666 is a simple sniffing program against msn messenger, it intercepts all msn messages on your network, so you could find who is on the net with msn messenger on and who talk with whom.

Metasploit – Exploitation framework

Nbtscan – A program for scanning IP networks for NetBIOS name information

NBTStat – This is a small Unix utility that does the equivalent of NT's nbtstat

NetBIOS auditing tool – Performs various security checks on remote servers running NetBIOS file sharing services

Netcat – The swiss army knife of network tools. A simple utility which reads and writes data across network connections, using TCP or UDP protocol

netddemsg – Privilege escalation exploit for Windows 2000 (up to and including Service Pack 1)

NetE – Null session enumeration tool.

NetSed – NetSED is small and handful utility designed to alter the contents of packets forwarded thru your network in real time.

Netstumbler – Wardriving software.

Netu – Bruteforce password tester using WNetAddConnection2() or RAS.

Netviewx – A tool that lists servers in a domain or a workgroup

Nikto – A web server scanner, based on and inspired by Whisker 1.4. Support for proxy, host authentication, and SSL

Nltest – NLTEST.EXE is a very powerful command-line utility that can be used to test Trust relationships and the state of Domain Controller replication in a Microsoft Windows NT Domain.

NMAP – The best known port scanner around.

N-Stealth – A nice graphical CGI scanner. The software comes with a extensive database of over 19,000 vulnerabilities and exploits.

OpenSSL – The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.

p0f – Passive OS Fingerprinting - A tool that listens on the network and tries to identify the OS versions from the information in the packets.

Phishing security test - phishing-ul propriilor utilizatori este la fel de important ca și un antivirus și un firewall, este o bună practică și eficientă de securitate cibernetică de ajustare a ultimei linii de apărare, care îi reprezintă pe Utilizatori.

Pwdump – Tools that grab the hashes out of the SAM database, to use with a brute-forcer like L0phtcrack or John

RPCTools – The RPC tools package contains three separate tools for obtaining information from a system that is running RPC services

Samba – Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients

Samba-TNG – Samba-TNG is an Open Source/Free Software suite that implements a dce/rpc* library

Samdump – Dumping passwords without being an administrator

SamSpade – Graphical tool that allows to perform different network queries - ping, nslookup, whois, IP block whois, dig, traceroute, finger, SMTP VRFY, web browser keep-alive, DNS sone transfer, SMTP relay check,etc.

Sara – A security analysis tool based on the SATAN model. It is updated twice a month to address the latest threats

Satan – Security Administrator Tool for Analysing Networks

ScanDNS – Script that scans a range of IP addresses to find DNS names

ScanSSH – An SSH version scanner

ShoWin – Show information about windows, reveal passwords, etc.

SID2User – SID2User and User2SID are command line interfaces to WIN32 functions, LookupAccountName and LookupAccountSid

Sing – Send ICMP Nasty Garbage. A little tool that sends ICMP packets fully customised from command line

Skravel – Windows remote user enumerator based on the SID2USER calls

SMBGrind – Tool to brute-force SMB shares over the network (part of CyberCOP)

SolarWinds – Network Management & Discovery Tools

Sqlat – SQL Auditing Tools

SqlBf – MSSQL server brute force tool

SqlDict – MSSQL server dictionary attacker

SqlExec – A little tool that allows to execute commands on an MSSQL server using the XP_CMDSHELL stored procedure

SqlPing – SQLPing is a utility for querying SQL Servers (2000+) listening on UDP 1434 to return detailed information about the instances installed. Note that broadcast addresses may return multiple results.

SqlPoke – Used to scan a range of IP addresses for SQL Servers and then execute a predefined script. Could be used to track down SQL Servers in your own organisation and ensure they stay locked down

SqlTools – Two Unix tools that allow to hack MSSQL servers

SSHWinClient – A full blown Win32 SSH Client implementation

SSLProxy – A tool that allows running non SSL-aware tools/programs over SSL.

Strobe – A command-line port scanner that also performs banner grabbing

STunnel – Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL

Superscan – Simple TCP port scanner with nice GUI. Also performs banner grabbing.

Teleportpro – Software that mirrors websites to your hard disk (Evaluation Version)

THC-scan – A nice war dialer

twwwscan – A fast windows based command line WWW Vulnerability scanner

Typhon – Evaluation version of the commercial vulnerability scanner

UCD-Snmp (aka NET-Snmp) – Various tools relating to the Simple Network Management Protocol including snmpget, snmpwalk and snmpset.

Unix Exploits – Various publicly available exploits

UserDump – Tool that uses RPC mechanisms (LookupAccountSid, LookupAccountName, and NetUserGetInfo) to enumerate users on NT. Bypasses the RestrictAnonymous registry setting

Vlad – An open-source security scanner that checks for the SANS Top Ten security vulnerabilities

WAST – Microsoft Web Application Stress - A tool for stress testing web servers

Weak Password Test - verifică Active Directory la prezența mai multor vulnerabilități legate de parole.

Webreaper – Software that mirrors websites to your hard disk (Freeware)

Wellenreiter – Wellenreiter is a GTK/Perl program that makes the discovery and auditing of 802.11b wireless networks much easier. All three major wireless cards (Prism2 , Lucent, and Cisco) are supported.

Whisker – The most famous CGI scanner

WinDbg – The WinDbg debugger is a powerful, graphical tool that allows you to debug applications on Microsoft® Windows NT® and Microsoft Windows®.

Windows exploits – Various Windows exploits

WinPcap – Packet capture device drivers for Windows. Most sniffing utilities use these.

WinScan – Tool that scans all systems in a domain and enumerates shares, users, etc.

WPoison – Find any potential SQL-Injection vulnerabilities in dynamic web documents which deals with databases: php, asp, etc.