Bank of England PRA

STAR-FS Penetration Test Report Specification

Simulated Targeted Attack & Response Assessments for Financial Services

Contents

Executive Summary

This document presents the specification for the Penetration Test Report deliverable developed by the Penetration Testing service provider (PTSP) during the Penetration Testing (PT) phase of a STAR-FS assessment.

This guide aims to improve standardisation of the STAR-FS Penetration Test Reports and improve the report writing methodology. This document presents the minimum requirements the PTSP should consider while writing a STAR-FS Penetration Test Report.

Minimum requirements are defined in terms of both the structure of the report and the content for each section. Since this document represents guidelines to professional service providers, the content is an example of what should be provided. This format may be adapted at the discretion of the PTSP, but it should include at least the level of detail specified in this document. The PTSP is free to provide additional information in the sections or add more sections to the report, but the report should aim to be as clear and concise as possible. The Penetration Test Report template is included as an appendix to this document from page 26.

Comments and feedback on this document are welcome from all parties and should be sent to **STAR-FS@crest-approved.org.** Please place “[STAR-FS PENETRATION TEST REPORT FEEDBACK]” in the subject line of the email.

This document should be used in the Penetration Testing phase, as described in section 7 of the **STAR-FS implementation guide**.

Legal Disclaimer

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

Copyright notice

© 2024 Bank of England

This work is licensed under the Creative Commons Attribution 4.0 International Licence.

To view a copy of this licence, visit **https://creativecommons.org/licenses/by/4.0/** or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

1. Introduction

Purpose of this document

The main output of the STAR-FS PT phase is the Penetration Test Report. This deliverable is produced by the PTSP for delivery to the firm/FMI.

The Penetration Test Report is accessed by a wide range of stakeholders, including firm/FMIs' board members, senior executive management, technical leaders and subject matter experts (SMEs). The PT Report should therefore meet the needs of both technical and non-technical readers and be understandable by users across a range of different functions in the organisation.

2. Report Structure

This section describes the STAR-FS Penetration Test Report structure and format, including the minimum required sections to be included.

The final STAR-FS Penetration Test Report should show the assessment completed during the STAR-FS PT phase, the methodology adopted, as well as testing results and recommendations.

As mentioned in the introduction, the audience for the STAR-FS Penetration Test Report will vary and the report should accommodate the needs of all categories of readers. As an example, it is likely that an executive summary will be read by Board members or senior management, who will need to understand the strategic implications of the findings. This contrasts with information security or other SME readers, who will need to understand the technical details in far greater detail.

The STAR-FS Penetration Test Report should include the following sections:

- Executive Summary
    - Business Management Executive Summary
    - Technical Leadership Executive Summary
- STAR-FS Results
    - STAR-FS Scenarios summary
    - STAR-FS target actions summary
- STAR-FS summary of findings
- STAR-FS detailed findings and recommendation

- STAR-FS scenario description
- Full report detail

Please see the Appendix which provides a template for this information.

3. Content

This section describes the minimum content required for each section of the STAR-FS Penetration Test Report structure.

Business Management Executive Summary

The report should include an executive summary for the board and senior executive management of the firm/FMI assessed during STAR-FS.

The Business Management Executive Summary should be concise (one or two pages) and written in language that would be readily understood by a non-technical business audience.

This section should address the needs of senior business (not just technical) management within the target organisation, as well as senior regulatory supervisors and potentially other interested parties.

It should go beyond a simple synthesis of the technical test results and where possible comment on the overall implication of the test outcome for the target organisation as a whole.

As a minimum this section should include the following:

- Summary of the STAR-FS engagement, including a description of STAR-FS scope, objectives, timeline, limitations and any other relevant information for board/senior executive understanding.
- Summary and overall assessment of firm/FMI responses to testing and the cyber security of the firm/FMI. This should include a short comment on the firm’s detection and response capabilities and whether this evaluation is above/below expectation for this type of firm/FMI,
- Summary of high level STAR-FS findings and any other material observations. This should be a distilled list of key findings written for the senior management audience, rather than a repetition of a list of issues and a PTSP severity (risk) level.

- An assessment of the implications for cyber resilience and business risk exposure for the Important Business Services (IBS) in scope, both at firm/FMI and industry level.
- A summary of the programmatic recommendations for technical and organisational remediation; and, any other action required as a result of the finding.

Business Management Executive Summary [Example]

PTSP] was commissioned by [firm/FMI] to undertake the STAR-FS cyber security assessment. This exercise was undertaken between [month / year] and [month / year].

The objective of the exercise was to assess the impact and likelihood of a successful, targeted cyber-attack against the [firm/FMI] and its Important Business Services (IBS) targeting their supporting technology assets, personnel and resources.

The approach simulates the tactics, techniques and procedures (TTPs) commonly used by real-world threat actors. The basis of this information was the threat intelligence (TI) report as delivered by the [TISP] in [month / year].

