Với sự phát triển tự động hóa các nghành công nghiệp và sự quan tâm nhiều hơn đối với các vấn đề an ninh mạng cho hệ thống OT.

Để minh bạna tấn công trong hệ thống OT mình mô phư lại hệ thống OT trạm biến áp không người trực. Đây là mô hình phổ biến trong hệ thống truyền tải điện lưới. Các trạm biến áp này khi bị khai thác không những ảnh hưởng đến cuộc sống người dân mà còn đe dọa tới an ninh của một quốc gia.

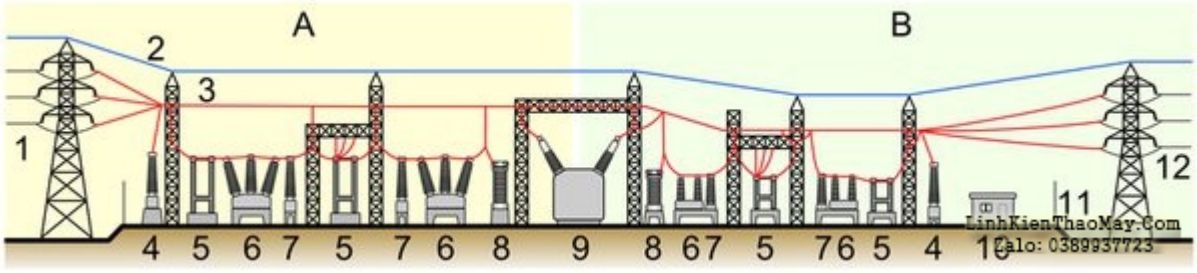
Mô hình thực nghiệm

Hệ thống truyền tải điện thông thường bao gồm các linh kiện:

- Nhà Bộ đổi điện.
- Trạm biến áp trung chuyển.
- Tiêu thụ điện: nhà máy, khu dân cư.
- Phòng điều khiển.



Xu hướng đang chuyển dịch từ các hệ thống cũ tới các hệ thống tự động giám sát và điều khiển từ xa được tích hợp các thiết bị trạm biến áp cho phép thu thập các thông số kỹ thuật của trạm, điều khiển từ xa. Trong mô hình lab này, mình mô phư các trạm biến áp không người trực với các thiết bị như sau:



- Thiết bị đo lường điện áp nguồn vào, ra và cường độ dòng điện tại vị trí máy cắt. Thiết bị lấy thông tin đo lường từ cảm biến sau đó được trung tâm cập nhật thông tin và được hiển thị hệ thống monitoring (4, 7).
- Dao cách ly dụng cụ điện để đóng cắt mạch điện cao áp không có tải hoặc dòng điện nhỏ được sử dụng khi có sự cố, sửa chữa (5).
- Máy cắt hỗ trợ ngắt tải cho giao cách ly có điện áp lớn tại hai điểm dao cách lý tránh cách hiện tượng nguy hiểm như hồ quang điện (6).
- biến áp thay đổi điện áp theo các khu vực sử dụng như tăng áp tại nhà máy, giảm áp gần các khu dân cư (9).
- Thiết bị chống sét (8) bảo vệ các thiết bị.
- Hệ thống đường dây và cột điện (1, 2, 3)
- Hệ thống điện tự dùng.
- Khu vực điều hành, vận hành trực tiếp.

Như mô tả ở trên có thể nhận thấy rằng máy cắt, dao cách ly là những thiết bị có tác động trược tiếp tới đường truyền tải điện do vậy mình minh bạna hệ thống lab mô phư bảng điều khiển máy cắt, dao cách lý thông minh có khả năng giao tiếp với PLC, HMI thông qua giao thức Modbus.

Điều kiện khai thác

Quan điểm an toàn cho hệ thống OT có tính độc lập về an toàn kể cả khi các thiết bị có kết nối tới hệ thống OT hệ thống bị tấn công cũng không ảnh hưởng tới tính an toàn của hệ thống OT. Rủi ro lớn khi các hệ thống điều khiển từ xa có khả năng bị truy cập, hay nhiễm mã độc cho phép tin tặc có thể điều khiển các thiết bị gây mất điện ảnh hưởng tới sản xuất kinh doanh và các khu vực điện trọng yếu.

