|  |
| --- |
| ../../../Downloads/logo.pngPenetration Test ReportClient CompanyFebruary 8th, 2019 |



Table of Contents

Executive Summary 3

Summary of Results 4

Attack Details 5

Reconnaissance 5

Host A (Compromised) 5

Initial Access 5

Privilege Escalation 5

Post Reconnaissance/Compromise 5

Host B (Partially Compromised) 5

Initial Access 5

Privilege Escalation 5

Post Reconnaissance/Compromise 5

Conclusion 6

Recommendations 6

Risk 7



Executive Summary

[High level summary with almost 0 technical jargon. This must be easily digestible to any leadership positions regardless of technical expertise. This will be a short description of what the attack was, the scope, what was found and the final outcome and the base risk associated with it.]



Summary of Results

[While keeping at a high level overview you will describe the results found. This can have technical information as it is mainly read by the recipient of the report that will be able to start of remediation’s.]



Attack Details

[The following sections of the Attack Details will contain the report in the order that seems most appropriate to tell the store of the attack. Be sure to add screenshots, commands, etc so that the admins are able to retrace your steps to replicate the attack.]



Conclusion

Recommendations

[Provide a full list of recommendations that the company or client can follow to get the issues resolved. Keep in mind it is not your job to build out a full resolution plan for them. Provide a recommendation and that’s all. Even if you are an internal Red Team its important to let experts fix the problems they are experts to fix. Provide a base recommendation and if they ask for more input then provide it.]



Conclusion

Risk

[Brief explanation of the risk rating you provide to the client or organization. If you are able to gain Domain Administrator for example the risk rating would be high.]