Penetration testing efforts focused on attack scenarios aimed at compromising the Confidentiality, Integrity, and Availability of IBS. The test initially made use of [high level list of methods: phishing campaigns, implant devices, etc.) in order to deliver the attack. [PTSP] was successful in [compromise action] through the use of [attack method] suggesting that [PTSP comment on detect / prevent / respond / recover capability with regards to the attack method used]. OR;

[PTSP] was /[not] able to achieve compromise actions suggesting that [PTSP comment on detect / prevent / respond / recover capability with regards to the attack method used]. As a result of the [PTSP comment on firm/FMI capability] the test made use of ‘leg-ups’ to [outcome – e.g. obtain a foothold into the network].

[PTSP limitations if applicable] The testers encountered [limitation description and root cause– e.g. physical access was not possible due to site closure] which [implications / impact on testing]. This was discussed with the firm/FMI and it was agreed that [agreed course of action and any impact on delivering the attack scenarios].

[PTSP any other matters – for example pen test activity detected by Security Operations Centre how this was confirmed and managed, subsequent actions, impact on delivering attack scenarios, information sharing, etc.]

Overall, the following key findings were identified during testing (set out in detail in the technical sections to this report): … [list of key findings written for the senior management audience] …

[PTSP] therefore conclude that the security environment [comment on control environment – for example falls above, within, below] the level we would expect for this type of organisation. The conclusion on the control environment is specifically driven by the following areas of concern [summary of most significant vulnerabilities]

There is a high risk that Important Business Services are exposed to cyber-attack impact the [Confidentiality, Integrity, and/or Availability] because of [level, significance of vulnerabilities identified during testing, firm/FMI capability, etc.]

[PTSP] recommend the [firm/FMI] to prioritise mitigation in the following areas: [details] to ensure that the risk of an attack on IBSs is effectively mitigated. Further details on recommendations and technical information on findings are included in the remainder of this report.

Technical Leadership Executive Summary

The report should include a technical executive summary for the technology leaders of the organisation (in particular, the CIO and CISO) assessed during STAR-FS.

The Technical Leadership Executive Summary should be short (typically no more than two pages) and set out in clear and specific technical language the key findings, their implications for security and resilience risks and any recommendations.

This section should also provide more information about the:

- A summary and technical assessment of firm/FMI technical performance in relation to its detection and response capabilities. The summary should include a brief description of security weaknesses and detection and response high-level findings.
- An assessment of the underlying cause(s) of issues identified in findings along with highlighting themes or patterns within the results e.g. particular NIST categories being more prevalent than others
- Proposed thematic technical remediation and suggestions for improvements, highlighting in broad but actionable technical detail both longer-term programmatic changes required and priorities for urgent action by technical leaders.

Technical Leadership Executive Summary [Example]

[PTSP] were able to demonstrate control over [metric] of the [firm/FMI] systems supporting the Important Business Services in scope for this STAR-FS assessment highlighting gaps in the [detection / prevention / response] capabilities of the [firm/FMI].

In detail, the PTSP was able to deliver effective attacks and achieve compromise actions against IBS in scope as follows:

Effective phishing campaigns leading to exfiltration of sensitive data impacting the confidentiality of [IBS and supporting systems] due to inadequate user training and awareness programmes;

Successful escalation of privileges providing excess access to information impacting the integrity of [IBS and supporting system] due to ineffective identity and access management controls;

Successful exploitation of application vulnerabilities impacting the availability of [IBS and supporting system] due to lack of configuration baselines and ineffective application traffic monitoring.

As part of our testing a number of key [detective / preventive / response] controls were assessed. Based on the observations above our opinion is that the [detection / prevention / response] capabilities of the [firm/FMI] require significant improvement with regards to the [design / operating effectiveness / maintenance and monitoring].

Our experience during testing and information gathered suggest that while some detective and preventive controls exist and have worked to identify, delay and halt certain attacks, they proved ineffective in preventing attacks from succeeding. This may also be reflective of the relationship between these types of controls and the incident response framework in general to manage incidents from detection through prevention and response.

In summary, the Technical Leadership of the [firm/FMI] should prioritise the remediation of the technical issues outlined in this report through the following recommendations:

Staff Awareness – monitor completion of training and awareness programmes to staff, update the curriculum to reflect current techniques and deliver special training to users in key areas of the firm/FMI;

Identify & Access Management – review access to key systems in line with least privileged principles and enhance SIEM processes to analyse log activity of privileged users;

Configuration management – monitor application configurations against baselines;

Application monitoring – enhance traffic monitoring and analysis and application error handling and response to triggers.

STAR-FS Results

This section should outline all Important Business Services (IBS) and systems in detailed within the Scope Specification and their status of compromise during the penetration test.

STAR-FS Scenario Summary

The STAR-FS Scenario Summary is a simple table describing:

- Scenario - Number and name of the scenario from the TI report and PT plan
- Objective - Result of Scenario assessment in relation to its objectives (Achieved, Partially achieved, not achieved).
- Facilitation - Indicator of information provided by the tested organisation to proceed in the assessment, if any. (Yes/No, information provided)
- Summary of assessment – Short description (max. 10 lines) of the scenario implementation assessment. PTSP should also comment on what controls would need to fail to change the objective from a ‘not’ or ‘partially’ achieved to a ‘achieved’.