Trong kịch bản demo lần này, mình tạm bỏ qua quá trình leo thang từ mạng ngoài vào mạng OT và giả định attacker đã có thể kiểm tra được mạng OT thông qua mã độc hoặc backdoor. Attacker sẽ lợi dụng điểm yếu trong giao thức Modbus để tiến hành khai thác vào các thiết bị.

Giao thức Modbus là giao thức được phát triển tương đối sớm và có rất nhiều các thiết được cài đặt. Hầu hết trên thị trường các thiết bị PLC điều cho phép lập trình một cách dễ dàng. Do tính tiện dụng nên được sử dụng rất phổ biến.

Giao thức modbus tồn tại những điểm yếu như không có phương xác thực, không được mã hóa đường truyền. Từ đó tin tặc có thể quét ra các địa thanh ghi được sử dụng khi cài đặt trên thiết bị hoặc được phát hiện bằng việc lắng nghe mạng OT để xác định thanh ghi. Giao

thức không yêu cầu xác thực các ai cũng có thể ghi các giá trị vào các thanh ghi làm thay đổi trạng thái thực thi của thiết bị.

Để hiểu thêm tấn công các tấn công modbus và chi tiết kỹ thuật vui lòng tham khảo bài viết modbus .

Mô tả trình tự thực hiện tấn công

1. Script tấn công thực hiện scan port và xác định dịch vụ dùng.
2. Từ danh sách các thiết bị nghi ngờ, chạy code xác định tất cả các chức năng modbus của thiết bị và giá trị cho các chức năng, tiến hành đọc tất cả các dữ liệu hiện tại.
3. Ghi ngẫu nhiên các giá trị trong khoảng xác định vào coils, holding registers làm rối loạn hoạt động của thiết bị.

TRUNG TÂM SỬA CHỮA ĐIỆN TỬ QUẢNG BÌNH

MR. XÔ - 0901.679.359 - 80 Võ Thị Sáu, Phường Quảng Thuận, tx Ba Đồn, tỉnh Quảng Bình



Thực hiện tấn công bởi: Nguyễn Huy Hoàng.

Hỗ trợ chuẩn bị thiết bị cơ học và lắp ráp: Hoàng Vĩnh Quang.

Các bài viết tương tự:

1. Âm ly 4sò. Model 6300. – Moj ng cho m hỏj bo công suất am ly này lúc đâu chết 2sò vế tráj. M đã thay và đã chạy như con A1013 khj chạy nóg bỏg tay, nge đc mấy ngày là cháy loa và chết sò laj. Đã thay hâu như gân hết lk vẫn vậy. Bo này mua cũg rẻ nhưg m muốn tìm hjểu nguyên nhân.hjx.
2. Bếp từ Sunhouse, nổ sò – Ban đầu khách mang đến, nổ cầu chì, kiểm tra sò hư. Kiểm tra cặp sò driver ko sao, diot 4148 gần khu vực cặp sò ko sao (đã thay thử). thay sò mới, dùng bóng đèn 60W thay cho cầu chì, cắm điện bật nguồn thì nó bị như video. linhk đây ạ:https://www.youtube.com/watch?v=qkiVTg1bf7o. Em thấy ko ổn nhưng ko có hướng nào cứ hàn thử cầu chì vào xem sao, nhưng khi bật nguồn cái, bếp ra từ cái là

tạch luôn sò. Em đo diện áp tại chân G của sò là từ 1 đến 4VDC (điện áp nhấp nháy, ko cố định) ảnh của bếp đây ạ: http://i.imgur.com/Mq1sxGy.jpg http://i.imgur.com/0a9B32F.jpg http://i.imgur.com/hwXIv1z.jpg. :

