Nomad P@ther
Bag of Rocks
The rogues zine

id like to thank the defcon conference, deviant ollam, howard payne, nightowl and the lockpicking lawyer for indirectly teaching me everything i know.

theanarchistlibrary.org

Bag of Rocks

The rogues zine

Nomad P@ther

this is the first issue of Bag Of Rocks.

none of this zine is gonna be written in prose. cuz its hella boring and sounds too much like the bourgeoisie.

the definition of a rock in this context is anything that uses anything in a way that wasnt intended. hacking is a synonym.

there are 3 pillars of Rocks. social engineering, physical and cyber. this zine will mainly be focusing on social engineering and physical since cyber takes

alot of prior knowledge to understand entirely and the equipment necessary is usually prohibitively expensive.

if the reader is a fan of DnD, the idea of a rogue is already known. to everybody else, a rogue is someone that slinks in the background, the thief, the lockpicker, the smooth talker.

all these traits define a rogue and their purpose. they arent frontliners but frontliners are fre-

quently helped by them. they are the masters of observing advantages and taking opportunities when they are seen.

one of the main philosophies i wish to share to the reader is the idea of The Hammer Versus The Chisel

there are 2 ways to break a wall down, the brute force way with a hammer and slowly cutting out large pieces of the wall until there is nothing left with a chisel. think of a rogue as the chisel.

the hammer is more of a barbarian tactic though still is helpful.

The Bag Of Rocks.

this is the rogues toolkit and knowledge. we live in cities, towns and a world made of glass and we all possess a bag of rocks. some are bigger than others, but all can be used to shatter glass.

this zine is being written to expand your bag of rocks. rogues know exactly what to do with their rocks and when (giggity). mastery of the bag of rocks is impossible in my opinion as the world of security and

its exploits is ever expanding with new knowledge and techniques. perfection is the enemy of progress meaning dont worry about becoming a master rogue, thats a futile effort.

the first lesson i wish to impart onto the reader is the importance of patience and observation. the best thing you can do for yourself is slow down and not expect exploits to work instantly.

sets on wish for pennies sometimes but they arent going to be very good. do some research for yourself on locks.

free public librarys more than likely will have some literature on locks or their computers will have access to the internet.

see how the mechanisms work because the best first step to picking locks is to understand how they work.

CAPITALism is a societal poison.
1312. BREAK THE GLASS.
next issue hint: 68616e646375666673 :^]

take hopping a turnstile for example, you need to make sure there arent any transit cops ready to snatch anyone that cant pay the sometimes obscene fare and you need to have proficiency in the technique itself.

this zine is here to teach the reader such, as well as the building blocks of creating their own techniques in the future. observe, discover, exploit.

other resources for rogue knowledge include https://toool.us/education.html and https://www.youtube.com/user/DEFCONConference [btw the author of this zine is in no way affiliated with either of these groups]

now lets define the 3 pillars

Social Engineering

this is using people against themselves, posing as a construction worker to scope out a place, dressing up in a business suit to rob a bank dry without the teller even knowing it happened etc...

Physical

this employs techniques such as lockpicking and alike to exploit flaws in mechanical access control devices like locks and doorknobs etc...

Cyber

this is the most difficult to master division of rocks i would say, it involves some incredibly powerful tools to exploit flaws in electronic systems and devices.

now, there is always a caviat to the rogues skills. some places expect rogues, thats why barbarian tactics exist. all war is based on deception

and illusion. same applies here. do not be afraid to pull out the drill.

now lets lay out a basic toolkit that every rogue should have, ill try to keep this as cheap as possible

a high viz vest and a hard hat, sometimes you can just swipe these from construction sites if you get lucky or get them at home depot
also keep an eye on the ground around construction sites or in bandos.

a lockpick set. something with a 25 thousands of an inch hook and 3 tensioners in different widths is ideal in my opinion but the super duper cheap method is finding an abandoned car that still has windshield wipers, pulling out the rubber strip that actually contacts the windshield and there will be 2 strips of
spring steel inside it, bend one into a tension
wrench and you can sand down the other piece on concrete if you have to though a dremel rotary tool with a sanding wheel is preffered. i have also made them out of bicycle spokes and pliers. thats a little harder to do since they arent the correct thickness when you find them, again dremel and sanding wheel.
alot of hackerspaces/makerspaces have open houses every week so take a peek around different ones, they should have all the tools you need.

a high strength magnet, u can find these in hard drives in abandoned or pilfered computers though they are hard to extract. a fridge

by the springs on each lock will tell you with small indentations on the blank where
you need to file more or less, take off small tiny bits of metal at a time to ensure you dont overfile and ruin the blank, theres also a tool called a packapunch machine that you can actually dial in the code you want and punch the key out by hand but those are eXpensive af and make u look hella sus.
theres another way to Impression is with a photo and a 3D printer, hackerspaces usually have them. take a clear photo with a monocolor backgrounD and bring it into a photoEditing program, Crop away the background and brIng it into the CAD prograM of your choice, extrude it to the desired width and print with as little support material as possible.
then take Away the flash (the excess plastic surrounding the print)
and wham bam afghanistan, you gots a key that hopefully works. super easy, usually super cheap and can be dupLicated again into an actual metallic key.