All the scenarios agreed during the STAR-FS Threat Intelligence phase – Validation activity should be included in the table. The PTSP can add additional information of other scenarios assessed during the Execution activity, if any.

STAR-FS Scenario Summary [Example]

Scenario	Objective	Facilitation Provided?	Summary of assessment
Scenario 1	Achieved	No	Achieved privileged access supporting systems and data sources, in order to demonstrate the ability to carry out the compromise actions of serious disruption to system activities and user interactions

STAR-FS Scenario Summary [Example]

Scenario 2	Partially Achieved	Yes, access to the internal network was provided	System D was not compromised and code files not accessed. However, the initial phishing campaign was successful and the tester gained access to the internal network
Scenario 3	Not Achieved	Yes, access to the internal network was provided and additional information on network architecture	All the activities were promptly detected by the security team

STAR-FS Target Action Summary

The STAR-FS Target Action Summary is a table for each of the target actions in scope describing:

- System/service name – Name of the system/service in scope of the assessment
- Compromise – Indication of the type of disruption achieved (confidentiality, Integrity and/or Availability)
- IBS affected - List of IBS impacted by the compromise
- Evidence – Flag captured evidencing the compromise
- Detection assessment - Short description (max. 10 lines) of the Target Action and related detection assessment.
- Applicable scenario – Reference to threat Scenario (ID and name) in scope of STAR-FS assessment

All the target actions agreed during the STAR-FS Initiation phase – Scoping activity, formalised in the Scope Specification document, should be included in the report and a descriptive table for each case. The PTSP can add additional information of other target actions assessed or achieved during the Execution activity, if any.

STAR-FS Target Action Summary [Example]

System/service name	System A		
Compromise	Confidentiality	Integrity	Availability
	Yes	Yes	Yes
Important Business Services affected	IBS A		
Evidence	Achieved privileges access on System A and its data sources		
Detection assessment	Poor detection. The system A is not actively monitored and PTSP actions no detected. The following procedures (…) were implemented		
Applicable Scenario	Scenario 1		

STAR-FS Target Action Summary [Example]			
System/service name	System B		
Compromise	Confidentiality	Integrity	Availability
	Yes	No	No
Important Business Services affected	IBS A		

STAR-FS Target Action Summary [Example]	
Evidence	The PTSP was able to exfiltrate specific data file
Detection assessment	Poor detection. The system B is not actively monitored and PTSP actions no detected. The following procedures (…) were implemented
Applicable Scenario	Scenario 1

STAR-FS Summary of Findings

This section should outline (at high level) the findings identified during the STAR-FS execution.

The findings should be described via a STAR-FS findings table, providing a brief summary of all the results found during the STAR-FS assessment and the following information:

- Finding ID # - Finding reference number.
- Finding – Finding short name and short description of the finding.
- Scenario – Reference to Scenario IDs.
- Impact – Indication of impact level (Very Low/Low/Medium/High/Critical). This should reflects the amount and type of data exposed, privilege level obtained, scope of systems, proportion of users affected and possible business ramifications that the technical finding exposes. Further guidance on Impact levels is provided in the following paragraphs of this section.
- Speed of Impact – Indication how quickly the impact could materialize in relation to the preventative and detection capabilities of the organisation. This speed of impact indicator is inversely proportional to the presence and effectiveness of security controls in place in the organization (Very Low/Low/Medium/High/Very High). Further guidance on Speed of Impact levels is provided in the following paragraphs of this section.
- NIST Sub-Category – Mapping to NIST Category and Sub-Category
- Status at the end of STAR-FS - Indication if the finding has been closed during STAR-FS execution (Open/Closed)

The findings should be visually mapped in an Impact / Speed of Impact matrix.

The Impact / Speed of Impact matrix provides the means for the PTSP to assess the impact of a successful attack on the firm/FMI and the relative speed with which the attack can be delivered. There are five impact levels (Critical, High, Medium, Low, Very Low) assessed based on the level of control or access the PTSP establishes on systems supporting IBS enabling the PTSP to successfully deliver all compromise actions defined for these systems. There are also five speed of impact levels (Very High, High, Medium, Low, and Very Low) to capture the relative ease with which the PTSP deliver the attack to achieve compromise actions for each scenario.

The main focus of the assessment should be on the firm/FMI detection, prevention and response capability at each level of the cyber kill chain, the degree of firm facilitation required to achieve compromise actions and the sophistication of tools and techniques used by the PTSP. As opposed to the traditional risk matrix, focusing on impact and likelihood, the impact / speed of impact matrix places less emphasis on likelihood, since in alignment with the Bank's Operational Resilience Consultation Paper1, it is assumed that disruptions to service delivery will occur. The speed of impact dimension is based on the ease with which a threat actor could be expected to exploit the vulnerability. Since each vulnerability, architecture and mitigating controls will be unique to the particular firm/FMI, this is a judgement based on both the nature of the vulnerability and the extent to which effective mitigating measures are place to reduce the ease of exploitation.