3. Cách khắc phục lỗi. 1:không stand by được 2:stand by sau 2-5s thì quay trở lại màn hình log 3:Mờ biểu tượng stand by. 4: mục system trong windows task manager chếm dụng trên 20% cpu khiến hiệu suất hoạt động máy giảm sút (lỗi 2 là nguyên nhân cơ bản) khi măc lỗi này máy sẽ gặp vấn đê vê stand by-computer sleep. – Ai đang gặp những lỗi trên vui lòng liên hệ với tiny mino trên facebook http://facebook.com/tiny.mino.3 hoặc LH: 016577082380 để được hướng dẫn.
4. cần giúp đỡ âm ly 8 sò 2 ngày vẫn chưa tìm ra bệnh_áp đói xứng +-17vol qua 2 ổn áp 7912 7812 cấp cho rơ le mạch music master mic,,+-52 cho công suất – ban đâu hỏng công suất chết câu chì,,thay thế và kiểm tra các điện áp chân b công suất =nhau 52 vol,các tâng khuyeh đại thúc, đệm, trở tụ tốt,(,bo nguôn ,ổn áp và công suất đi liên),,,tháo đường 52 vol thì rơ le lại đóng cấp vào lại ko đóng ,bỏ 1 câu chì 1 vế lại đóng(vế đã bị nổ câu chì lúc đâu),,,,kiểm tra ko thấy bị sao? 2 trở cân bằng vê rơ le bảo vệ loa em đo 1 đường vê 52vol còn 1 đường vài mili vol,,,ko hiểu là sao lại chênh lệch thế,,,
5. Dau thu pantesat HD02 Trung Quoc – nguon van binh thuong,khong thu duoc kenh nao,em thu quet do tim may bao khong co ke hoach phat hien
6. may giat electrolux EWF549 – máy giặt electrolux 5,5kg chỉ có 2 nút ấn là start và nút ấn chọn tốc độ và núm xoay chọn chương trình . máy cấp nước giặt được khoảng 5 đến 7 phút là mất nguôn. rút điên ra căm lại thì lại có điện và giặt được khoảng 5 đến7 phút lại mất điện . chưa thực hiện được 1 chu trình giặt- xả văt thì mất nguôn
7. máy giặt panasonic F70A6 lồng đứng – + máy bật nguôn để khoảng 30s máy tự động kéo xả .nhung khi bật chạy thì lại ngát xả và cấp nuocs giạt bình thường nhung đến lân giạt thứ 2 thì lại tụ đọng kéo xả và cáp nuocs nhung khi nhấc canh của hoạc án tạm dùng sau đó bám lai thì lại haotj động bình thường
8. SAM SUNG MODEL CS 21-M16MG – pan mất nguồn không có bóng báo nguồn,đấu tải vào thì nguồn nháy bóng tải đường B+ nhấp nháy…sửa song nguồn không bị nhấp nháy nữa thì hàn hại toàn bộ cắm nguồn vào thì không có bóng báo .màn hình không sáng không có biểu hiện gì.đấu tải thì có tải nhưng bỏ tải ra lại bị mất nguồn..kt nguồn +16.5v,-16.5v,24v,185v đều bị mất…Nguồn 5Q0765,Cao Áp 14A001 và tổng là TDA 9361PS
9. Ti vi samsung slim cs 21z45ml – Co hình trên dưới . E đã kt và thay thử 7845 , diode đường 16v , tụ và các R sung quanh . Nhưng vẫn khôg có gì mới lạ .
10. tivi TCL model kg nhớ rỏ tại gấp quá””’tại lãnh sữa tai nhà – bên thứ cấp ””12v có 24v và 110v kg có .đèn nháy 1 nhịp rồi đi đai.e thây IC giao động 1506 và sới lên hết phân nguồn cũng kg ăn thua gì.e nap card mới đăng tin đc. e mới vào diễn đàn mong ae giúp đở e. e cám ơn ae trên diễn đàn nhiều lăm
11. tivimau- sam sung 29 in ic dán – máy ko chạy đo tại chân B sò kim dao động . nhả đèn kích dòng q403 .. kiểm tra tại chân b q403 đèn kích kim dao đông liên tục … e thử tải giả nguồn b+125v ok 3v3 5v 0k đã thay D402 D403 ….
12. tuyển thợ phụ sửa chữa điện tử- điện lạnh(ưu tiên thợ điên tư muốn học thêm điên lạnh) – tuyển thơ sửa chữa điện tử – điện lanh(ưu tiên thợ điện tử muốn học thêm điện lạnh,và ngược lại)có chỗ ăn ở+lương thỏa thuận