some suggestions for practice to round out this issue
start paying attention to locks in the wild, take some time to observe the vulnerabilities that surround you and if you feel confident enough, try to exploit them.
(provided of course it is safe to do so, dont get caught and blame me cuz u didnt check around the corner for pigs)
build or buy or steal yourself a pickset, sparrows lockpicks is my vendor of choice, you can get

is again taking advantage of the flaws in the lock and creating binds in the
pins, it is trickier to do with traditional tools but there are picks sold online (aliexpress, sometimes wish, ebay) for no more than 30 dollars usually that will get you into most
tubular locks.

those are the top 3 locks i would spend time on in the wild, there are many other lock designs but they were made with pick resistance in mind. if it says medeco, you can try but they
are very difficult to pick as a novice or even an experienced picker. theres actually a book on picking medeco locks, the name has escaped me but it goes very in depth on exploiting
medecos.

there is also key duplication and impressioning.
you ever seen someone press a key into some clay or silly putty to make a sHillouette? this is how that works and you dont even need a kEy duplication machine to do it.
this is especially helpful for someone thats
moving into a bando and doesnt want to replace the lock or drill it. youll need a keyblank for the specific keyway of the lock
and a set of files. a key bitting guide is incredibly useful too
most common ones to find in the wild are shlage, yale or kwikset keyways. all of these can be found at home depot or any hardware store and are sometimes easy to purloin.
the technique involves inserting the blank and pressing into the pins, the pressure created

magnet can work sometimes but you really want it as strong as you can find.

a hotel key or some kind of plastic card, these are crucial for carding doors and some advanced attacks involve rewriting the magnetic stripe or the RFID technology on the inside of the card.

a wire coathanger or some kind of wire and a doorwedge, these are crucial for gettin into cars.

the bag or thing you store these objects in should be nondescript and black or some solid primary color that isnt red or a color that stands out. most of these tools are legal to own in pennsylvania in non suspicious circumstances, like if youre caught with a ski mask in the same bag for example will get you a misdimeanor and
if youre caught again, a felony so be careful.

in terms of facial coverings, a regular ol blue or n95 mask will do you well, their about as non descript as it gets.
bloc can work sometimes but if youre trying to do something in broad daylight, bloc will stand out too much even with a hi viz and hard hat.

the topic of this issue is locks, these devices and the technology that surrounds them are really easy to exploit and defeat with the correct know how and tools.

theres 2 rules to traditional locksport, dont pick locks you do not own and do not pick locks that are in use.

feel free to ignore those, theres 2 other rules i want to teach the reader

1) do not, ever, under any circumstances, make promises you cannot keep.

1b) do not make time frame promises i.e. do not say you can have something open in under a certain amount of time, you can not guarantee you can keep that promise.

2) (this is probably the most important rule) be patient, you will open it eventually, just be patient and work through it even if your comrades or whoevers with you got ants in they pants and want it open faster.

there are many types of locks but in my experience theres 2 that are the most common, wafer locks and pin & tumbler locks.

wafer locks operate with a series of tiny discs (the wafers) that when the key is inserted, allow the cylinder containing the discs to turn allowing the lock to open.

the exploit is taking advantage of the imperfections in the lock itself, more specifically the discs and their relationship to the cylinder. when you apply tension to

the cylinder with a tool called a tensioner or wrench, there will be one wafer that binds against the top and bottom of the cylinder, then with either what is known as a

jiggler or a hook, you can then move the wafers into place essentially doing the same thing as a key just one wafer at a time. you will be able to identify wafer locks by

the shape and size of the keyway (the place the key is actually inserted and where it travels within

the lock itself) jiggling technique involves just inserting the tool

and rocking it back and forth with tension until the cylinder rotates. using a traditional hook involves searching for the binding wafer and lifting the wafer

until a click is felt on your tensioner, that click is the wafer passing what is known as the shear line and making another wafer bind. move all the wafers into place and

the lock will open.

pin & tumbler locks work on a similar principle though instead of a series of wafers, its 2 kinds of pins that travel inside the cylinder and inside the lock body. the two kinds

of pins are the driver pins and the key pins. key pins interact directly with the key and move the driver pins, the driver pins are kept under spring tension and push the keypins down

the cylinder is never machined perfectly on a pin and tumbler lock so its basically the same technique to picking a wafer lock just instead of a series of wafers to find, its a

series of pins. binds are produced because like stated before the cylinder is never machined perfectly so it will contact the side of a pin. the technique is just finding the binding

pin with a hook tool and lifting until a click is felt.

another kind of lock is the tubular or cylinder lock and theyre usually seen on change machines, septa usually has some on the el for compartments etc..

they work on a similar principle the two previous locks but in a much different layout. the exploit