Guidance on 'Impact' and 'Speed of Impact' criteria can be found in the following tables:

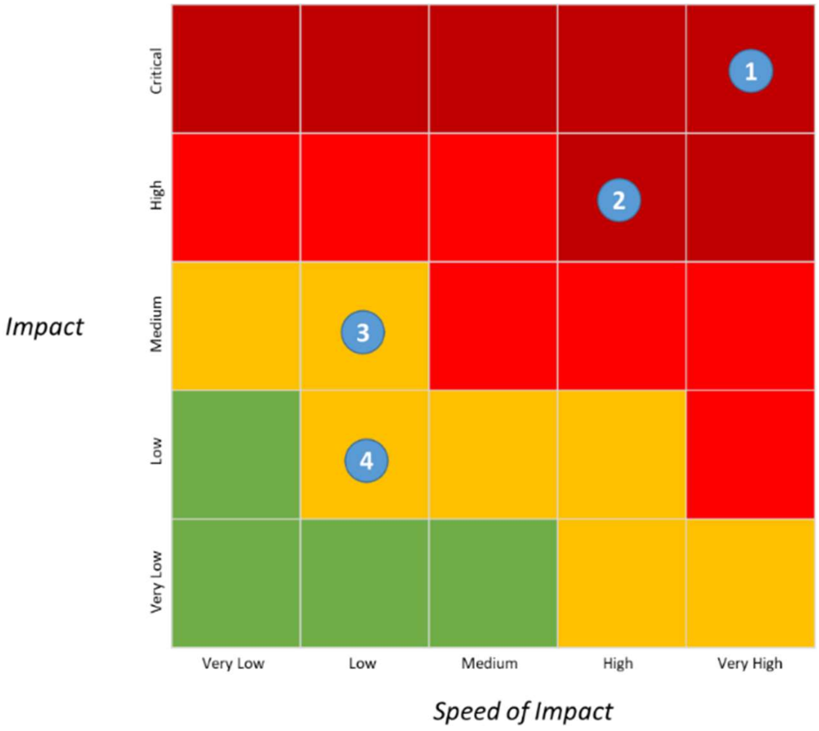
Impact	
Critical	Full control over the target system, all agreed compromised actions delivered demonstrating the ability to significantly disrupt important business services.
High	Partial control over the target system with access to numerous user accounts or sensitive information. Any compromised action is likely to disrupt delivery of important business services.
Medium	Partial control over the target system, with limited ability for significant or large scale compromise actions. Likely to lead to some disruption to delivery of important business services.
Low	No material control over the target system, but the level of control could be leveraged for lateral movement or to perform or prepare other malicious activities.

Impact	
Very Low	There is no control over the target system and therefore no direct impact can be delivered to important business services.

Speed of Impact	
Very High	An attack is easy to deliver without sophisticated TTPs, using readily available information. The firm/FMI is missing key detective or preventive controls. Impact achieved without firm/FMI facilitation.
High	An attack is easy to deliver using established tools and techniques with few prerequisites and no firm/FMI facilitation. Key detective or preventive controls are not operating effectively.
Medium	A relatively sophisticated approach is required using a suite of more customised TTPs. Whilst direct firm/FMI facilitation is not required, the attack's starting point requires some action by firm/FMI users (e.g. social engineering, phishing campaigns, etc.). A longer time is required to deliver the attack objectives.
Low	Key detection controls are well designed and operating effectively, but some gaps exist with preventive controls. Attack delivery timelines are relatively longer and may require firm/FMI facilitation. TTPs do not need to be customised for use on the target system.
Very Low	Key detection and preventive controls are well designed and operating effectively. Attack delivery relies on firm/FMI facilitation. Significant time, resources and detailed prior knowledge would be required to customise TTPs in order to deliver an effective attack.

STAR-FS Summary of Findings [Example]						
ID #	Findings	Scenario	Impact	Speed of Impact	NIST sub-category	Status at the end of STAR-FS
1	Legacy System in use - Systems such as Windows XP are in use in the organisation have an increased likelihood of vulnerability, contain less advanced security protections and prevent other security mitigations from being implemented.	1	Critical	Very High	PR.IP-1	Open
2	Poor Network Segmentation - Controls to separate access to sensitive networks do not seem to have been enforced. All systems were accessible from the endpoint workstation.	1	High	High	PR.AC-1, PR.AC-7	Open
3	Poor detection capability - During testing the tester observed active response and investigations to the simulated attack using an implant from an external perspective, but not when simulating an insider threat.	2	Medium	Low	PR.AT-1	Open
4	Weak Passwords - Some service accounts had weak passwords policies.	3	Low	Low	PR.IP-1	Closed

STAR-FS Impact / Speed of Impact matrix [Example]



STAR-FS Detailed Findings and Recommendations

This section should provide additional details on STAR-FS findings and describe the recommendations proposed by the PTSP to the firm/FMI in order to mitigate the risks identified in relation to each security findings.

