Departamenti Shkenca Kompjuterike
Studimet Bachelor

Projekt Propozimi për temë të Diplomës

Tema

Exploiting User Trust: Weaponizing Legitimate Remote Access Tools Using Social Engineering Techniques

Mentor:

Studenti: Lundrim Aliu

Tetore, 2024

1. Hyrje e përgjithshme

Ky projekt ka për qëllim të demonstrojë se si mjetet legjitime të qasjes në distancë, UltraVNC, mund të shfrytëzohen për qëllime të paautorizuara. UltraVNC është një mjet i përdorur gjerësisht për administrim në distancë dhe mbështetje, por është gjithashtu cenueshëm ndaj abuzimeve. Ky projekt do të tregojë se si UltraVNC mund të shndërrohet një mjet të rrezikshëm duke përdorur teknikën e inxhinierisë sociale, ku përdoruesi mashtrohen të ekzekutojnë një skedar që duket si një imazh i pafajshëm.

1.1 Qëllimi

Qëllimi i këtij hulumtimi është të tregojë se si aplikacionet legjitime për qasje në distancë mund të përdoren për të fituar akses të paautorizuar në sistemet e përdoruesve. Projekti eksploron përdorimin e skripteve automatizuese dhe teknikave të inxhinierisë sociale për të maskuar qëllimin e keq. Në fund, ky projekt synon të theksojë cenueshmëritë që lidhen me keqpërdorimin e këtyre mjeteve dhe rëndësinë e vetëdijes së përdoruesve për mbrojtje nga sulmet sociale.

1.2 Pyetjet kërkimore

- Si mund të përdoren mjetet legjitime si UltraVNC për të shmangur mbrojtjet e zakonshme të sigurisë?
- Çfarë teknikash mund të përdoren për ta bërë keqpërdorimin e UltraVNC të duket i pafajshëm për përdoruesin?
- Sa efektive janë praktikat e zakonshme të sigurisë së përdoruesve në zbulimin dhe parandalimin e këtyre kërcënimeve?
- Çfarë hapash mund të ndërmerren për të zbutur rreziqet që lidhen me softuerët e shfrytëzuar?

1.3 Hipotezat

1. Mjetet legjitime për qasje në distancë mund të shfrytëzohen lehtësisht për të shmangur masat konvencionale të sigurisë kur kombinohen me taktika të inxhinierisë sociale.
2. Përdoruesit ka gjasa të ekzekutojnë skedarë të maskuar si lloje të njohura të skedarëve, si imazhe.
3. Përdorimi i softuerëve të besuar, së bashku me mungesën e vetëdijes për zgjerimet e skedarëve dhe atributet e fshehura, bën që sistemet të jenë shumë të cenueshme ndaj qasjes së paautorizuar.

2. Shqyrtimi i literaturës

Në këtë seksion, do të diskutohet koncepti i **LOLBins (Living-off-the-Land Binaries)** dhe se si sulmuesit përdorin mjete të besuara për qëllime keqdashëse. Shqyrtimi i literaturës përfshin raste reale ku mjetet për qasje në distancë, si UltraVNC, TeamViewer, dhe RDP, janë përdorur për sulme. Analizoni natyrën dyfishe të këtyre mjeteve, duke përfshirë funksionet e tyre legjitime dhe keqpërdorimin për qasje të paautorizuar.

3. Metodologjia e hulumtimit

- **Zhvillimi i Skriptit**: Shpjegoni zhvillimin e skriptit PowerShell që automatizon shkarkimin dhe instalimin e UltraVNC. Shpjegoni se si skripti përdor komanda të zakonshme për të shkarkuar, konfiguruar dhe ekzekutuar UltraVNC ndërsa maskon ekzekutuesin për t'u dukur si një imazh.
- **Konvertimi në Skedar Ekzekutues**: Përshkruani procesin e konvertimit të skriptit PowerShell në një skedar `.exe` duke përdorur **Win-PS2EXE**. Emërtoni se si një ikonë (imazh) përdoret për ta bërë ekzekutuesin të duket si një skedar i pafajshëm.
- **Ambient Testues**: Përshkruani vendosjen e një laboratori virtual që do të përdoret për të demonstruar sulmin. Përfshini informacione për sistemin e synuar dhe hapat që janë ndërmarrë për të testuar funksionalitetin e skriptit dhe për të vlerësuar efektivitetin e teknikave të inxhinierisë sociale.
- **Ekzekutimi i Inxhinierisë Sociale**: Shpjegoni rolin e rëndësishëm që ka inxhinieria sociale për të nxitur viktimën të ekzekutojë skedarin e dëmshëm dhe metodat e përdorura për ta bërë sulmin më pak të dukshëm (p.sh. hapja e një imazhi si shpërqendrim).

4. Referenca / Bibliografia

https://adamtheautomator.com/ultravnc-silent-install/

https://community.spiceworks.com/t/deploy-and-connect-vnc-via-powershell/972990

https://uvnc.com/docs/uvnc-server/69-ultravncini.html

https://learn.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.4