BAB V

KESIMPULAN DAN SARAN

Berdasarkan hasil uji coba serangan *remote exploit* yang sudah penulis lakukan. Penulis menyimpulkan dan mengajukan saran-saran yang dapat diberikan pada penelitian berikutnya mengenai penelitian yang telah dilakukan dan ditulis pada laporan ini.

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian terkait "Serangan *Remote Exploit* Menggunakan *Arduino Micro* pada sistem operasi *Windows, Linux dan Mac OS*" adalah sebagai berikut :

1. Serangan *remote exploit* dapat bekerja atau dapat dijalankan pada sistem operasi *Windows, Linux,* maupun *Mac OS.* Di dalam proses serangan *remote exploit, payload* merupakan peran penting dalam berhasil atau tidaknya serangan.. Serangan *remote exploit* akan gagal jika *payload* tidak sesuai *format executable* pada sistem operasi target.

2. Serangan *remote exploit* dapat dilakukan pada jaringan yang berbeda, atau secara umum disebut dengan jaringan publik. Melalui *tunnels* pada *ngrok port forwarding*, serangan yang awalnya pada jaringan lokal atau *LAN* dapat diubah menjadi serangan pada jaringan publik melalui *port dinamis* yang disediakan oleh *ngrok,* sehingga serangan *remote exploit* dapat bekerja pada jaringan yang berbeda dan jarak yang berbeda.

3. Serangan *remote exploit* dapat lebih optimal dengan memanfaatkan perangkat lunak *Arduino IDE* dan papan *Arduino*. Tujuan nya adalah sebagai papan ketik otomatis guna mengunduh dan mengeksekusi *payload* secara otomatis pada sistem operasi target, sehingga serangan lebih dioptimalkan dan dimaksimalkan.

4. Dampak pada sistem operasi target yang telah terkena serangan *remote exploit* sangatlah berbahaya, karena penyerang telah mendapatkan hak akses secara penuh terhadap sistem operasi target. Dampak paling berbahaya adalah penyerang bekerja di dalam *background* sehingga apapun yang penyerang lakukan tidak dapat terlihat dilayar sistem operasi target seperti menghapus *file* atau *directory* penting, merubah konfigurasi, mengenkripsi *file*, membuat *backdoor* permanen pada *windows*
5. Hal yang harus diperhatikan dalam serangan *remote exploit* adalah *delay* untuk menjalankan script, konfigurasi *lhost* dan *lport* pada *ngrok* dan koneksi jaringan antara penyerang maupun target harus stabil.
6. Keunggulan menggunakan *Arduino* dibandingkan menggunakan *Usb Rubber Ducky* adalah harga yang relatif murah, dapat dibeli di toko elektronik, dan untuk *HID* bisa digunakan sebagai *keyboard* maupun *mouse*.

5.2 Saran

Berikut ini merupakan saran dari penulis untuk penelitian selanjutnya berdasarkan proses maupun hasil dari penelitian yang telah penulis lakukan, sebagai berikut :

1. Serangan *remote exploit* diharapkan dapat diuji coba secara permanen atau disebut dengan *run persistent backdoor* pada sistem operasi selain *Windows*, yaitu sistem operasi *Linux* dan *Mac OS*.

2. Serangan *remote exploit* dapat diuji coba pada sistem operasi *mobile* seperti *Windows Phone, Android* dan *iOS.*

3. Membuat antivirus untuk melawan *automatic keyboard* dan *remote exploit*.