The section should include detailed findings and recommendation table with:

- **Finding ID** - Finding indicator. This should match the ID in the previous section.
- **Finding Title and Description** – Finding short name and short description of the finding. This description should provide additional content and details about the findings, describing in details the vulnerabilities and the penetration test evidences.
- **Impact** – Impact level indicator. This should match the risk analysis in the previous section.
- **Speed of Impact** – Speed of Impact indicator. This should match the risk analysis in the previous section.
- **Recommendation** - Description of the mitigation actions recommended to mitigate the risk related to the finding.
- **Recommendation Priority** – Priority for the recommendation(Very Low/Low/Medium/High/Critical)

STAR-FS Summary of Findings [Example]					
ID #	Findings	Impact	Speed of Impact	Recommendation	Priority
1	Legacy system – Part of the systems is running the Windows XP Professional operating systems. This is less secure than Windows 7 and later versions for a number of reasons. Windows XP is out of support and vulnerabilities will remain unpatched. Recent analysis confirmed considerably higher incidences of malware infection in Windows XP rather than other OS. More details can be found in the full report detail document.	Critical	Very High	Upgrade systems to latest Operative System - It is recommended to migrate service from out of support systems as soon as possible and then limit these in segregated network. Where not possible, make sure that legacy systems are not exposed to the public internet. Implement virtualisation of environments were possible.	Critical
2	Poor Network Segmentation – There is an evident lack in the segregation of critical network environment. Testers were able to connect to administrative servers in Domain 1 from standard corporate network. Testers identified a lack of network controls and traffic was not restricted between different geographies. Lack of network segregation may help attacker to access directly privileged position on critical systems.	High	High	Kick off a Network segmentation programme - It is recommended to assess the whole network from the high level and define a strategy, considering what zones are required at minimum. Review the network architecture in line with your strategy and then implement network access control, firewalls and intrusion prevention systems accordingly to the new organisation's policies. It is advisable to adopt behavioural controls based on data analytics in order to improve	Critical

				monitoring and detection of malicious activities.	
3	Poor detection capability – Limited detection capability was observed. There are limited automated controls and response activities were actioned after many days from the start of the delivery of the payloads. No additional activities were observed, therefore we deduct the detection and incident response was not enforced, even if testers were trying unauthorised actions on the systems.	Medium	Low	Review detection and response capabilities - It is recommended a review of monitoring systems configuration and related detection processes to ensure that malicious activities are effectively detected and promptly analysed. In detail, where alerts are raised, an incident response process should be in place to investigate any potential attacks.	High
4	Weak Passwords – Multiple service account are configured with weak passwords policies. The tester was able to crack a large number of passwords. Examples of weak passwords found are: Abcdef, 123456, London, Admin, Test.	Low	Low	Strengthen Password policies. Update password length and review password configuration for complexity, history and expiry. In addition, consider changing the password policy to require service accounts to have their passwords changed every 90 days. Consider performing regular audits of administrator passwords to identify weak passwords.	Medium

STAR-FS Scenario Descriptions

In this section, PTSP should provide a description of how the STAR-FS threat scenarios have been implemented. The description should detail all the steps and actions carried out for each of the agreed testing scenarios.

The section also should provide further details regarding the issues discovered, together with detailed comments on the recommendations and references made, where appropriate.

Scenario # description

For each scenario the following elements should be provided:

1. A visual representation of the scenario implemented in the IT infrastructure of assessed organisation. As a minimum requirement the following details should be presented:

- Clear visualisation and link of tactics and techniques based on MITRE ATT&CK, Cyber Kill Chain or any other recognised framework
- Clear indication of attack path and techniques employed (e.g. phishing campaign)
- Clear reference to the perimeter and targeted infrastructure systems
- Clear link to compromise action (Confidentiality, Integrity, Availability) and
- Clearly mark test outcome (success / failure)

2. A high level description of methodology, actions implemented and results for the scenario.

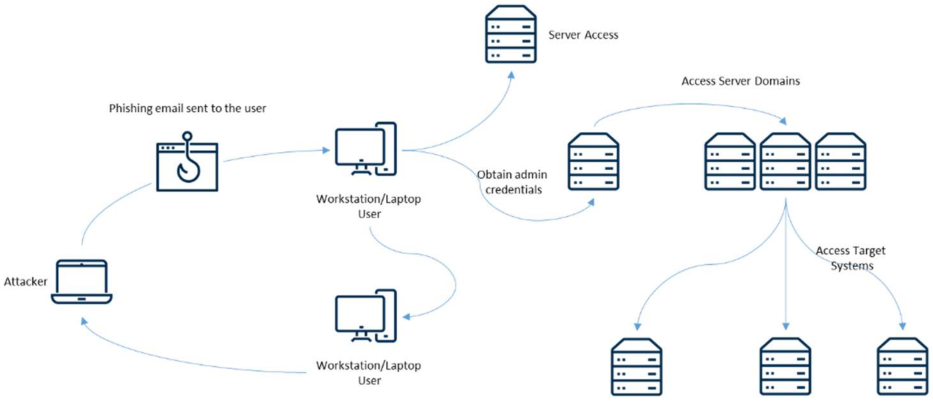
3. A table with the list of all the actions executed in the scenario and their results including:

- Summary of Actions - Short description of the actions implemented. This should include indication of tools, techniques and tactics used.
- Results - Short description of the results of the action, indicating its success or failure.
- Mapping to Finding ID# - Reference to findings (if any). This should align to indicators in the previous section.

