

# Table Of Contents

---

<b>Introduction .....</b>	<b>8</b>
<b>Acknowledgment.....</b>	<b>14</b>
<b>The Setup.....</b>	<b>15</b>
<b>Reconnaissance.....</b>	<b>20</b>
Passive Reconnaissance .....	21
Active Reconnaissance .....	24
<b>Analysis of Reconnaissance Activity .....</b>	<b>57</b>
Analyzing the internet facing server apache logs.....	57
Packet Analysis of the internet facing server.....	62
Log Analysis of the internet facing server .....	76
Additional Packet Analysis of Reconnaissance Activity.....	79
Additional Log Analysis of Reconnaissance Activity .....	84
Report on First Day's Activities.....	88
<b>Weaponization .....</b>	<b>89</b>
<b>Packaged and Ready for .....</b>	<b>95</b>
... Delivery.....	95
... Exploitation .....	95
... Installation .....	95
<b>Analysis of public facing host.....</b>	<b>118</b>
Log analysis of internet facing sever.....	119
Packet Analysis of compromise Linux Server .....	127
Implementing Mitigation Measures .....	154
Report on compromised Web Server .....	156
<b>Spear+Phishing = ?.....</b>	<b>157</b>
<b>Pivoting/Lateral Movement .....</b>	<b>170</b>

---

<b>Command &amp; Control (C2) - Actions &amp; Objectives.....</b>	<b>182</b>
<b>Analysis of Compromised Domain Controller.....</b>	<b>195</b>
Packet Analysis .....	195
Log Analysis of Compromised Domain Controller.....	201
Mapping the Threat Actor's Tools Techniques and Procedures (TTP).....	224
Implementing Mitigation Measures .....	225
Report on Day's Activities – Compromised Windows Domain Controller.....	228
<b>Actions and Objectives .....</b>	<b>230</b>
<b>Analysis of Actions and Objectives of Windows 2008 DC .....</b>	<b>238</b>
Firewall Log Review .....	238
Implementing Mitigation Techniques .....	240
Packet Analysis .....	241
Log Analysis of Compromised Windows Server 2008.....	247
Mapping The Threat Actor's Tools Techniques and Procedures (TTPs).....	262
Implementing Mitigation Techniques .....	263
Report on compromised Domain Controller.....	265
<b>Command and control - spear-phishing.....</b>	<b>267</b>
<b>Lateral Movement and Relay.....</b>	<b>280</b>
<b>Analyzing the Windows 10 beachhead.....</b>	<b>293</b>
Log Analysis .....	294
Mapping the Threat Actor's Tools Techniques and Procedures (TTP).....	342
Packet Analysis of Windows 10 Communication .....	343
<b>Log Analysis of pivoted device (access gained from lateral movement) .....</b>	<b>355</b>
Mapping The Threat Actor's Tools Techniques And Procedures (TTP).....	375
Packet Analysis of pivoted device.....	376
Report on compromise and data breach .....	398
<b>Conclusion.....</b>	<b>400</b>