4. A table with the Mitre attack mapping (**https://attack.mitre.org/**):

- MITRE ATT&CK Stage – Reference of the MITRE Stage (Recon, Weaponise, Deliver, Exploit, Control, Execute, Maintain)
- MITRE ATT&CK Tactic – Reference of the Tactic (Initial Access, Execution, Persistence, Privilege escalation, Defence Evasion, Credential)
- MITRE ATT&CK Technique - Reference of the Technique (Txxx)
- Outcome - Failed/Success (or not tried if planned but not implemented)

Example - Scenario # description



Summary

PTSP identified that local administrator profile was enabled in Windows 10 and delivered a successful brute force attack against local administrator password on a Windows PC which resulted in escalation of privileges with the testers ‘running as’ local administrators.

From information gathered during the TI phase and during the course of testing the PTSP concluded that during the recent deployment of Windows 10 the firm followed a process which involved provisioning PCs with a copy of the same Windows 10 image which had the local administrator enabled leading to every PC provisioned via this image having the same credentials. It was possible for the PTSP to use the one password to unlock each of these endpoints.

Furthermore, through the local admin user the PTSP was able to install malware and obtain sensitive information and other passwords for software installed on the machine, including systems that support Important Business Services in scope.

After discussion with the firm on its approach in provisioning Windows 10 as demonstrated through the level of access gained through the use of local admin credentials it was agreed that there was sufficient evidence to demonstrate that scenario 1 was achieved and that the risk of attack and the impact from compromise actions was a likely possibility.

Summary of actions

Summary of Actions	Results	Finding ID #
PTSP using repetitive and iterative mechanisms and tools guessed the local admin password of their own machine before	From public resources such as LinkedIn and job recruitment boards the PTSP identified that the firm was looking to hire skillsets for rolling out Windows 10 and implementing Microsoft Local Admin Password Solution (LAPS). By using tools to extract their own local admin password	

Summary of Actions	Results	Finding ID #
delivering brute force attack.	they delivered a brute force attack on the basis that the default password was still in use for some of the PCs and that the local admin password was enabled. After a number of attempts the local admin credentials for initially one Windows PC and then another five were obtained.	
Spear phishing emails targeting credential theft via legitimate looking portals, to gain access to user email accounts	Spear phishing was performed as a spear phishing exercise that targeting 10 employees. A low click rate was registered during the exercise.	
Installation of remote access malware on end user systems.	PTSP was unable to deploy malware remotely during the engagement timescales. This was partially due to the low click-through rate for the emails delivered, however all discovered (via user clicks) browsers were vulnerable to an exploit.	
Use of hacking tools and built in system tools to obtain user credentials and access to additional systems, including domain administrator credentials.	PTSP managed elevating local privileges and gaining full privileged access to the […] domains, which in turn resulted in access to a large number of systems.	1
Elevate privileges to be in position so that the threat actor can deploy destructive malware across the network.	PTSP gained access to a number of systems that are believed to be related to the outlined IBS and given the level of access, would have been in a position to deploy destructive malware to all Windows domain systems.	2
Activate the implants across the domain to simultaneously cause a	Deployment of executables across all systems was not performed given the critical nature of the systems under test, but PTSP consider that the domain admin level access obtained over	3

Summary of Actions	Results	Finding ID #
full DoS condition across the network.	the […] domains would allow an attacker to initiate this. The access obtained to […] environments was at standard user level, and further time would be needed to determine the effort required to elevate to a root user and deploy destructive malware.	

MITRE ATT&CK Mapping

Stage	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Outcome
Deliver	Initial Access	T1190 Exploit Public-Facing Application	**Failed**
		T1189 Drive-by Compromise	**Failed**
		T1192 Spear-phishing Link	**Failed**
	Discovery	T1046 Network Service Scanning	**Not tried**
Exploit	Persistence	T1133 External Remote Services	**Success**
		T1053 Scheduled Task	**Success**
	Defensive Evasion	T1036 Masquerading	**Success**
	Collection	T1113 Screen Capture	**Success**
		T1125 Video Capture	**Success**
Control	Command and Control	T1094 Custom Command and Control Protocol	**Success**

Stage	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Outcome
		T1032 Standard Cryptographic Protocol	**Success**
	Execution	T1035 Service Execution	**Not tried**
	Privilege Escalation	T1078 Valid Accounts	**Success**
Execute	Defensive Evasion	T1107 File Deletion	**Success**
	Test Capabilities	T1358 Review logs and residual traces	**Success**
Maintain	Defensive Evasion	T1070 Indicator Removal on Host	**Success**

Full Report Detail

- Technical evidences and artefacts (e.g. command lines, system logs, snapshots, etc.) should be included in the “Full Report” section and form part of the evidence prepared by the PTSP and shared with the firm/FMI to support findings and recommendations included in the PT report.
- Technical evidence and artefacts should not be shared with the Regulator(s). However, the Regulator(s) may request this evidence to facilitate further discussions with providers and the firm/FMI as part of the STAR-FS exercise. In circumstances where the full report is shared the Regulator(s) should receive a redacted copy with no actionable information, technical details, or any other business and technical sensitive information (e.g. Personally Identifiable Information).
- As a minimum, this section should contain a log of significant actions executed during the assessment by the PTSP. The information reported should be relevant for use of the firm/FMIs in debriefing their detection and response activities.
- The PTSP should also include technical evidence supporting all the assessment assertions described in the previous sections (e.g. sufficient evidence to demonstrate and validate the technical findings).
- This section can be provided as a separate document, as needed or required by the firm/FMI.

- As a reminder for the firm/FMI, the reports shared with the Regulator should be redacted of sensitive information (e.g. PII, emails and related information, systems name, IPs, etc.) related to the firm/FMI organisation and IT infrastructure.

Document Management

- At the end of the STAR-FS Penetration Test phase – Execution activity, the draft Penetration Test Report must be issued by the PTSP within two weeks of test completion.
- The PTSP should deliver the report to the Firm/FMI in sufficient time ahead of the Penetration Test Review workshop
- A final Penetration Test Report produced by the PTSP for delivery to the Firm/FMI
- The report shared with the Regulator(s) should be redacted of sensitive information (e.g. PII, emails, systems name, IPs, etc.) related to the firm/FMI organisation and its IT infrastructure.
- The report must be shared only via the secure channels and protocols agreed during the STAR-FS Initiation phase.

Appendix – Penetration Test Report Template

1. Business Management Executive Summary

<insert summary statement here>

2. Technical Leadership Executive Summary

<insert summary statement here>

3. STAR-FS Results

STAR-FS Scenario Summary

<insert summary statement here>

STAR-FS Scenario Summary [Example]			
Scenario	Objective	Facilitation Provided?	Summary of assessment
Scenario 1	Achieved		
Scenario 2	Partially Achieved		
Scenario 3	Not Achieved		

STAR-FS Scenario Summary [Example]

STAR-FS Target Action Summary

<Insert summary statement here>

STAR-FS Target Action Summary [Example]			
System/service name	System A		
Compromise	Confidentiality	Integrity	Availability
Important Business Services affected			
Evidence			
Detection assessment			
Applicable Scenario			

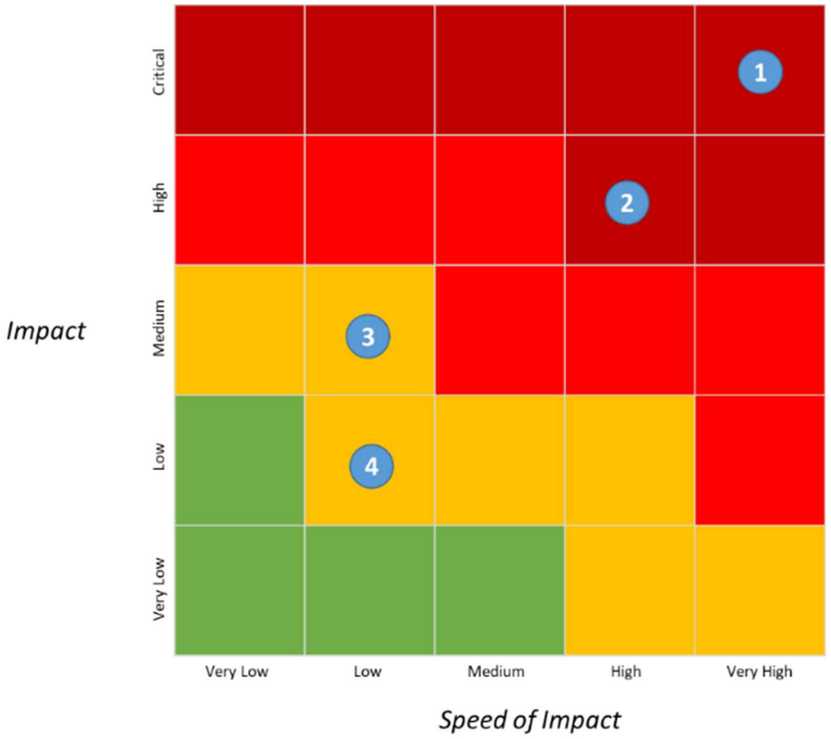
4. STAR-FS Summary of Findings

<insert summary statement here>

STAR-FS Summary of Findings [Example]

ID #	Findings	Scenario	Impact	Speed of Impact	NIST sub-category	Status at the end of STAR-FS
1		1	Critical	Very High	PR.IP-1	Open/Closed
2		1	High	High	PR.AC-1, PR.AC-7	
3		2	Medium	Low	PR.AT-1	
4		3	Low	Low	PR.IP-1	

STAR-FS Impact / Speed of Impact matrix [Example]



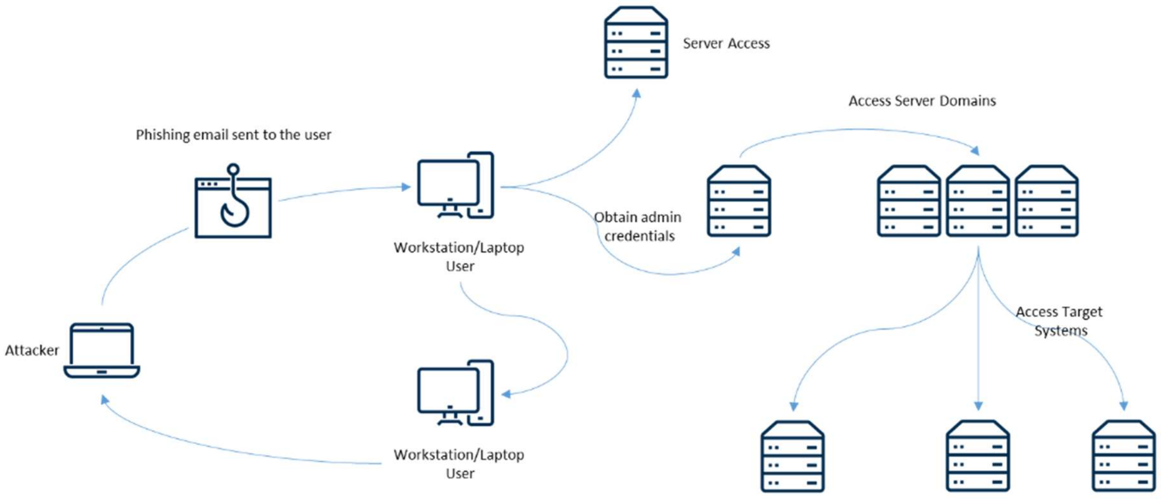
5. STAR-FS Detailed Findings and Recommendations

<Insert summary statement here>

ID #	Finding Description	Impact	Speed of Impact	Recommendation	Priority
1					
2					
3					
4					

6. STAR-FS Scenario Descriptions

Scenario 1



Summary

<insert summary statement here>

Summary of actions

<insert summary statement here>

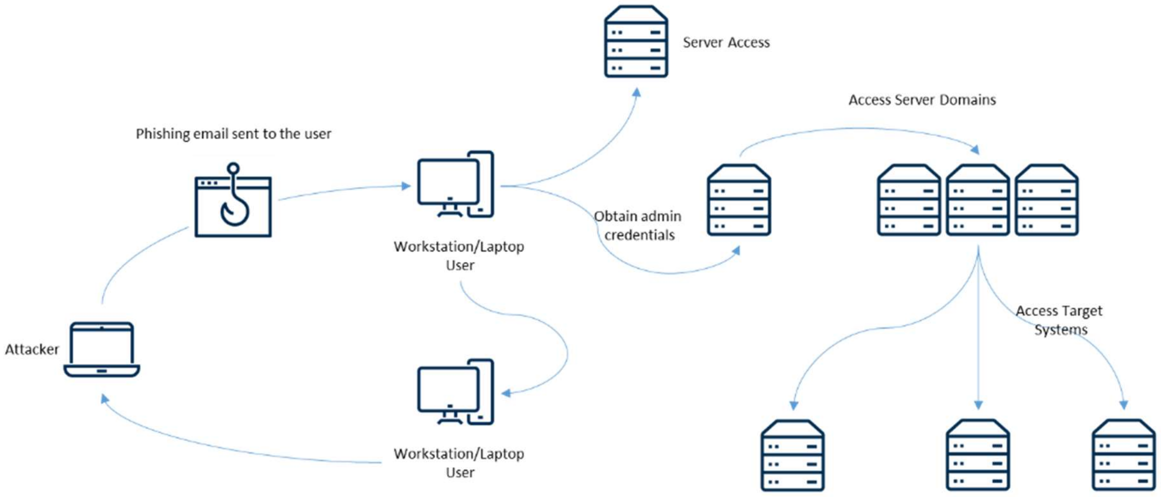
Summary of Actions	Results	Finding ID #

MITRE ATT&CK Mapping

<insert summary statement here>

Stage	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Outcome
Deliver	Initial Access		Failed Not tried Success
			Failed
			Failed
	Discovery		Not tried
Exploit	Persistence		Success
			Success
	Defensive Evasion		Success
	Collection		Success
			Success
Control	Command and Control		Success
			Success
	Execution		Not tried
	Privilege Escalation		Success
Execute	Defensive Evasion		Success
	Test Capabilities		Success
Maintain	Defensive Evasion		Success

Scenario 2



Summary

<insert summary statement here>

Summary of actions

<insert summary statement here>

Summary of Actions	Results	Finding ID #

MITRE ATT&CK Mapping

<insert summary statement here>

Stage	MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Outcome
Deliver	Initial Access		Failed Not tried Success
			Failed
			Failed
	Discovery		Not tried
Exploit	Persistence		Success
			Success
	Defensive Evasion		Success
	Collection		Success
			Success
Control	Command and Control		Success
			Success
	Execution		Not tried
	Privilege Escalation		Success
Execute	Defensive Evasion		Success
	Test Capabilities		Success
Maintain	Defensive Evasion		Success

Scenario 3

[…]

7. Full Report Detail

<Insert full report detail here>